CASP+ (CAS-004) Exam Foundations

- **CASP+ (CAS-004)**
  - *CASP+ is an advanced-level cybersecurity certification for security architects and senior security engineers charged with leading and improving an enterprise's cybersecurity readiness (CompTIA.org)*

- **Exam Description**
  - CASP+ covers the technical knowledge and skills required to architect, engineer, integrate, and implement secure solutions across complex environments to support a resilient enterprise while considering the impact of:
    - Governance
    - Risk
    - Compliance requirements

- **Four Domains**
  - Domain 1 (29%): Security Architecture
  - Domain 2 (30%): Security Operations
  - Domain 3 (26%):Security Engineering and Cryptography
  - Domain 4 (15%): Governance, Risk, and Compliance

- **Exam Details**
  - Up to 90 questions in 165 minutes
    - Multiple-choice
    - Performance-based/Simulations
  - Recommended Experience:
    - CompTIA A+/Network+/Security+/CySA+/PenTest+ Certifications
    - 5 years of IT security experience or 10 years of general IT experience
  - Released: October 6, 2021

- **Are You Ready?**
  - This course is presented based on a logical order, not based on the sequential order of the domains above (Domain 4, Domain 1, Domain 3, and Domain 2)
  - Take practice exams
  - Did you score at least 90% or higher?
  - If you need more practice, take additional practice exams to hone your skills before attempting the exam

Data Considerations

Objectives 4.3

- OBJ 4.3: Explain compliance frameworks and legal considerations, and their organizational impact

- **Data Security**
  - **Confidentiality**
    - Preventing the disclosure of data or information to unauthorized people or systems
    - How secure is the information, and how secure does that information need to be?
    - Confidentiality fails if someone can obtain and view the data that we are attempting to protect
  - **Integrity**
    - Deals with protecting data from unauthorized modifications or data corruption
    - How correct is the information, and has the data been modified during retrieval, in transit, or in storage?
    - Integrity fails if someone can modify the data during its retrieval, transferal, or while it is being stored
  - **Availability**
    - Deals with ensuring that the data is accessible when and where it is needed
    - How much uptime is the system providing, and is the data always accessible by the end users?
    - Availability fails if the end user cannot access the data when they need it
  - Categorize potential risks by considering the impact to your organization
    - **Low impact risk to confidentiality**
      - An unauthorized disclosure of information will have a limited adverse effect
    - **Moderate impact to integrity**
      - An unauthorized modification will have a more serious adverse effect on the organization
    - **High impact to availability**
      - There will be a severe, potentially catastrophic effect on the organization

- **Data Classification**
  - Data classification is based on its value to the organization and the sensitivity of the information if it were to be disclosed
    - **Public Data**
      - No impact to the company if released and is often posted in an open-source environment such as their website
    - **Sensitive Data**
      - Minimal impact if released and includes data like organizational financial data
    - **Private Data**
      - Contains information such as personnel records, salary information, and other data used only within the organization
    - **Confidential Data**
      - Contains items like trade secrets, intellectual property data, source code, and other data that would seriously affect the business if disclosed
        - **Unclassified**
          - Can be released to the public under the Freedom of Information Act
        - **Controlled Unclassified Information (CUI)**
          - Includes unclassified information that should be protected from public disclosure
        - **Confidential Data**
          - Includes data such as trade secrets and other information that could seriously affect the government if unauthorized disclosure were to happen
        - **Secret Data**
          - Includes data such as military deployment plans, defensive postures, and other information that could seriously damage national security if disclosed
        - **Top Secret Data**
          - Includes blueprints for weapons or other such information that could gravely damage national security if known to those unauthorized for this level of information

- **Data Types**
  - A tag or a label to identify a piece of data under a subcategory of a classification
    - **B-I-G-O-T**
      - British Invasion of German Occupied Territory
  - **Health Data**
    - Categorized as any data related to health conditions, reproductive outcomes, causes of death, and quality of life for an individual or population
      - **HIPAA**
        - Health Insurance Portability and Accountability Act of 1996
  - **Financial Data**
    - Consists of pieces or sets of information related to the financial health of a business
  - **Intellectual Property**
    - A type of data that includes intangible creations of human intellect
      - Copyright
      - Patent
      - Trademark
      - Trade secret designation
  - **Personally Identifiable Information (PII)**
    - Any data that could potentially identify a specific individual
  - **Data Format**
    - This is the organization of the information into preset structures or specifications
      - Structured Data
        - Something like a comma-separated value list
      - Unstructured Data
        - Something like a PowerPoint slide, an email, a text file, or a chat log
  - **Data State**
    - The location of data within a processing system
      - Data at Rest
        - Data is stored on a hard drive
      - Data in Motion
        - Data is currently moving from one computer to another over the network
      - Data in Use

    - Data has now been read into memory or inside the processor that is currently being worked on

- **Data Retention**
    - Maintains and controls certain data in order to comply with business policies and applicable laws and regulations
    - **Data Preservation**
        - Information that's kept for a specific purpose outside of an organization's data retention policy
            - **Short-Term Retention**
                - A term by how often the youngest media sets are overwritten
            - **Long-Term Retention**
                - Any data that's moved to an archive storage to prevent being overwritten
        - All of your backups are going to take up valuable storage space
        - Back up everything you're legally required to base on your retention policies
        - Back up what you need to base on policies or your corporate operations
    - **Recovery Point Objective (RPO)**
        - The maximum amount of time that can be lost after a recovery from a disaster, failure, or comparable event
        - RPO helps drive the recovery window or the redundancy decisions made in your business

- **Data Destruction**
    - **Data Removal**
        - A generic term that refers to any process that deletes or makes some form of data inaccessible
    - **Data Destruction**
        - A step further than data removal that makes an effort to destroy the underlying data
    - **Data Sanitization**
        - A step further than data destruction, it performs a verification function to ensure the data has been wiped and is no longer accessible
        - Organizations may decide to opt for physical destruction of the data

- **Data Ownership**
  - **Stakeholders**
    - Provide the proper data classification for the information security professionals
  - **Data Ownership**
    - The process of identifying the person responsible for the confidentiality, integrity, availability, and privacy of the information assets
      - Data Owner
        - A senior executive role who is mainly responsible for maintaining the confidentiality, integrity, and availability of the information asset
      - **Data Steward**
        - Focused on the quality of the data and the associated metadata
      - **Data Custodian**
        - Responsible for handling the management of the system where data assets are stored
      - **Privacy Officer**
        - A role that is responsible for the oversight of any kind of privacy-related data
        - Make sure that we are complying with the legal and regulatory frameworks
        - Make sure that we have the right purpose, limitations, and consent
        - Ensure that the organization is properly performing data minimization, data sovereignty, data retention, and data destruction
    - **Data owners** should really be the people who know more about the data

- **Data Sovereignty**
  - The principle that countries and states may impose individual requirements on data collected or being stored within their jurisdiction
    - **GDPR**
      - protects the privacy of any European Union citizen, while they are within Europe or within the European economic area or the EU

- That protection only protects you within the walls of the European Union but it does not protect you once you move outside

Risk Management

Objectives 4.1

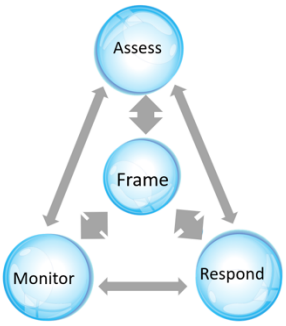
- OBJ 4.1: Given a set of requirements, apply the appropriate risk strategies

- **Risk Strategies**
  - **Facets of Risk Management**
    - Risk Assessment
    - Risk Measurement
    - Risk Handling
    - Risk Tracking
    - Risk Management Lifecycle
    - Risk Considerations
  - **Risk**
    - The probability that a threat will be realized and a continual balancing act of a vulnerability against a threat
  - **Vulnerabilities**
    - Are any weakness in the system design or implementation
      - Software bugs
      - Misconfigured software
      - Improperly protected network devices
      - Lacking physical security
  - **Threat**
    - Anything that could cause harm, loss, damage, or compromise to our information technology systems
    - Risk exists in the intersection area between threats and vulnerabilities, and this is a key point
  - **Risk Management**
    - Finding ways to minimize the likelihood of a certain outcome from occurring and achieving the outcomes that we want to achieve

- **Risk Management Lifecycle**
  - **Risk Management**
    - Helps us see all of the different risk that is out there and puts controls in place to help bring the level of risk down to an acceptable level
    - Risk Management can also help us avoid legal troubles

- Risk Management ensures that we are able to establish trust and mitigate liability

- **Risk Identification**
  - Considers all types of risks or uncertainties that may impact us to achieving a set of objectives
    - Managing Information Security Risk by NIST
      - (National Institute of Standards and Technology)



- **Frame**
  - Aims to establish a strategic risk management framework that is supported by key stakeholders at the top tier of the organization
- **Respond**
  - Focused on the mitigations put into place to lower the risk that was just assessed
  - CompTIA calls it “Control” in the exam objectives
    - 7 Different Categories of Control
      - People
      - Process
      - Technology
      - Protect
      - Detect
      - Respond
      - Restore/Recover
- **Monitor**
  - Evaluates the effectiveness of the risk response measures and identifies changes that could affect how risk can be managed
  - CompTIA calls it “Review” in the exam objectives
  - Risk determination is conducted through performance of a formal risk analysis
- **Qualitative Risk Analysis**
  - Uses intuition, experience, and other best practices to assign non-numeric values to a given risk value
    - Brainstorming sessions
    - Focus groups
    - Surveys

        - Interviews
        - Estimation of the likelihood of the events occurring under the Delphi method
            - Proposed impact severity
            - Loss potential
            - Likelihood of occurrence
    - **Quantitative Risk Analysis**
        - Uses numeric values and monetary values for all parts of the risk analysis
            - Equations
                - Used to determine the total and residual risk, and can provide a cost directly associated with those risks
                - Most risk determinations and risk analysis will use a hybrid approach

- **Risk Types**
    - **Inherent Risk**
        - Occurs when a risk is identified but no mitigation factors are applied
        - Inherent risk is the level of risk in place prior to taking any mitigating actions to reduce the impact or likelihood of that risk being realized
    - **Residual Risk**
        - Occurs when we calculate the risk after we apply our mitigations and security controls
    - **Risk Exception**
        - Any risk that is created due to an exemption being granted or failure to comply with corporate policy
            - **Avoid**
                - Allowing risk exceptions from occurring in your organization

- **Risk Handling**
    - **Risk Avoidance**
        - A strategy that involves stopping a risky activity or choosing a less risky alternative
        - Risk avoidance eliminates the hazards, activities, and exposures that could negatively affect us
    - **Risk Transfer**

        - A strategy that passes the risk to a third party, most commonly an insurance company
    - **Risk Mitigation**
        - A strategy that seeks to minimize the risk to an acceptable level which an organization can accept
    - **Risk Acceptance**
        - A strategy that seeks to accept the current level of risk and the costs associated with it
    - **Risk Appetite**
        - The amount of risk that an organization is willing to accept in pursuit of its objectives
        - Risk appetite is also called risk attitude or risk tolerance

- **Risk Tracking**
    - **Risk Tracking**
        - Systematically tracking and evaluating the performance of risk mitigation actions against established metrics throughout the lifecycle of an identified risk
    - **Risk Register**
        - A tool that is used to identify potential risks in a system or organization
            - Risk Register Should Include:
                - Risk identified
                - Description
                - Level
                - Likelihood
                - Owner
                - Mitigation measures implemented
                - Residual level
    - **Owner**
        - The person responsible for managing the threats and vulnerabilities that might exploit this risk
        - Reassess the risk and determine the residual level
    - **Key Performance Indicators (KPIs)**
        - Used to gauge and measure different things within your organization
            - **Scalability**

        - The ability of a system to handle the increase in demand without impacting the application's performance or availability
      - **Reliability**
        - The measurement of the probability that the system will meet certain performance standards and yield the correct output for a specific time
      - **Availability**
        - The percentage of time that the infrastructure, system, or solution is operational under normal circumstance
    - KPIs tend to be metrics and numbers
  - **Key Risk Indicators (KRIs)**
    - Used to measure risk, instead of system performance

- **Risk Assessment**
  - A tool used during risk management to identify vulnerabilities and threats, to assess their impact, and to determine what controls to utilize
    - Identify assets and their value
    - Identify vulnerabilities and threats
    - Calculate threat probability and impact
    - Balance the threat impact with the cost of counter-measures
  - Risk assessments should be conducted prior to any mergers, acquisitions, or deployment of new technologies
  - Risk assessments can only be successful when they are supported by senior management
    - **Likelihood**
      - A measure of the probability that a particular risk will be realized and impact the organization
    - **Motivation**
      - What causes someone to act
        - Acquisition or theft
        - Business advantage
        - Damage
        - Embarrassment
        - Technical advantage
    - **Magnitude of Impact**

        - An estimation of the amount of damage that a negative risk can achieve or the amount of opportunity cost if a risk is realized
    - **Single Loss Expectancy (SLE)**
        - The cost associated with the realization of each individual threat that occurs
    - **Annual Loss Expectancy (ALE)**
        - The expected cost of a realized threat over a given year
            - SLE x ARO = ALE
    - **Annualized Rate of Occurrence (ARO)**
        - Provides us with an estimate of how many times per year a given threat might be realized

SLE x ARO = ALE
SLE = $2,000
ARO = 3
$2000 x 3 = $6000

    - **Return on Investment (ROI)**
        - A ratio that considers how long it would take to make up for the expense, or investment, by preventing the risk from occurring
        - ROI determines the expected fiscal gains for improvements and balances that against the cost of implementing the changes
            - **Six Types of Loss**
                - **Loss of Productivity**
                    - Occurs whenever there is downtime or repair time
                - **Loss of Revenue**
                    - Occurs during an outage if the system is required for us to receive payments and provide services
                - **Data Loss**
                    - A downtime that reduces productivity leading to productivity loss
                - **Data Compromise**
                    - Occurs whenever there is a disclosure or modification of data
                - **Cost of Repairs**
                    - The actual costs that an organization must pay to procure and replace hardware and software, as well as to any repair companies for their labor
                - **Loss of Reputation**

        - Occurs whenever there is a security incident
    - Decide what to measure and how to perform the estimates
    - **Payback**
        - A calculation that simply compares the Annual Loss Expectancy against the expected savings from implementing a given control
    - **Net Present Value (NPV)**
        - It considers the cost of the money spent today against the savings that we might see tomorrow
        - Your organization's resourcing department has a discount rate they use for calculations
    - **Total Cost of Ownership (TCO)**
        - A financial estimate intended to help buyers and owners determine the direct and indirect costs of a product or service
        - Consider not just the sticker price but also the other parts of the cost of ownership to support the countermeasure
    - **Total Cost of Ownership**
        - Refers to the overall costs associated with running your organization's risk management program
            - Organizations can identify inefficiencies in their risk management programs and work to drive down costs and save money
            - Industry benchmarks aren't always representative of your organization
            - Minor risks should be covered within the organization, not through insurance
            - Utilize risk management software to help when decision making due to the complexity of risk
            - Consider the value of risk management when budgeting because it isn't just about saving money
            - Total cost of ownership analysis doesn't instantly save money
            - The organization cannot solve all possible problems
    - **Mean Time to Recovery (MTTR)**
        - The average time that a device will take to recover from any failure
    - **Mean Time Between Failures (MTBF)**
        - The predicted average time that will elapse between a failure of a component during normal system operation
    - **Gap Analysis**

        - The performance we are experiencing and the performance we expected to provide the users
    - **Trend Analysis**
        - Provides a math-based methodological process for historical data and provides a baseline and possibly a future projection of risk

Policies and Frameworks

Objectives 4.1 and 4.3

- OBJ 4.1: Given a set of requirements, apply the appropriate risk strategies
- OBJ 4.3: Explain compliance frameworks and legal considerations, and their organizational impact

- **Policies**
  - **Separation of Duties**
    - A preventative administrative control that should be considered whenever we're drafting authentication and authorization policies for the organization
    - High risk functions in our organization should utilize proper separation of duties
  - **Split Knowledge**
    - When two people each have half of the knowledge for how to do something
  - **Job Rotation**
    - Different users are trained to perform the tasks of the same position to help prevent an identity fraud that could occur if only one employee had that job
  - **Mandatory Vacation**
    - An employee is required to take a vacation at some point during the year
    - Job rotation and mandatory vacations provide us the ability to cross train our employees and develop trained personnel
  - **Least Privilege**
    - The concept of providing users or services with the lowest level of access required to perform their job functions
    - Not every user needs access to every file
  - **Employment and Termination Procedures**
    - An administrative control that is focused on what to do when hiring and firing employees
      - **Security Awareness Training**
        - Used to reinforce users with the importance of their help in securing the organization's valuable resources
      - **Security Training**

        - Used to teach the organization's personnel the skills that they need to perform their job in a more secure manner
    - **Security Education**
        - Used to gain more expertise and to better manage the security programs in an organization
        - Security awareness training should be developed based on the intended audience
        - Specialized training can be developed for the organization based on the applicable laws, regulations, and business model
- **Auditing Requirements and their Frequency**
    - Any essential items to organizational security that should be discussed in the security policy
    - Know what you will audit and to what level

- **Frameworks**
    - **Policies**
        - Used to state the role of security in an organization and establishes the desired end-state of the security program
        - Policies are very broad and provide the basic foundation upon which the standards, baselines, guidelines, and procedures are built
    - **Organizational Security Policies**
        - Provide general direction and goals, a framework to meet the business goals, and define the roles, responsibilities, and terms
    - **System-specific Policies**
        - Address the security needs of a specific technology, application, network, or computer system
    - **Issue-specific Policies**
        - Address a specific security issue, such as email privacy, employee termination procedures, or other specific issues
            - **Regulatory Policies**
                - Address mandatory standards and laws that affect the organization
            - **Advisory Policies**
                - Provide guidance for acceptable activities
            - **Informative Policies**

  - Focus on a certain topic and are designed to be educational in nature
  - Standards are used to implement a policy in an organization
    - **Baselines**
      - Created as reference points that are documented for use as a method of comparison during an analysis conducted in the future
    - **Guidelines**
      - It is flexible in nature, allowing exceptions and allowances when a unique situation occurs
    - **Procedures**
      - Detailed step-by-step instructions that are created to ensure personnel can perform a given action

- **Regulations**
  - **Health Insurance Portability and Accountability Act (HIPAA)**
    - Affects healthcare providers, facilities, insurance companies, and medical data clearing houses
  - **Health Care and Education Reconciliation Act of 2010**
    - Affects both healthcare and educational organizations by increasing some of the security measures to further protect healthcare information
  - **Sarbanes-Oxley (SOX)**
    - Publicly traded U.S. corporation are affected by this regulation and must follow certain accounting methods and financial reporting
  - **Gramm-Leach-Bliley Act of 1999 (GLBA)**
    - Affects the security of personal identifiable information, prohibits sharing financial information with any third-parties, and provides guidelines for securing that financial information
  - **Federal Information Security Management Act of 2002 (FISMA)**
    - Affects federal agencies and require them to develop, document, and implement an agency-wide information systems security program
  - **Federal Privacy Act of 1974**

        - Affects any U.S. government computer system that collects, stores, uses, or disseminates personally identifiable information
        - Federal Privacy Act only places requirements directly upon federal government agencies, it does not apply to private corporations
    - **Family Educational Rights and Privacy Act (FERPA)**
        - A federal law that protects the privacy of student education records
    - **Computer Fraud and Abuse Act of 1986**
        - Defines hacking of what is referred to as "protected computers" which includes computers that hold financial records or government information
    - **Economic Espionage Act of 1996**
        - Affects organizations with trade secrets and anyone who tries to use encryption for criminal activities
    - **Children's Online Privacy Protection Act (COPPA)**
        - Imposes certain requirements on websites owners and online services that are directed to children under 13 years of age
        - **COPPA** can put a ton of extra requirements on companies trying to serve younger markets with educational content
    - **Personal Information Protection and Electronic Documents Act (PIPEDA)**
        - It requires organizations to obtain consent when they collect, use, or disclose personal identifiable information and to have clear, understandable, and readily available policies for their customers to read
    - **General Data Protection Regulation (GDPR)**
        - It states that personal data cannot be collected, processed or retained without the individual's informed consent
        - GDPR provides a provision in the law to ensure a user has the right to withdraw their consent at any time

- **Standards**
    - **Payment Card Industry Data Security Standard (PCI DSS)**
        - An agreement that any organization that collects, stores, or processes credit card customer information must abide by
            - **International Organization for Standardization (ISO)**
                - A group of standards created as a series of best practices across multiple industries
            - **Capability Maturity Model Integration (CMMI)**

    - A standard model that focuses on processes and behaviors used during the development of software, products, and services within an organization
    - CMMI categorizes an organization within a certain Maturity Level from 1 to 5
  - **National Institute of Standards and Technology (NIST)**
    - Supplies industry, academia, government, and other users with over 1300 different standards that can be used
    - NIST also have a Cybersecurity Framework called the CSF
  - **Common Criteria (CC)**
    - A set of standards in which computer system users can specify their security functional and assurance requirements in a given system
  - **Cloud Security Alliance's Security Trust Assurance and Risk (CSA STAR)**
    - A publicly accessible registry that documents the security and privacy controls provided by popular cloud computing offerings

- **Contracts and Agreements**
  - **Service-Level Agreement (SLA)**
    - This agreement is concerned with the ability to support and respond to problems within a given timeframe while providing the agreed upon level of service to the user
  - **Operational Level Agreement (OLA)**
    - An internal agreement that provides the details of the relationships involved between different departments of an organization as they support the business functions
  - **Master Service Agreement (MSA)**
    - This is an agreement for future agreements, allowing the organizations involved to negotiate future contracts much more quickly since they can reference the Master Service Agreement
  - **Non-Disclosure Agreement (NDA)**
    - Signed between two parties and define what data is considered confidential and cannot be shared outside of the relationship

        - Penalties for breaking the NDA may include fines, forfeiture of their intellectual rights to the property, or even jail time in extreme circumstances
    - **Memorandum of Understanding (MOU)**
        - A non-binding agreement between two or more organizations to detail an intended common line of action
    - **Interoperability Agreements**
        - Binding agreements and are used during normal operations
    - **Reciprocal Agreements**
        - Non-binding and generally only used during disaster recovery scenarios
    - **Interconnection Security Agreement (ISA)**
        - An agreement for the owners and operators of the IT systems to document what technical requirements each organization must meet
    - **Business Partnership Agreement (BPA)**
        - Conducted between two business partners and establishes the conditions of their relationship
    - **Privacy-Level Agreement**
        - Address what personally identifiable information can be shared, with whom can it be shared, how it is transmitted and exchanged securely and confidentially, and how the owner of the information can opt out of the collection and use methods if they desire
            - **Examples of PII**
                - Person's Full Name
                - Driver's License Number
                - Social Security Number
                - Date of Birth
                - Place of Birth
                - Digital Versions of a Person's Biometric Features
                - Financial Account Numbers
                - Addresses
                - Email Addresses
                - Social Media Names

- **Legal Considerations**
    - **Due Diligence**
        - Defined as having investigated all reasonable measures to address a given risk

- **Due Care**
  - Defined as having taken all reasonable actions to prevent security issues or to mitigate a possible security breach
- **Export Control Regulations**
  - A federal law that prohibits the unlicensed export of certain commodities or information for reasons of national security or protections of trade
    - Oral
    - Written
    - Electronic
    - Visual Disclosure
    - Shipment
    - Transfer
    - Transmission of commodities
    - Technology
    - Information
    - Technical data
    - Assistance
    - Software codes
- **Legal Hold**
  - A process that an organization uses to preserve all forms of potentially relevant information when litigation is pending or reasonably anticipated
  - Data must be kept until the legal actions are completed
- **Electronic Discovery (e-discovery)**
  - Refers to discovery in legal proceedings such as litigation, government investigations, or Freedom of Information Act requests in electronic format
  - Electronic information has an intangible form, volume, transience and persistence
  - Electronic information is usually accompanied by metadata
- **Attestation**
  - Means that you are stating you have met the requirements and are compliant
    - **Third-party Attestation of Compliance**
      - Means that another organization came in and did an independent audit of your organization to validate you meet the requirements

- **Integrating Industries**
  - Every organization has its own rules for how it conducts the information technology portion
  - of its business
  - Rules are directive and specific in nature
  - Policies are easier to standardize because they are more generic and don't usually provide specific solutions or methods
  - Some technologies are not allowed to be exported to certain areas of the world due to their encryption strength
  - There are legal and regulatory differences between different countries and geographic regions

Business Continuity

Objectives 4.4

- OBJ 4.4: Explain the important of business continuity and disaster recovery concepts

- **Business Continuity Plan**
  - **Business Continuity Plan (BCP)**
    - Refers to the plans and processes used during your response to a disruptive event
  - **Disaster Recovery Plan (DRP)**
    - Refers specifically to the plans and processes used during a disaster
    - BCP is a plan used for any disruptive event or in response to any type of threat
    - The development of the business continuity plan is the responsibility of senior managers within the organization
    - This committee works to determine the recovery priorities for the different types of events that may occur
    - They must determine the level of risk that they are willing to accept based on the organization's risk appetite and risk toleranc
      - **7 Major Steps to Perform in BCP**
        1. Develop a policy for contingency planning
        2. Conduct a business impact analysis
        3. Identify the preventative controls
        4. Create recovery strategies
        5. Develop the business continuity plan (BCP)
        6. Test, train, and exercise the BCP
        7. Maintain the BCP
      - **Hot Site**
        - Defined as a site that is up and running continuously
      - **Warm Site**
        - It is not fully equipped like a hot site
        - A hot site comes with a high price tag, a warm site is cheaper
      - **Cold Site**
        - Add more time to the recovery but it is even cheaper than a warm site
      - **Mobile Site**

- Uses independent and portable units to provide the recovery
- You can't just think of the technology stack, but also where are your people going to work and how will you support them long term

- **Business Impact Analysis**
  - **Business Impact Analysis (BIA)**
    - A functional analysis that is conducted as part of the development of the business continuity and disaster recovery plan
    - BIA is a management-level analysis performed to identify the impact of losing organizational resources
  - **Mission Essential Functions (MEFs)**
    - Limited set of functions that must be continued throughout, or resume rapidly after, a disruption of normal operations
    - **Four Steps in Business Impact Analysis**
      1. Identify the crucial processes and resources in the organization
      2. Identify the impacts of an outage and estimate the downtime for crucial processes
         - Critical
         - Urgent
         - Important
         - Normal
      - **Nonessential**
        - Critical resources should be restored within minutes or at most 1 hour, while urgent ones may stay down for up to 24 hours
        - If everything is considered your number one priority for service restoration, then nothing is really the priority
      - **Maximum Tolerable Downtime (MTD)**
        - The most amount of time that the business can tolerate the asset or component being down
        - Sometimes called the Maximum Period of Time Disruption (MPTD) or Maximum Tolerable Outage (MTO)

        - To calculate the MTD you would add the Recovery Time Objective (RTO) and the Work Recovery Time (WRT) together
    - **The Recovery Time Objective (RTO)**
        - The shortest period of time in which an asset or component should be fixed to prevent any negative consequences to the business
    - **The Work Recovery Time (WRT)**
        - This metric tells us how much time was left over after our Recovery Time Objective but before any negative effects are experienced
    - **Mean Time to Repair (MTTR)**
        - This is the average amount of time that is would take to repair an asset or component when a disaster or disruption occurs
    - **Mean Time Between Failures (MTBF)**
        - The average amount of time an asset or component will operate before failing
    - **Recovery Point Objective (RPO)**
        - An established point in time that the disrupted asset or component should be returned to normal function
    - **Recovery Service Level (RSL)**
        - A metric that is displayed as a percentage of how much computing power will be needed during a disaster
3. Identify your resource requirements
4. Identify the recovery priorities

- **Privacy Impact Assessment**
  - **Privacy Impact Assessment (PIA)**
    - A process of identifying and managing the privacy risks arising from new projects, initiatives, systems, processes, strategies, policies, business relationships, and other risk events
      - Seek to ensure conformance with applicable legal, regulatory, and policy requirements for privacy
      - Seek to identify and evaluate the risks of privacy breaches or other incidents and effects
      - Seek to identify appropriate privacy controls to mitigate unacceptable risks
    - **PIA** should be conducted if the organization possesses sensitive information, or if the security controls systems protecting private or sensitive information are undergoing changes
      - **Benefits of PIA to the Organization**
        - Provides a warning system to detect privacy problems and build safeguards
        - Provides evidence of privacy risk
        - prevention attempts
        - Helps improve informed decision-making by senior leaders
        - Helps the organization gain public trust
        - and confidence
        - Demonstrates that the organization takes privacy seriously
          - Initiate the Project
          - Conduct a Data Flow Analysis
          - Conduct a Privacy Analysis
          - Publish a Privacy Impact Assessment Report

- **Incident Response Plan**
  - **Six Steps of Incident Response**
    - Detection
    - Response
    - Report
    - Recover
    - Remediate
    - Review

- **After-action Report (AAR)**
  - Provide insight into the specific incident and how to improve response processes in the future
  - Meetings and interviews are conducted with those who were involved in the incident response
- **Event**
  - A positive or negative change in the state of security or operations
- **Incident**
  - A negative event that impacts an organization's security or operations
    - **Cyber Security Incident Response Team (CSIRT)**
      - Made up of a manager, cyber security personnel, a representative from the legal counsel, and possibly someone from public relations or human resources, depending on the type and severity of the incident
      - The single point of contact for security incidents within your organization
    - **Microsoft Incident Response Team (MIRT)**
- **Rules of Engagement**
  - Gives authority and scope to conduct the investigation
- **Incident Response Manager**
  - Oversee and prioritize actions during the detection, analysis, and containment of an incident
- **Security Analyst**
  - Play detective on the affected network in order to determine what happened
- **Triage Analyst**
  - Helps filter out false positives by configuring intrusion detection and protection systems, as well as performing ongoing monitoring and analysis
- **Forensic Analyst**
  - Recovers key artifacts and evidence from the network and use them to build a timeline of the different events to understand what happened
- **Threat Researchers**
  - Provide threat intelligence and overall context during your incident response
  - It is important to plan not just for the technical response, but the business and public relations response as well

- **Testing Plans**
  - **Checklist**
    - A list of items that are required, a list of things to be done, or a list of points to be considered
  - **Walkthrough**
    - Used as a basic training event for team members
  - **Tabletop Exercise**
    - A discussion-based session where team members discuss their roles and what they would do in response to a given scenario
  - **Full Interruption Test**
    - Shuts down operations at the primary site and shift operations to the recovery or backup site
    - Full interruption tests are great, but they are expensive
  - **Parallel Test**
    - Uses recovery systems that are built and tested to see if they can perform actual business transactions to support key processes
  - **Simulation Test**
    - Puts groups of team members together to go through a simulated disaster or incident response to identify whether emergency response plans are good enough to work

Risk Strategies

Objectives 4.1 and 4.4

- OBJ 4.1: Given a set of requirements, apply the appropriate risk strategies
- OBJ 4.4: Explain the important of business continuity and disaster recovery concepts

- **Risk Management Processes**
  - Identify the assets and their value
  - Identify threats
  - Identify vulnerabilities
  - Determine likelihood
  - Identify impact
  - Determine risk as a combination of likelihood and impact

- **Asset Value**
  - Assets can be both tangible and intangible
    - **Tangible**
      - Computers
      - Servers
      - Facilities
      - Supplies
      - Personnel
    - **Intangible**
      - Intellectual Property
      - Data
      - Organization's Reputation
  - The value the asset has to the owner
  - The work required to develop or obtain that asset
  - The damage that would result if the asset were lost
  - The cost to maintain the asset
  - The cost that a competitor would pay for that asset
  - The penalties that might result if that asset were lost
  - **Human**
    - Refers to both non-malicious and malicious insiders and outsiders, spies, adversaries, terrorists, and others
  - **Natural**

        - Phenomena like floods, fires, tornados, earthquakes, hurricanes, and other types of natural phenomenon
    - **Technical**
        - Failures of hardware or software, malicious code such as viruses, trojans, worms, and other technology used inflict harm
    - **Physical**
        - Failure of any of our physical security measures, like our gates, fences, closed circuit TVs, mantraps, and more
    - **Environmental**
        - Refers specifically to failures of power, heating and cooling systems, and other similar problems
    - **Operational**
        - Any process or procedure that might affect one of the three tenets of information security

- **Access Control**
    - **7 Different Categories of Access Control**
        - **Compensative**
            - Used in place of a primary access control measure in order to mitigate a given risk
        - **Corrective**
            - Used to reduce the effect of an undesirable event or attack
        - **Detective**
            - Used to detect an attack while it is occurring and to notify the proper personnel
        - **Deterrent**
            - Used to discourage any violation of the security policies, both to attackers and insiders
        - **Directive**
            - Used to force compliance with the security policy and practices within the organization
        - **Preventive**
            - Seeks to prevent or stop an attack from even occurring
        - **Recovery**
            - Used to recover a device after an attack
    - **Administrative**

        - Manages personnel and assets through security policies, standards, procedures, guidelines, and baselines
            - **Logical**
                - Implemented through hardware or software and used to prevent or restrict access to a system
            - **Auditing**
                - A one-time evaluation of a security posture
            - **Monitoring**
                - An ongoing process that evaluates the system or its users
            - **Change Management**
                - A baseline is created and all changes to that baseline are tracked and assessed
                - Organizations should automate the process as much as is practical
    - **Physical**
        - Includes installing new devices like firewalls, IDS, IPS, authentication schemes, encryption, auditing or monitoring software, and more

- **Aggregating Risk**
    - **CIA Scoring in FIPS 199**
        - Low
        - Moderate
        - High
    - If a system is made up of multiple assets, then it needs an aggregate CIA score
        - SCwebsite = {(confidentiality, low), (integrity, moderate), (availability, high)}
        - SCdatabase = {(confidentiality, high), (integrity, moderate), (availability, high)}
        - SCaccounting = {(confidentiality, high),(integrity, high), (availability, low)}
    - SCsystem = {(confidentiality, high), (integrity, high), (availability, high)}
    - SCwebsite = {(confidentiality, low), (integrity, moderate), (availability, high)}
    - SCdatabase = {(confidentiality, high), (integrity, moderate), (availability, high)}
    - SCaccounting = {(confidentiality, high), (integrity, high), (availability, low)}

- **Scenario Planning**
    - **Internal Actors**
        - Employee threats, such as disgruntled, untrained, or uncaring employee

- **External Actors**
  - Competitors, hackers, activists, vandals, terrorists, nation state cyber attackers, data miners, criminals, and others
    - **Skill Level**
      - Refers to the competency of the threat actor
    - **Resources**
      - The threat exists as an individual, team, organization, or even a nation state or government
    - **Limits**
      - Refers to how the threat operates
    - **Visibility**
      - Refers to whether the threat actor cares if they get caught
    - **Objective**
      - Refers to what end state the threat actor is trying to accomplish
    - **Outcome**
      - Refers what they are achieving through their attack on our organization
- **Steps to Conducting Plans**
  - Analyze all of the threats that the organization faces
  - Determine what the organization wants to protect from those threats
  - Develop a scenario incorporating those threats and assets
  - Develop an attack tree for each scenario
  - Determine the security controls used to protect the assets from the identified threats

- **Security Controls**
  - Security control reviews should be conducted annually
    - What security controls are in use?
    - How can we improve these controls?
    - Are these controls needed?
    - Has the architecture changed?
    - Have any new problems been identified through trend analysis?
    - What security controls can be added to solve these issues?
  - **Gap Analysis**
    - Compares the current performance of the organization's security posture to the desired security posture

- **Baseline**
  - Used as a reference point to compare against a future metric
  - Longer duration of time
  - A baseline establishes what is considered normal
- **Benchmark**
  - Captures the same information as a baseline but at a different point in time
  - Single point in time

- These metrics should be captured at similar times
  - **Metrics** provide a quantitative look at risk and performance in the network

- **Chief Security Officer (CSO)**
  - Works with experts within the organization to determine the security costs necessary for the organizational information systems
    - **Short-term**
      - Current daily workload
    - **Long-term**
      - Future security budgets
- **Key Performance Indicator (KPI)**
  - Provides actionable information that helps manage an IT service, process, or activity
  - Increase security by identifying activity patterns

- **Security Solutions**
  - Testing in live environments should be done in stages and during low periods of activity
  - "How would an attacker break into my network?"
    - **Performance**
      - A technology's ability to fulfill its intended purpose or the efficiency with which it fulfills it
    - **Latency**
      - The delay that occurs during data processing on a network
    - **Scalability**
      - A technology's ability to perform under an increased or expanding use case
        - Load balancing

    - Clustered servers
    - Cloud architectures
- **Capability**
    - A technology's ability to perform a solution
- **Usability**
    - The ease-of-use of a security solution or how closely the solution matches the requirements
- **Maintainability**
    - The measure of how often the solution must be updated, upgraded, or fixed
- **Availability**
    - The amount of time that a system is available for use and is often measured as a percentage
- **Recoverability**
    - The probability that a failed solution can be restored to normal operations within a given time period

Vendor Risk

Objectives 4.2

- OBJ 4.2: Explain the importance of managing and mitigating vendor risk

    - New technologies are mostly brought by third-party vendors
        1. User behavior monitoring
        2. Ongoing and continual training and security policy updates
        3. Forward-thinking mindset during technology adoption

- **Business Models**
    - **Risk Profile**
        - An organization's willingness to take and accept various types of risk
            - **Partnership**
                - Establishes a requirement for the information and data exchange between two organizations
                    - **Third-Party Connection Agreement (TCA)**
                        - Dictates the security controls that should be taken to protect the data being exchanged between two partners
            - **Outsourcing**
                - Occurs whenever a business function or process is provided by a third-party outside of the organization
                - Outsourcing companies sometimes outsource to other companies
            - **Downstream Liability**
                - Occurs when a partner or outsource provider fails to fulfill the organizational requirement
                    - **Due Diligence**
                        - Investigating all reasonable measures to address a given risk
                        - Gathering information
                    - **Due Care**
                        - Taking all reasonable actions to prevent security issues or mitigate a possible security breach
                        - Taking action

- The **cloud** is NOT always the right answer for an organization
- We are still responsible for the security of our data in the outsourcing business model
    - **Hybrid Cloud**
        - Combines private and public infrastructures
    - **Community Cloud**
        - Shares resources across multiple organizations that share the same needs
        - It is challenging to support different types of hardware, software, and peripherals
            - Due diligence
            - Penetration test
            - ISA
            - Risk analysis
- **Divestiture/Demerger**
    - Occurs when a part of a company is "spun off" to form its own company
        1. Define a plan to set and measure the security controls along the way
        2. Identify gaps or overlaps in security between the two networks
        3. Create a risk profile for risks in moving the data
        4. Prioritize process refinement based on our findings
        5. Ensure auditing and compliance personnel use the same framework

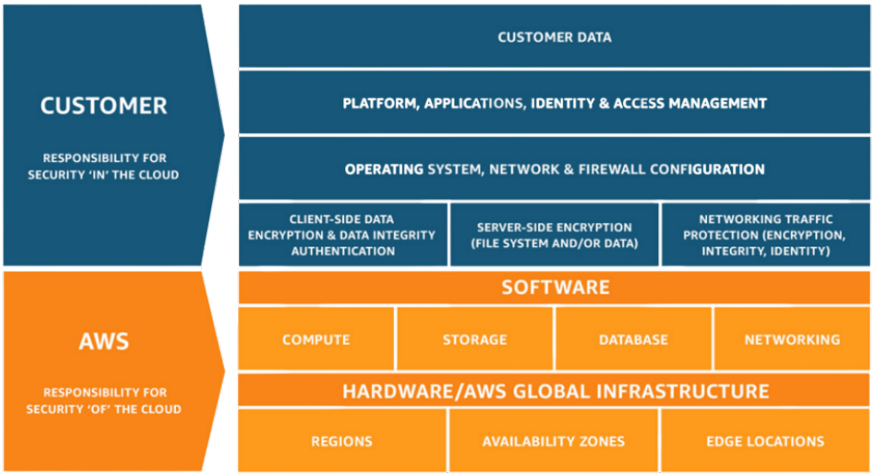
- Influences
    - Competitors
    - Auditors and audit findings
    - Regulators
    - Client requirements
    - Top-level management
    - De-perimeterization
    - Conduct internal audits at least on a quarterly basis and external audits at least annually
        - Onsite assessment
        - Document exchange

        - Process/policy review
    - **Internal Clients**
        - An organization's own employees who use the company's information systems for their jobs
            - Telecommuting
            - Mobile devices
            - BYOD policies
            - Cloud computing
            - Outsourcing
    - **De-Perimeterization**
        - Constant change in the boundary of a network
        - Think through how employee devices can be supported, protected, and managed on a large scale

- **Organizational Changes**
    - **Internal Environment**
        - The culture within an organization
    - **External Environment**
        - Rest of the industry, including peers and competitors
        - It is important to review security policies often and regularly
            - International Organization for Standardization (ISO)
            - International Electrotechnical Commission (IEC)
            - ISO/IEC 27000 series
    - **Risk Assessment/Risk Analysis (RA)**
        - Determines a qualitative or quantitative estimate of risk related to a well-defined situation and a recognized threat
            1. Identify the assets and their value
            2. Identify the vulnerabilities and threats
            3. Calculate the probability of the threat being realized and its impact to the business
            4. Balance threat impact with the cost of mitigating against it with appropriate countermeasures
    - **Statement of Applicability (SOA)**
        - Identifies the controls selected and explains why those controls are considered appropriate based on the output of the risk assessment
    - **Process**
        - A collection of activities that work together for a specific outcome or goal

- **Procedure**
  - Step-by-step lists of how the policy, standards, and guidelines are carried out daily in the workplace
    - Business
    - Technology
    - Environment
    - Regulations
    - Emerging risks
  - Policies should be developed prior to developing processes and procedures

- **Shared Responsibility Model**
  - A security framework that dictates the security obligations of a cloud computing provider and its clients to ensure accountability
    - **Inherited Controls**
      - Fully controlled and managed by the cloud service provider
    - **Shared Controls**
      - Applies to both the infrastructure layer and the customer layers
    - **Customer/Client Specific Controls**
      - Sole responsibility of the client



- **Viability and Support**
  - **Vendor Viability**
    - Ensures a selected vendor will be around for the long-term
  - **Source Code Escrow**
    - Deposits the source code of the software with a third-party escrow agent

        - Consider the vendor's inherent riskiness and their firm's tolerance for supplier-related risk
            - **Financial Risk**
                - Assessed through a simple analysis of the vendor's financial statements or the company's financials
            - **Strategic Risk**
                - Focuses on the strategic viability of the vendor being considered
    - **Vendor Lock-in**
        - Occurs when a client becomes dependent on a vendor's products or services and would need to pay substantial costs to switch
            - **Application Transfer Risk**
                - Ensure application being developed could be deployed in Azure, AWS, and Google Cloud
            - **Infrastructure Transfer Risk**
                - Ensure virtual machine formats are supported by multiple vendors
            - **Human Resource Knowledge Risk**
                - Develop human capital to be able to support multiple cloud offerings
    - **Vendor Lock-out**
        - Occurs when a client loses access to its data because the cloud provider has ceased operation

- **Dependencies**
    - **Codes**
        - Even if your code is written extremely well from a security standpoint, if the third-party dependencies have a security flaw in them, you just inherited that flaw into your own application, too
        - All code is subject to the same types of vulnerabilities
            - Cross-site scripting
            - Cross-site request forgery
            - Clickjacking
            - Injection flaws
    - **Hardware**
        - Somethings in your networks that are installed by a third-party vendor take the form of hardware

        - A vulnerability in a third-party dependency becomes a vulnerability in your application
    - **Modules**
        - These often have firmware that contains specific code to run those specific functions
    - Most organizations don't develop their own modules and hardware, but instead rely on vendors and suppliers to provide components we can connect to perform the functions we desire

- **Considerations**
    - Technical considerations
    - Client requirements
    - Support availability
    - Geographical considerations
    - Vendor assessment
    - Incident reporting requirements
    - **Technical Testing**
        - Conducting unit level, performance, robustness, and vulnerability testing
        - Add segmentation into the network to provide some added defenses
    - **Transmission Control**
        - Involves an electronic mechanism that collects data and processes signals within the network
            - Fiber
                - Additional costs
            - Copper
                - EM
            - Wireless
                - RFI, Eavesdropping
        - Another set of considerations:
            - Legal
            - Change management
            - Staff turnover
    - **Device configuration**
        - Create a formalized process and incident report form for your vendor to utilize

- **Supply Chain**

- Ensure the operation of every element are all consistent and tamper-resistant
- Properly resourced cybersecurity program
- Security assurance and risk management
- Security controls for confidential data
- Product support life cycle
- Incident response and forensics assistance
- General and historical Company information
- Due diligence should apply to all suppliers and contractors

    - **Trusted Foundry**
        - A microprocessor manufacturing utility that is part of a validated supply chain
    - **Source Authenticity**
        - Ensures hardware is procured tamper-free from trustworthy suppliers

Securing Networks

Objectives 1.1

- **OBJ 1.1**: Given a scenario, analyze the security requirements and objectives to ensure an appropriate, secure network architecture for a new or existing network

- **Switches**
  - **Switch**
    - Makes traffic switching decisions based on the MAC address of the sending and receiving devices through transparent bridging
    - A switch remembers devices and their switchports based on their MAC addresses
  - **Content Addressable Memory (CAM) Table**
    - Stores information about the MAC addresses available on any given port of the switch
  - **MAC Flood**
    - Causes a MAC address overflow to occur in the CAM table by flooding the switch with random MAC addresses
    - Enable port security or MAC filtering on the switchports
  - **Port Security**
    - Allows a network administrator to associate specific MAC addresses from devices to specific interfaces
  - **Persistent MAC Learning (Sticky MAC)**
    - Enables an interface to dynamically associate the first MAC address that it connected to as an authorized address
  - **Switching Loop**
    - Creates a flood of traffic across the network and causes switches to become non-responsive, creating a self-imposed denial of service attack
  - **ARP Poisoning/ARP Spoofing**
    - Sends malicious ARP packets to a default gateway on the network to change the IP and MAC address pairings in its ARP tabl
  - **Dynamic ARP Inspection (DAI)**
    - Intercepts all ARP requests and responses and compares each one to the MAC-IP bindings in a trusted table a Cisco switch has access to
  - **DHCP Snooping**
    - Prevents a poisoning attack on the DHCP database itself and increases efficiency of the Dynamic ARP Inspection capability

- **Switch Spoofing**
  - Exploits the Dynamic Trunking Protocol (DTP)
- **Double Tagging**
  - Adds two VLAN tags, an outer and inner tag, to the traffic going to the switch

- **Routers**
  - **Router**
    - Makes routing decisions using IP addresses
  - **ARP Broadcast**
    - Locates the correct host on the local network and passes the traffic to the host using its MAC address
    - It became easier to rely on dynamic routing protocols
    - Use a hash-based authentication key and a hash of the router information
  - **Access Control List (ACL)**
    - Configured on the router interfaces to control the flow of traffic into or out of a certain part of the network
      - Ensure authentication is used between routers during routing table updates
      - Router management should be conducted using strong authentication and complex passwords
      - Management connection to a router should always be performed over SSH
  - **6to4**
    - Provides the ability for IPv6 packets to be transmitted over a standard IPv4 network without the need to create explicit tunnels
  - **Teredo**
    - Provides full IPv6 connectivity for hosts even if they do not have a connection to a native IPv6 network
  - **Dual Stack**
    - Allows network administrators to configure their devices to support both IPv4 and IPv6 routing simultaneously
  - **Generic Routing Encapsulation (GRE) Tunnel**
    - Carries IPv6 packets across an IPv4 network by encapsulating them inside of GRE IPv4 packets

1. Larger address space
   IPv4 = 232
   4.2 billion addresses
   IPv6 = 2128
   IPv6 = 2128
   340 undecillion addresses
2. Increased security by incorporating IPSec into the protocol by default
3. Provides for the stateless autoconfiguration of devices on the network

- **Wireless and Mesh**
  - **Wireless Controller**
    - Acts as a centralized appliance or software package to monitor, manage, and control wireless access points
      - Channel assignment
      - Load balancing
      - Coverage gap detection
        - 802.1x
        - PEAP
        - LEAP
        - EAP-TLS
        - WPA2 802.11i
        - L2TP
  - **Mesh Network**
    - Network topology where each node cooperates to relay data in an effort to ensure that all nodes maintain connectivity to one another
      - AHCP
      - PAA
      - DWCP

- **Firewalls**
  - **Access Control List (ACL)**
    - Controls the flow of traffic into or out of a certain part of the network
    - Most specific rules should be placed at the top of the list, with more generic rules towards the bottom
    - It is a best practice to include a deny all rule at the end of an ACL

- It is important to log the actions taken by network infrastructure devices

- **Firewall**
  - Inspects and controls traffic trying to enter or leave a network's boundary
    - **Packet-Filtering Firewall**
      - Only inspects the header of the packet to determine if traffic is allowed or denied based on IP addresses and port numbers
    - **Stateful Firewall**
      - Tracks the state of all connections and requests going into and out of the network
    - **Proxy Firewall**
      - Placed between internal and external connections in the network and makes connections on behalf of the other endpoints
        - **Circuit-level**
          - Operates at Layer 5
        - **Application-level**
          - Operates at Layer 7
    - **Kernel Proxy or Fifth Generation Firewall**
      - Has minimal impact to performance that it has on the network, even while still conducting a full inspection of the packet at every layer
        - **Next Generation Firewall (NGFW)**
          - Creates firewalls that are application-aware
          - NGFW can integrate with several other security products
        - **Unified Threat Management (UTM)**
          - Provides the ability to conduct numerous security functions within a single device or network appliance

Advantages	Disadvantages
Lower upfront cost, maintenance, and power consumption	Single point of failure
Easier to install and configure	Lacks detail provided by a specialized tool
Can be fully integrated	Less efficient than single function devices

        - Consider using NGFW for faster network speed and better efficiency
        - Place UTM devices between the LAN and the Internet
    - **Web Application Firewall (WAF)**
        - Utilizes specific rule sets to prevent common attacks against web applications, such as cross-site scripting and SQL injections

- **Proxies**
    - **Proxy Server**
        - Creates a network connection between an end user's client machine and a remote resource, such as a web server
            - Increased network speed and efficiency
            - Increased security
            - Additional auditing capabilities
        - **Forward/transparent proxy (Outbound traffic)**
            - is usually positioned at the edge of your corporate network and regulates the outbound traffic according to specific policies your organization has created
        - **Reverse proxy (Inbound traffic)**
            - content caching, traffic scrubbing, IP masking, and load balancing

- **Gateways**

- **NAT gateways**
  - Gives endpoints without public IP addresses access to the internet without exposing those resources to incoming internet connections.
- **Internet gateways**
  - Allows inbound connections to be initiated from the internet and relays or prosies them to internal resources.
- **Application Programming Interface (API) gateway**
  - Acts as a reverse proxy to accept all API calls and aggregates the required services to fulfill such requests.
- **Extensible Markup Language (XML) gateway**
  - Provides filtering and access controls that focus on XML-formatted inbound data to an API.

- **IDS and IPS**
  - **IDS**
    - **Logs and alerts**
    - **Network-based**
      - Network IDS (NIDS) Monitors the traffic coming in and out of a network.
    - **Host-based**
      - Host -Based IDS (HIDS) Looks at suspicious network traffic going to or from a single or endpoint.
    - **Wireless**
      - **Wireless IDS (WIDS)**
        - Detects attempts to cause a denial of a service on a wireless network.
      - **Signature-based**
        - Analyzes traffic based on defined signatures and can only recognize attacks based on previously identified attacks in its database
          - Pattern-matching
            - Specific pattern of steps
            - NIDS, WIDS
          - Stateful-matching
            - Known system baseline
            - HIDS
      - **Anomaly-based**

- Analyzes traffic and compares it to a normal baseline of traffic to determine whether a threat is occurring
- Five steps: statistical, protocol, traffic, rule/heuristic, application-based.

- **IPS**
  - Logs, alerts, takes action.
  - Scans traffic to look for malicious activity and takes action to stop it.

- **Network Access Control (NAC)**
  - Keeps unauthorized users or devices from accessing a private network.
    - **Persistent**
      - A piece of software installed on a device requesting access to the network
    - **Agentless NAC Volatile Agent**
      - Installs the scanning engine on the domain controller instead of the end
      - point device

- **Remote Access**
  - To do this, we can provide Virtual Private Networks and connections using Secure Shell, the Remote Desktop Protocol, or the Virtual Network Computing Protocol.
    - Serial Line Internet (SLIP)
    - Point-to-Point (PPP)
    - TACACS+ OR RADIUS
  - **Virtual Private Network**
    - Allows users to create an encrypted tunnel over an untrusted network and remotely connect back into an enterprise network
      - VPN tunnels can be encrypted using the Advanced Encryption System (AES)
      - VPN can be used in combination with NAC solution
  - **Secure Shell (SSH)**
    - Remotely accesses and configures servers and network devices over a text-based command line interface.
  - **Remote Desktop Protocol (RDP)**
    - Provides a graphical interface to connect to another computer over a network connection.

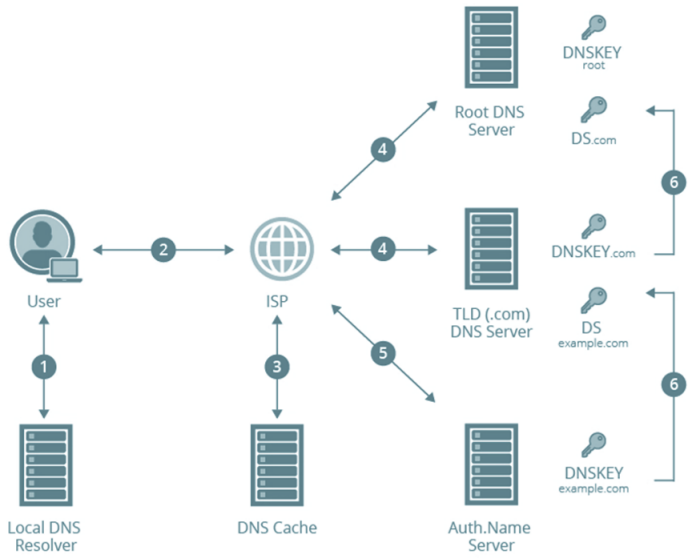
- **Virtual Network Computing (VNC)**
  - Similar to RDP but fully cross-platform and open-source.
  - should only be used in our internal networks
    - VNC server
    - VNC client
    - VNC protocol

- **Unified Communications**
  - Integrates multiple communication technologies that perform multiple functions into an enterprise network
  - **Presence**
    - Extensible messaging and presence protocol
    - Public key infrastructure
  - **Instant messaging**
  - **Email**
    - Inbound
      - IMAP
        - Port 143
        - Port 993
      - POP3
        - Port 110
        - Port 995
    - Outbound
      - SMTP
        - Port 25
        - Port 456
    - Sender Policy Framework (SPF)
      - Phishing
        - Large target audience
    - Spearphishing
      - Focused target audience
    - Whaling
      - High-level executives
  - **Phone**
    - Private Branch Exchange (PBX)
      - Prevents eavesdropping
      - Minimizes service theft and toll fraud

        - Minimizes DoS threats
    - Voice over IP (VoIP)
        - Lowe cost per minute
        - Combines voice and data
        - Session Initiation Protocol (SIP)
        - Real-time Transport Protocol (RTP)
        - Span over Internet Telephony (SPIT)
            - Creates unsolicited recorded phone calls to be sent over voice systems
        - Secure Real-time Transport Protocol (SRTP)
- **Conferencing**
    - Conference recording
    - Information disclosure
    - Unauthorized attendees
    - Data security
    - Video-teleconference system (VTC)
- **Storage Collaboration**
    - SharePoint
    - Web-based technologies

- **Cloud vs On-premise**
    - Charge by usage
    - No upfront costs
    - Constant updates
    - Increase efficiency
    - Data loss prevention (DLP)
    - Database activity monitoring (DAM)
    - Malware
        - Prevent malware by using a break and inspect system
    - Information disclosure
        - Prevent information disclosure by having a social media policy

- **DNSSEC**
    - Domain name system (DNS) helps network clients find a website using human-readable hostnames instead of numeric IP addresses
    - **Prevents cache poisoning**



- **Load Balancer**
  - Also known as content switch distributes incoming requests across a number of servers inside a server farm or cloud infrastructure.
  - **DoS**
    - Single attack
  - **DDoS**
    - Multiple attackers
  - **Blackholing/sinkholing**
    - identifies any attacking IP addresses and routes all their traffic to a non-existent server through the null interface, effectively stopping the attack
  - **IPS**
    - can also be used to identify and respond to a Denial of Service attack as well.
  - **Elastic cloud**
  - **Remote triggered black hole**
    - **Internal border gateway protocol (iBGP)**
      - Forwards route advertisements received from the external BGP router throughout the internal network.

Securing Architectures

Objectives 1.1

- **OBJ 1.1**: Given a scenario, analyze the security requirements and objectives to ensure an appropriate, secure network architecture for a new or existing network

- **Traffic Mirroring**
  - Enables monitoring of network traffic passing in or out of a network
  - **SPAN or mirrored port**
    - Configures the router or switch to make a copy of every packet that the device processes.
      - **Local traffic mirroring**
        - connects a monitoring device to a local port and receives a copy of every piece of traffic going into or out of the network device.
      - **Remote traffic mirroring**
        - Creates a GRE tunnel over an IP network to connect the network analyzer to the network device.
      - **ACL-based traffic mirroring**
        - Monitors the traffic based on the configuration of the interface's ACL .
      - **Virtual private cloud (VPC)**
        - Copes all inbound and outbound traffic to the network interfaces attached to cloud-based servers.
      - **Network tap**
        - is a physical hardware device that connects to your network

- **Network Sensors**
  - **SIEM systems**
    - Consolidates log files from various systems, servers, and devices into a centralized.
      - Syslog
      - Security Information Management (SIM)
      - Security Event Management (SEM)
        - Application logs
        - Antivirus logs

- Operating systems logs
- Malware detection logs
- Router logs
- Firewall logs
- NetFlow logs
- File integrity monitoring

- **SNMP traps**
  - Simple Network Management Protocol and sends its data over port 161 by default.
  - SNMP is an application layer protocol that is used widely in network monitoring. The latest and most secure version is SNMP v3
    - Visibility
    - Correlation
    - Compliance reporting
    - Prioritization
  - **Managed Device**
    - A device like a router, switch, firewall, printer or workstation
  - **Agent (SNMP Software)**
    - Collects, stores, and signals the presence of data on a device.
  - **Network Management Station (SNMP Manager)**
    - Provides the memory and processing functions between the devices and the agents
  - **Network Intrusion Detection/Prevention System (NIDS/NIPS)**
    - Monitors network traffic, reports on that traffic, and blocks or reacts to suspicious and malicious traffic.
    - Signature-based
      - Attack patterns
    - Anomaly-based
      - Normalized baseline
    - Stateful Protocol
      - Traffic deviations
  - **Break and Inspect (TLS/SSL Inspection)**
    - Allows organizations to use their proxy server as a form of man-in-the-middle
  - **Audit Log**
    - Provides the digital evidence when investigating anomalous issues on a network

- **Network Flow (NetFlow)**
  - A single session of information that shares certain characteristics between two devices

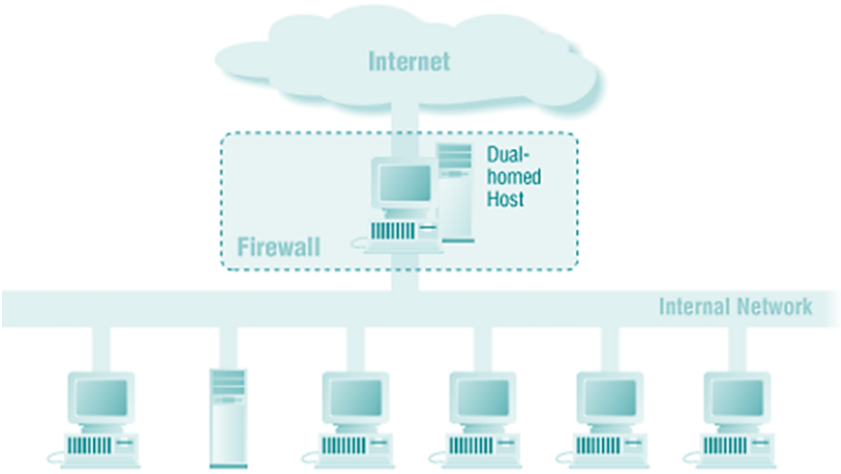
- **Host Sensors**
  - **File integrity monitoring**
    - A host-based intrusion detection system that creates a hash digest for every monitored file
    - Required for PCI-DDS, SOX, FISMA, HIPAA and CIS controls
  - **Antimalware**
    - Detects and stops adware, spyware, viruses, worms, and other destructive types of software
      - Update software
      - Scan regularly
      - Prevent autorun
    - Forward logs into the SIEM for correlation and analysis
  - **Data Loss Prevention (DLP) Endpoint Software**
    - Monitors and prevents data leakage
    - Network DLP installed at your network boundary and analyzes all your the traffic that is leaving your network
    - Endpoint DLP agents installed on a server or workstation within your organization and only protects data on that particular asset
  - **Precise methods**
    - Involve registering all the content considered sensitive
  - **Imprecise method**
    - Rely on keywords, regular expressions, metadata tags, Baysian analysis and statistical analysis to guess what files should be protected under the DLP program

- **Layer 2 Segmentation**
  - **VLANS**
    - Reduce the background traffic and allows the network to grow while still providing different security protections to different parts of the network
  - **ACLs**
    - Control which inbound and outbound traffic is allowed
  - **Management VLAN**
    - Passes inter-switch traffic which provides a layer of security

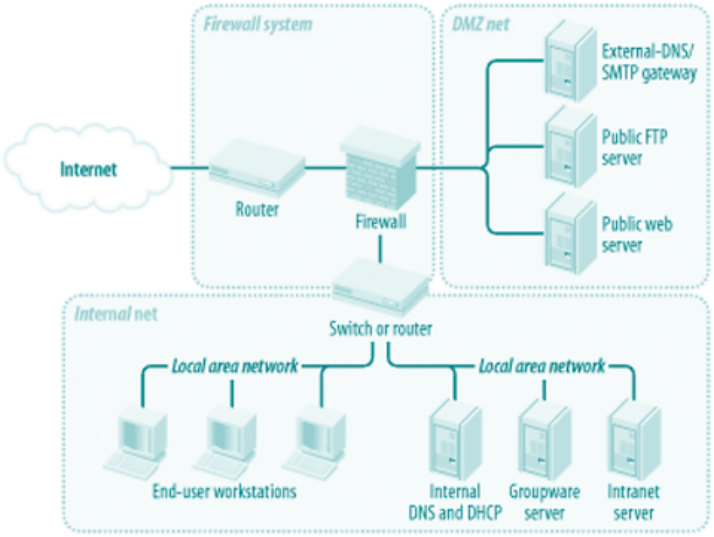
        - Out of band (OOB)
            - Connects to a separate and isolated network not accessible from the internet or the ret of the LAN
        - **Data interface**
            - Provides necessary network services to end users
            - Router
                - ACL, operates in layer three by filtering out IP addresses
            - Switch
                - Port security, operates at layer two by filtering out

- **Network Segmentation**
    - **Demilitarized Zone (DMZ)**
        - Provides controlled access to publicly available servers hosted within the organization's network
        - **Extranet**
            - A specialized type of DMZ that is created for partner organizations to access over a wide area network
    - **Server techniques**
        - **Boundary control**
            - Places devices at the boundaries of the security zone to controls the ingress and egress of data
        - **Access control**
            - Controls access to sensitive materials
        - **Integrity**
            - Ensures data is not changed, damaged, or corrupted during the transfer
        - **Cryptography**
            - Maintains the confidentiality of data
        - **Auditing and monitoring services**
            - Tracks all the activities of a user or system in the network
    - **Bastion Host**
        - Any device directly exposed to the internet or another untrusted network which may or may not be a firewall
        - **Firewall**
            - Most firewalls have at least two interfaces
            - **Dual-home firewall**

- One interface is connected to the internal or trusted network, while the other interface is connected to the internal or trusted network
- This configuration only requires a single firewall device using the appropriate Access Control Lists.



- Multi-homed firewall architecture is similar to a dual-homed architecture except it uses more than two interfaces



- **Jump Box**
  - Hardened server that provides access to other hosts in the DMZ
  - Physical machine
  - Virtual machine
- **Air Gap**
  - A type of network isolation that physically separates a network from all other networks

- **Server Segmentation**
  - **Group Policies and Security Groups**
    - Enforce the standard operating environments in a Windows domain
  - **Group Policy Management Console (GPMC)**
    - Allows the granular control to allow or disallow inheritance of a policy from one group or container to another
  - **Microsegmentation**
    - Creates zones in data center and cloud environments to isolate workloads from one another and secure them individually
  - **Data Zone**
    - A representation of data with a shared purpose, need and user
      - Financial data
        - PCI-DSS
      - Student data
        - GDPR
      - Proprietary software data
        - No requirement
  - **Region-based Segmentation**
    - Most cloud service providers give you the ability to dictate where your data will be stored based on different geographical regions
  - **Availability Zone**
    - Isolated location within data center regions where public cloud services originate and operate
  - **VPC/VNET**
    - deploys private networks in the cloud or extends on-premise network into the cloud
  - **Network Access Controls (NACLs)**
    - Stateless filtering rules applied at the subnet level and apply to every resource deployed to the subnet within the VPC or VNE

- **Production**
  - Intended audience
- **Staging**
  - Development team
- **Guest**
  - Visitors with limited access
- **Peer-to-Peer Segmentation**
  - Allows direct connection between two devices

- **Zero Trust**
  - Prevents data breaches by eliminating the concept of trust from an organization's network architecture
  - **Deperimeterization**
    - The removal of a boundary between an organization and the outside world
    - Has occurred due to the migration to the cloud, the increase in remote work, the embracing of the mobile technologies, the use of wireless networks, and a move to outsourcing and contracting

- **Merging Networks**
  - **Peering**
    - Interconnection of two separate networks to exchange traffic between users of each network
  - **Cloud to on-premise connections**
    - Supports large amounts of data integration and easy management
      - Involves adding API gateway as a reverse proxy
  - **Data sensitivity levels**
    - Major concern to think about when merging two networks, what level of data is being processed on each network and are there any regulatory issues with merging these networks.
    - Involves adding an API gateway as a reverse proxy
  - **Cross-domain connections**
    - Method in place for users to authenticate and use trainings resources
    - **Federation of identity or FIdM**
      - Describes the technologies standards and use cases that server to enable the portability of identity information across otherwise autonomous security domains

        - **Directory Services**
            - Creates a trust relationship between networks and their AD services to allow for authentication

- **Software-Defined Networking (SDN)**
    - Ability to mix and match products from different vendors
    - Increased choices in network development
    - Increase layers of automation and policy management
    - Fully automated deployments of a network within the cloud
    - Provisioning of networks links, appliances, and servers
    - **Control Plane**
        - Carries the traffic that provides the signals to or from a router
        - Decides how to move data
    - **Data Plane/Forwarding Plane**
        - Carries user traffic
        - Actually moves the data
    - **Management Plane**
        - Monitoring traffic conditions and network status
    - **Open SDN**
        - An open-source variant of software defined networking
    - **Hybrid SDN**
        - Employs traditional and SDN protocols to operate
    - **SDN overlay**
        - Creates virtual connections between different endpoints to provide additional security benefits

Infrastructure Design

Objectives 1.2

- **OBJ 1.2**: Given a scenario, analyze the organizational requirements to determine the proper infrastructure security design.

- **Scalability**
  - Measure by the number of requests a system or application can effectively support simultaneously
  - **Vertical Scaling (Scaling Up)**
    - Increasing the power of the existing resources in the working environment
  - **Horizontal Scaling**
    - Adding additional resources to help handle the extra load being experienced
    - Use service-oriented architectures when building for horizontal scaling
      - Continuous available resources
      - Unlimited capacity
      - Pay-per-use basis
      - Built-in redundancy
      - Easy to size and resize

- **Resiliency Issues**
  - Focused on maintaining business continuity for critical services, applications, and data
  - Creating a homogenous environment puts systems at a greater risk of breach
  - Perform a calculated risk management decision to decide if using same or different operating systems
  - Goes hand-in-hand with availability
  - **Orchestration**
    - Involves creating fully automated workflows
  - **Persistent**
    - Retained after power loss
  - **Non-Persistent**
    - Lost after power loss
  - **High availability**
    - Systems are up and available

- **Redundancy**
  - Having extra components which are not strictly necessary to the function, but are used in case of a failure in another component
  - **Redundant hardware**
    - Using multiple pieces of physical hardware
      - Mirror hard disks
      - Redundant routers
- **Fault tolerance**
  - By utilizing its measures, such as redundant hardware, power sources, and network connections, we can increase resiliency across the entire system
- **SLA**
  - Another way to mitigate costs of maintaining availability while also minimizing our downtime
  - Can also act as a formalized agreement between a service provider and our organization
- **MTBF/MTTR**
  - **MTBF**
    - Is a measure of how reliable our devices are since it measures the average amount of time the device operates before it breaks or fails
  - **MTTR**
    - Is the average amount of time it takes to get particular device fixed and back online
- **Single point of failure**
  - It is best to design our network without any single points of failure, such as a single router that connects to our business to the internet
  - The key to eliminate single points of failure is redundancy
- **Load balancing**
  - Spreads the computational workload across multiple hardware products
  - **Replication**
    - Is the act of copying or reproducing something
    - Ensures high availability of data, but not integrity
- **Clustering**

        - Relies on software instead of hardware to perform the load balancing functions
    - **Failover**
        - Allows a system to automatically switch over to a backup system if the primary system cannot continue to operate
    - **Failsoft**
        - Terminates any noncritical processes when a failure occurs in an attempt to continue operations

- **Automation**
    - Use of electronics and computer-controlled devices to assume control of processes
    - **Autoscaling**
        - Monitors applications and servers and then automatically adjusts their capacity to maintain performance at the lowest cost
    - **SOAR**
        - Facilitates incident response, threat hunting, and security configurations without any human assistance
    - **Playbook**
        - A checklist of actions to take to detect and respond to a specific type of incident
            - **Runbook**
                - An automated version of a playbook which leaves clearly defined interaction points for human analysis
    - **Bootstrap**
        - A Perl framework that takes manual release processes and makes them automated

- **Performance Design**
    - **Latency**
        - Time it takes to complete an action
    - **Traffic**
        - Busyness of systems and their components
    - **Erros**
        - Identify issues and indicate possible security issues
    - **Saturation**
        - How much of a given resource is being used by the system or service

- **Content Delivery Network (CDN)**
  - Allows for the quick transfer of assets needed for loading internet content
    - Improve website load times
    - Reduce bandwidth costs
    - Increase content availability and redundancy
    - Improve website security
- **Catching**
  - High-speed data storage layer that stores a subset of data for future requests

- **Virtualization**
  - A host computer installed with a hypervisor that can be used to install and manage multiple guest OSs or VMs
  - **Hypervisor**
    - Manages the distribution of the physical resources of a server to the VMs
  - **Virtual Desktop Infrastructure (VDI)**
    - Hosts desktop OSs within a virtualized environment hosted by a centralized server or server farm
  - **Centralized Model**
    - Hosts all the desktop instances on a single server or server farm
  - **Hosted Model/Desktop as a Server (DAAS)**
    - Maintained by a service provider and provided to the end user as a service
  - **Remote Virtual Desktop Model**
    - Copies the desktop image to a local machine prior to being used by the end user
  - **Terminal Services**
    - A server-based solution that runs the application on servers in a centralized location
  - **Application streaming**
    - A client-based solution that allows an application to be packaged up and streamed directly to a user's PC

- **Containerization**
  - A type of virtualization applied by a host OS to provision an isolated execution environment for an application

        - Docker
        - Parallels virtuozzo
        - Open VZ
    - Set up virtual servers in the cloud with proper failover, redundancy, and elasticity

Cloud and Virtualization

Objectives 1.6

- **OBJ 1.6**: Given a set of requirements, implement secure cloud and virtualization solutions

- **Cloud Deployment Models**
    - **Public cloud**
        - Systems and users interact with devices on public networks, such as the internet and other clouds
    - **Private cloud**
        - Systems and users only have access with other devices inside the same private cloud or system
    - **Hybrid cloud**
        - Combination of private and public clouds
    - **Community cloud**
        - Collaboration effort where infrastructure is shared between several organizations from a specific community with common concerns
    - **Multitenancy**
        - Allows customers to share computing resources in a public cloud or private cloud
    - **Single Tenancy**
        - Assigns a particular resource to a single organization

- **Cloud Service Models**
    - **On-premise**
    - **Hosted**
        - Authentication and authorization mechanisms
        - Redundancy and fault tolerance measures
        - Storage location and location-based laws
        - Multitenancy might cause your data to be hosted on the same physical server as another organization's data
    - **Software as a Service (SaaS)**
        - The service providers provides organization with a complete solution
    - **Infrastructure as a Service (IaaS)**

        - Allows for the outsourcing of the infrastructure of the server and desktops to a service provider
    - **Platform as a Service (PaaS)**
        - Provides a platform for companies that develop applications without the need for infrastructure

- **Deployment Considerations**
    - As you design cloud architecture it is important to consider the
        - Cost
        - Scalability
        - Resources
        - Location
        - Data protection
    - **Technical testing**
        - Conducting unit level, performance, robustness, and vulnerability testing
        - Fiber
            - Additional costs
        - Copper
            - EMI
        - Wireless
            - RFI, Eavesdropping

- **Provider Limitations**
    - Assign the IP address to a content switch or load balancer
    - Ensure the DHCP scope used by the VMs are properly configured
    - **VPC Peering**
        - Allows communication of traffic between two VPCs as if they were on the same network
        - Transfer data from region to region for redundancy and fallback purposes
    - **Middleware**
        - Software that connects computers and devices to other applications and networks
        - Gives functionality to for data transformations, monitoring, and administration

- **Extending Controls**
    - Use a small utility

- Always up-to-date
- Relies on fast internet
- Doesn't do full scan
- Vulnerability data may be stored on the provider's systems
- **Sandboxing**
  - Utilizes separate virtual networks to allow security professionals to test suspicious or malicious files
- **Cloud Security Broker**
  - Acts as a middleman and consolidates all of the different cloud security services into one suite of tools for an organization
- **Security as a Service (SECaaS)**
  - Provides security for organizations that do not have the necessary security skills

- **Provision and Deprovision**
  - **Provisioning**
    - To set a certain amount of resources in order to provide an established service
  - **Deprovisioned**
    - To free up resources back to the host server

- **Storage Models**
  - **Storage Model**
    - Describes the method used by a cloud computing infrastructure to store data
  - **Object storage**
    - A computer data storage architecture that manages data as distinct units called objects
  - **Filed-based Storage**
    - Similar to object storage but comes with a hierarchical file and folder structure imposed on the data
  - **Data Storage**
    - An organized and structured format for storage
  - **Binary Large Objective (Blob) Storage**
    - A collection of binary data stored as a single entity
  - **Key-Value Pair**

        - Type of nonrelational database that uses a simple key-value method to store data
    - **Metadata**
        - A set of data that describes and gives information about other data
    - **Tag**
        - Indicates the type of information and dictates its importance among other pieces of information

- **Virtualization**
    - **Hypervisor**
        - Manages the distribution of the physical resources of physical resources of a server to the VMs
    - **Type I (Bare Metal)**
        - Replaces the OS on the physical server
            - vSphere
            - ESXi
            - Hyper-V
            - XenServer
    - **Type II (Hosted)**
        - Installed after an OS is placed on the server
    - **Container-Based Virtualization**
        - Each container relies on a common host OS as the base for each container
    - **Hyperconverged Infrastructure**
        - Allows for the full integration of the storage, network, and servers without hardware changes
    - **Application Virtualization**
        - Encapsulates computer programs from the underlying OS on which they are executed
    - **Virtual Desktop Infrastructure (VDI)**
        - Hosts desktop OSs within a virtualized environment hosted by a centralized server or server farm
    - **Emulation**
        - involves having a system iitate another system
    - **Virtualization**
        - New “physical” machine

Software Applications

Objectives 1.3

- **OBJ 1.3**: Given a scenario, integrate software applications securely into an enterprise architecture

- **Systems Development Life Cycle**
    - Occurs from a system's initial idea, development, release and retirement
        - Acquire
            - Conduct risk assessment
        - Develop
            - Determined capability
    - **Asset Disposal**
        - Occurs whenever a system is no longer needed by an organization
    - **Degaussing**
        - Exposes the hard drive to a powerful magnetic field to wipe previously written data from the drive

- **Software Development Life Cycle (SDLC)**
    - A subset of a system's development which focuses on the creation of a software to support a give solution
    - Plan and initiate the project
    - Gather the requirements
    - Design the software
    - Develop the software
    - Test and validate the software
        - Functionality
        - Vulnerability
        - Penetration
        - Validation Testing
            - Meets requirements
        - Acceptance Testing
            - Accepted by end users
        - Unit testing
        - Integration testing
        - User acceptance testing

        - Regression testing
        - Peer review
    - Release and maintain the software
    - Certify and accredit the software
    - Perform change and configuration management

- **Development Approaches**
    - **Waterfall**
        - An incremental approach where steps are followed in a sequential order
    - **Spiral**
        - An iterative approach that places emphasis on risk analysis during each phase
        - Methodology consist of five phases
            - Planning
            - Risk assessment
            - Engineering
            - Coding/implementation
            - Evaluation
    - **Agile**
        - Requires continuous feedback and cross functional teamwork
        - Prioritizes customer satisfaction
        - Security
            - Embed security expert
            - Ensure security testing
        - **Development**
        - **Quality assurance**
        - **Operations**
    - **DevOPs**
        - Combination of development and operations.
        - Places the development, quality assurance, and operations functions all into one team to force collaboration across the functions
        - decrease the time to deployment for a product
        - **DevSecOps/SecDevOps**
            - Integrates security into every phase of the development lifecycle
    - **Versioning**
        - Indicates the history of a particular software base

- **CI/CD**
  - Eliminates handoffs and delays that the old methods utilized
- **Continuous Integration**
  - software development method where code updates are tested and committed to a development
    - Create
    - Test
    - Implement
- **Continuous Delivery**
  - Software development method where the application and platform requirements are frequently tested and validated for immediate availability
    - Tests
    - Compliance
    - Validations
  - Focused on automated testing of code in order to get it ready for release. Not released, just ready for release
- **Continuous Deployment**
  - Takes the concept of continuous integration and continuous delivery, and take it even one step further because there is no a software development model
  - Deploy a code to staging and then at regular intervals move things from staging into production
  - Focuses on automated testing and the release of code in order to get it into the production environment much more quickly

- **Software Assurance**
  - Ensures applications meet and acceptable level of security for the functions they are designed to provide
  - Planning
  - Contracting
  - Monitoring/accepting
  - Follow-on
- **Risk Management**
  - Continually looks at risks, vulnerabilities and the appropriate mitigations
- **Sandbox (Development Environment)**

        - Isolates untested code changes and outright experimentation from production repository
    - **Standard Libraries**
        - Contain common functions and objects used by a programming language which allows a developer to reuse them
        - Application Security Libraries
            - Input validation
            - Secure logging
            - Encryption/decryption
            - Authentication
    - **DevOps**
        - Allows developers and other professionals to collaborate on building and deploying code to a production environment
    - **Code Signing**
        - An operation where a software developer or distributor digitally signs the file being sent out
    - **Interactive Application Security Testing**
        - Testing done while the app is run by any activity "interacting" with the application's functionality
    - **Fuzzer**
        - Injects invalid or unexpected inputs into an application to determine its reaction
        - Always use fuzzing during application testing
        - Adhere to good project management and safe coding practices
        - Deploy an application-level firewall to help detect and stop fuzzing from occurring on web applications
        - **Mutation**
            - Changes existing input values
        - **Generation-Based**
            - Generates inputs from scratch
    - **Static Application Security Testing**
        - Analyzes source code to find security vulnerabilities that make applications susceptible to attack
        - **Code Review**
            - Method of formal or informal review of the programming instructions
            - Informal methods

- Pair programming
- Email
- Over-the-shoulder
- Tool-assisted

- **Dynamic analysis**
  - Application security solution that can help to find certain vulnerabilities in web applications while they are running in production
  - Often assisted through the use of automated tools but can also be performed manually

- **Baselines and Templates**
  - **Baseline**
    - Standard operating system environment
    - Simplifies the process of securing a new machine
    - Allows a system administrator to create a standardized set of configuration settings
    - Check workstations against the baseline configuration on weekly basis
  - **Secure Design Pattern**
    - Eliminates the accidental insertion of vulnerabilities into code and mitigates their consequences
  - **Storage Design Pattern**
    - Provides a more secure layout for the storage of data in a web application
  - **Container API**
    - Creates and manages data containers using an application programming interface
  - **Secure Coding Standards**
    - another great thing to utilize as a form of baseline and templates
    - Have been developed through a community effort for each of the major programming languages
      - Computer Emergency Response TEam (CERT)
      - National Institute of standards and technology (NIST)
  - **Application Vetting**
    - Verifies if an application meets an organization's security requirements
  - **API Management**
    - Creating and publishing web applications programming interfaces
    - Enforcing usage policies

        - Controlling access
        - Nurturing subscriber community
        - Collecting and analyzing usage statistics
    - **Middleware**
        - Connects computers and devices to other applications and networks

- **Best Practices**
    - **Open Web Application Security Project (OWASP)**
        - Injections
        - Broken authentication
        - Sensitive data exposure
        - XML external entities
        - Broken access control
        - Security misconfigurations
        - Cross-site scripting
        - Insecure deserialization
        - Using components with known vulnerabilities
        - Insufficient logging and monitoring
    - **Build Security In (BSI)**
        - Program under the Department of Homeland Security
        - Provides additional security recommendations and architectures can use to reduce vulnerabilities, mitigate exploitations, and improve the quality of their software applications
    - **ISO/IEC 27034**
        - Provides industry wide guidance on securely developing and maintaining software applications
    - **WSS**
        - Add a security layer for web services which can allow for the digital signing and encryption of SOAP messages as well as methods to utilize security tokens for secure authentication
    - **The OWASP Secure Headers Project**
        - Describes the different HTTP responses headers that your application can use
        - Increases security of your application when placing calls
    - **Ex-Frame-Options Header**
        - Used to prevent clickjacking from occurring by declaring a policy that communications are only allowed from a host to the client browser

directly without allowing frames to be displayed inside of another web page

- **Security requirements Traceability Matrix**
  - Documents the security requirements a new application must meet
- **Requirements definition**
  - Documents each function and security requirements that must be built into an application
  - In Agile, requirements definitions are captured as a user story
- **System design document**
  - Describes the application and its architecture
    - Data design
    - Architecture design
    - Interface design
    - Procedural design
- **Test Plans**
  - Describes what will be tested in application and how it will be tested
    - Master
      - Unified
    - Level-specific
      - Outline
    - Type-specific
      - Specific Issue
  - **Identify key factors**
    - Overview
    - Items
    - Approach
    - Pass/fail criteria
    - Suspension criteria
    - Deliverables
    - Environment
    - Schedule
    - Cost estimates
    - Staffing needs
    - Risks
    - Assumptions
    - Dependencies
    - Required approvals

- **Integrating Application**
  - **The Customer Relationship Management (CRM)**
    - Stores all of the data relating to the organization's customers
  - **Enterprise Resource Planning (ERP)**
    - Collects and consolidates data from across the organization
  - **Configuration Management Database (CMDB)**
    - Keeps track of every asset in the organization
  - **Content Management System (CMS)**
    - A centralized repository of organizational information
  - **Directory Services**
    - Often used to integrate other services
  - **Domain Name System (DNS)**
    - Associates a hostname with an IP address
  - **Service-Oriented Architecture (SOA)**
    - Provides services with a single purpose or function
  - **Enterprise Service Bus (ESB)**
    - Enables communication between applications and protocols

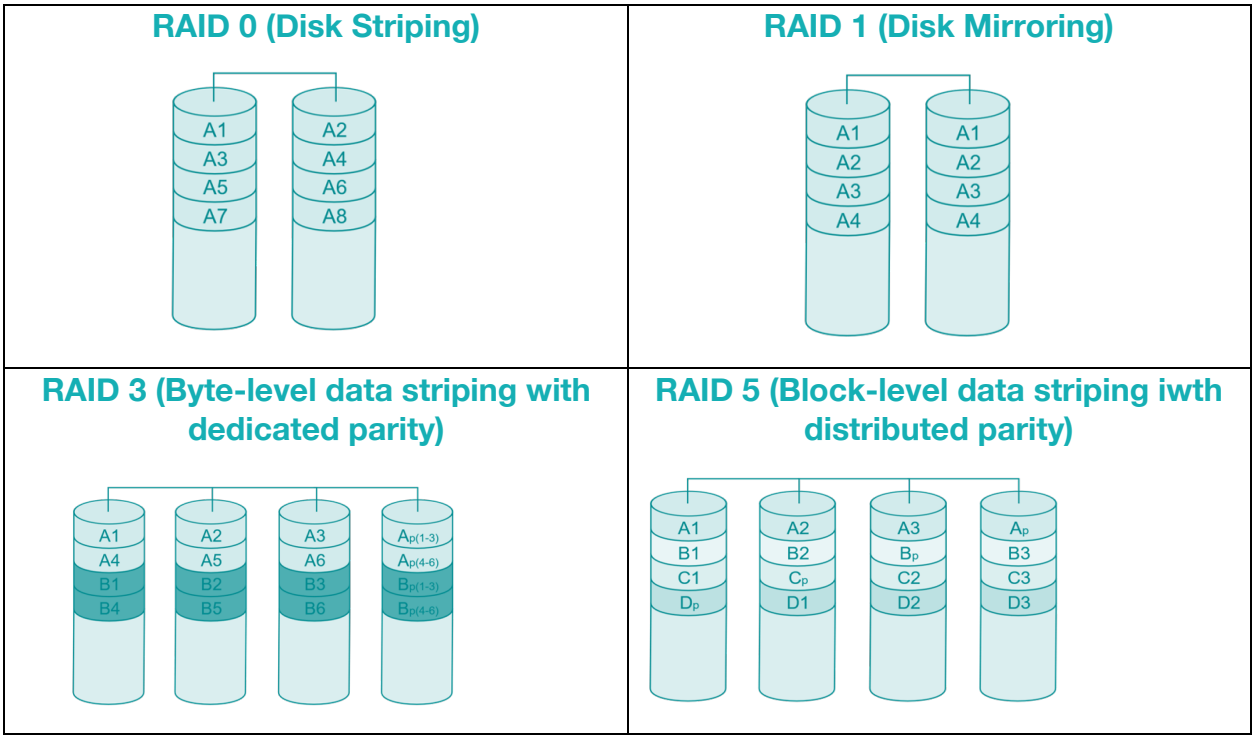
Data Security

Objectives 1.4

- **OBJ 1.4**: Given a scenario, implement data security techniques for securing enterprise architecture

- **Data Life Cycle**
  - The entire period of time that data exists within your systems
    - Creation
    - Usage
    - Sharing
    - Storage
    - Archival
    - Destruction
  - **Data Creation**
    - Occurs when existing data produced outside the system is imported into the system
  - **Data Entry**
    - Occurs when information is manually typed into the system by personnel in the organization
  - **Data Capture**
    - Occurs when data is generated by a divide used in the organization
  - **Data Use**
    - Phase where data is put to work to achieve some purpose within your organization
  - **Data Sharing**
    - Occurs when user makes the data available to someone outside the organization
  - **Data Storage**
    - Occurs when the data is not being actively used
  - **Data Archival**
    - Copying of data to an environment where it is stored in case it will be needed in an active production environment again later
  - **Data Destruction**
    - At some point, the data you have created, used, shared, stored, and archived is no longer valuable to you

- **Data Inventory/Data Mapping**
  - Serves as a single source of truth within the organizatio
- **Data Integrity Management**
  - Protects data against improper modification or alteration
- **Redundant Array of Inexpensive Disks (RAIDs)**
  - Allow data to be written to a logical partition spread across multiple physical disk drives
    - RAID 0
      - Disk striping
    - RAID 1
      - Mirroring
    - RAID 3
      - Byte-level data striping with dedicated parity
    - RAID 5
      - It is known as a block-level data striping with distributed parity.



- RAIDs can be either software or hardware

- **Storage Area Network (SAN)**
  - Connects storage storage devices using a high speed private network interconnected by storage-specific switches

- **Data Classification**
  - Applies confidentiality and privacy labels to a piece of information
  - **Unclassified**
    - No restrictions and presents no risk if disclosed to the public
  - **Classified**
    - Controlled data restricted to authorized persons or third parties under an NDA
  - **Confidential**
    - Highly-sensitive data restricted to approved persons or those trusted under an NDA
  - **Secret**
    - Valuable and has to be protected by several restricting its viewing
  - **Top Secret**
    - Any type of information that could cause grave danger if disclosed

- **Labeling and Tagging**
  - **Declassification**
    - Downgrading of a classified piece of data or information to the unclassified level
  - **BIGOT**
    - British Invasion of German Occupied Territories
  - **Data Tag**
    - Identifies a piece of data under a subcategory of a classification
  - **Unclassified Classification Label**
    - PII (Personally Identifiable Information)
    - SPI (Sensitive Personal Information)
    - PHI (Personal Health Information)
    - Financial data
    - SI
      - Special Intelligence
    - TK
      - Talent keyhole
    - HCS

        - Human intelligence control system
    - **Data format**
        - The way information is organized into present structures or specification
            - Structure data
            - Unstructured data

- **Deidentification**
    - Removes identifying information from data before distribution
    - **Data Masking**
        - Substitutes a generic or placeholder label from real data
        - Keeps the same format and same structure of the data
    - **Tokenization**
        - Substitutes a unique token for the real data
    - **Aggregation and Banding**
        - Gathers and generalized the data to protect the individuals involved
    - **Data Scrubbing**
        - Amends or removes data in database
    - **Anonymization**
        - Removes or modifies personal identifiable information from a data set
    - **Reidentification**
        - Combines deidentified data sets with other data sources

- **Data Encryption**
    - Is a form of risk mitigation
    - **Unencrypted Data (Cleartext/Plaintext)**
        - Stored, transmitted, or processed in an unprotected format that anyone can view and read
    - **Data State**
        - Location of data within a processing system
    - **Data State**
        - Location of data within a processing system
    - **Data at Rest**
        - Any data stored in memory, a hard drive, or a storage device
            - **Full disk encryption**
            - **Folder encryption**
            - **File encryption**
            - **Database encryption**

- **Data in Transit/Data in Motion**
  - Any data moving from one computer or system to another over the network or within the same computer
    - **TLS or SSL**
    - **IPSec or L2TP**
    - **WPA2 with AES**
- **Data in Use/Data in Processing**
  - Any data read into memory or is currently inside the processor and being worked on or manipulated

- **Data Loss Prevention (DLP)**
  - Detects and prevents sensitive information from being stored or transmitted over unauthorized networks
    - **Policy server**
    - **Endpoint agent**
    - **Network agent**
      - **Structured data format**
        - Follows a specific format
      - **Unstructured data format**
        - Does not follow a specific format
  - **Four actions used by DLP**
    - **Alert**
      - if the DLP is set to alert only, it will allow the data transfer to continue its destination, but logs and alerts
    - **Block**
      - Stops the users from being able to copy the file from the shared drive
    - **Quarantine**
      - Will block the user from copying the file and then it will take away the user's access to even read or open the file
    - **Tombstone**
      - The file on the share drive is replaced by a file that simply contains a message that states a policy violation has occurred
  - **Data Security Features**
    - **Removable/external media blocking**
      - Prevents a user from conducting mass data exfiltration using an external device

    - **Print blocking**
        - Blocks the ability to print to a networked or USB-connected printer
    - **RDP blocking**
        - Prevents copying and pasting between the remote client PC connected over RDP and their host
    - **Clipboard privacy controls implementation**
        - Prevents attempts of copying and pasting files into another file type that may not be protected by the DLP system
    - **VDI implementation restriction**
        - Protects the VDI-hosted image when being used by end users
    - **Classification-based data blocking**
        - Allows or blocks data movement based on its associated classification level

- **DLP Detection**
    - **Classification**
        - Process of classifying something according to shared qualities or characteristics
    - **Dictionary**
        - Acts as a set of patterns that should be matched by the system
    - **Policy template**
        - Contains dictionaries optimized for data points in a regulatory or legislative schema
        - Different policy templates contain different formats
    - **Exact data match (EDM)**
        - A structured database of string values that will be search for by the DLP until it finds a matching entry
    - **Document matching**
        - Matching of an entire or partial document against a set of known hashes
    - **Statistical or lexicon**
        - Document matching that uses machine learning to analyze a range of data sources

- **Data Loss Detection**
    - **Watermarking**

        - Process of superimposing a logo or piece of text to a document or image file as a means of aiding the copyright protection
    - **Forensic Watermark**
        - A digital watermark hidden in the file and can be validated by a piece of software
    - **Digital Rights Management (DRM)**
        - Mitigates the risk of unauthorized distribution of digital media without the copyright holder's permission
        - Hardware
            - Requires an authorized player
        - Software
            - Requires a specific type of software player
    - **Network Traffic Decryption**
        - Breaks open encrypted traffic and inspects its content using deep packet inspection
    - **Deep Packet Inspection**
        - Examines the content of data packets as they pass by the checkpoint on the network
    - **Network Traffic Analysis**
        - Monitors the data flows on a network to identify patterns or anomalies

Authentication and Authorization

Objectives 1.5

- **OBJ 1.5**: Given a scenario, analyze the security requirements and objectives to provide the appropriate authentication and authorization controls

- **Access Control**
  - **Mandatory Access Control**
    - Uses security labels to determine which users are authorized to access a resource
  - **Discretionary Access Control (DAC)**
    - Allows the resource owner to specify which users can access each resource
  - **Role-Based Access Control**
    - Allows an administrator to assign roles and permissions to access each resource
  - **Rule-Based Access Control**
    - Allows an administrator to implement security policies across all of their users
  - **Attribute-Based Access Control**
    - Relies on a set of characteristics of an object to make access control decisions
      - User Attributes
      - Environment attributes
      - Resource attributes

- **Credential Management**
  - Creates and manages strong passwords with only one master password to remember
  - **Hardware Key Manager**
    - Stores usernames, passwords, or encryption keys
  - **Privileged Access Management (PAM)**
    - Safeguards accounts that contain special access or capabilities beyond a regular user

- **Password Policies**
  - Promotes strong passwords by imposing acceptable password specifications

- **Complexity**
  - Having different characters used, such as lowercase letters, uppercase letters, numbers and special characters
- **Minimum Age**
  - Certain numbers of days before a user can reset their password
- **Password History**
  - Dictates the number of different passwords to be used before using a previously used one
- **Auditing**
  - reviews the password policy to ensure proper settings

- **Multifactor Authentication**
  - Uses two or more means (or factors to prove a user's identity
    - Identification
      - Provides identity
    - Authentication
      - Validates identity
    - Knowledge
      - Something you know
    - Ownership
      - Something you have
    - Characteristics
      - Something you are
    - Location
      - Somewhere you are
    - Action
      - Something you do
  - **Multifactor authentication**
    - Occurs if you have two or more factors required
  - **Time-Based On-Time Password (TOTP)**
    - Computers password from a shared secret and the current time
  - **HMAC-Based One-Time Password (HOTP)**
    - Computers password from a shared secret is synchronized across the client and the server
  - **In-Band Authentication**
    - Relies on a an identity signal form the same system requesting the user authentication

- **Out-of-Band Authentication**
  - Uses a separate communication channel to send the OTP or PIN

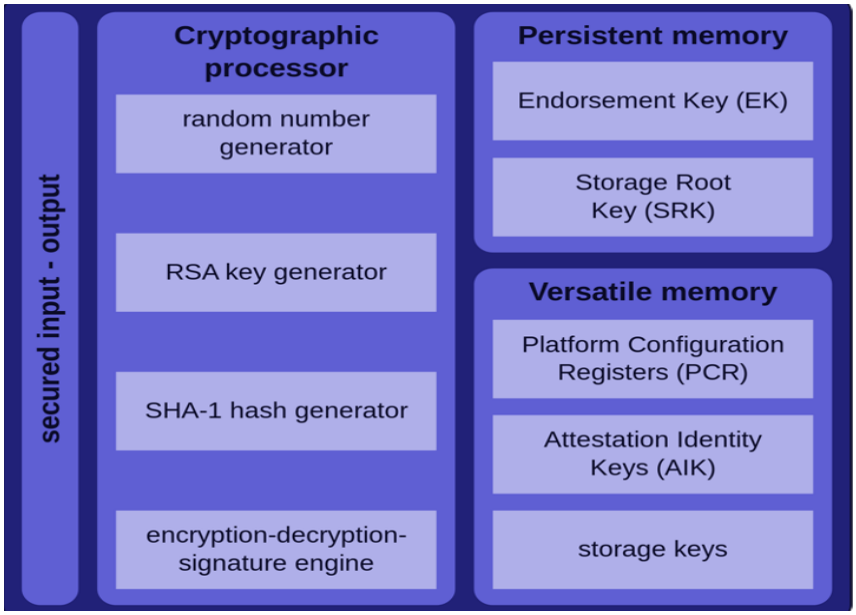
- **Authentication Protocols**
  - **Remote Authentication Dial-In User service (RADIUS)**
    - Cross-Platform protocol that authenticates and authorizes users to services, and accounts for their usage
  - **Terminal Access Controller Access Control System Plus (TACACS+)**
    - Cisco-proprietary protocol that provides separate authorization, authorization, and account services
  - **Diameter**
    - Peer-to-peer protocol created as a next-generation version of RADIUS
  - **The Lightweight Directory Access Protocol (LDAP)**
    - Cross-platform protocol that centralized info about clients and objects on the network
  - **Single Sign-On (SSO)**
    - Enables users to authenticate once and receive authorizations for multiple services across the network
  - **Kerberos**
    - Uses symmetric encryption and the Key Distribution Center to conduct authentication and authorization functions
  - **802.1x**
    - Used for port-based authorization on both wired and wireless networks
      - Supplicant
      - Authenticator
      - Authentication Server
  - **Extensible Authentication Protocol (EAP)**
    - Allows for numerous different mechanisms of authentication
    - **EAP-MD5**
      - Utilizes simple passwords and the challenge handshake authentication process to provide remote access authentication
    - **EAP-TLS**
      - Uses public key infrastructure with a digital certificate being installed on both client and the server
    - **EAP-TTLS**

        - Requires a digital certificate on the server and a password on the client of its authentication
    - **EAP-Flexible authentication via Secure Tunneling (EAP-FAST)**
        - Uses a protected access credential to establish mutual authentication between devices
    - **Protected EAP (PEAP)**
        - Uses server certificates and Microsoft's Active Directory databases to authenticate a client's password
    - **Lightweight EAP (LEAP)**
        - A proprietary protocol that only works on Cisco-based devices

- **Federation**
    - **Cross-Certification**
        - Utilizes a web of trust between organizations where they certify one another inside the federation
    - **Trusted Third Part (Bridge)**
        - Allows organizations to place their trust in a single third-party
    - **Transitive Trust**
        - A two-way relationship automatically created between parent and child domains within MS Active Directory
    - **Security Assertion Markup Language (SAML)**
        - An attestation model built upon de XML for SOAP-based web services
            - When the organization needs to provide single sign-on services or participate in them
            - When the organization needs to allow an application to access its web portal
            - When the organization needs to provide a centralized identity service and process
    - **OpenID**
        - An open standard decentralized protocol for authentication users
    - **Open Authorization (OAuth)**
        - Allows different websites to rely on a trusted third party to authenticate users
    - **JSON Web Token**
        - Provides authorization and specifies what access rights and privileges a user will have on a given system

- **Shibboleth**
  - An open-source option for SSO capabilities that utilized SAML

- **Root of Trust**
  - Contains the keys used for cryptographic functions and enables a secure boot process
    - Scans the boost metrics and OS files to verify signatures



  - **Hardware Security Module (HSM)**
    - Generates and stores cryptographic keys and is less susceptible to tampering and insider threats

- **Attestation**
  - Allows enterprise security personnel to determine if a change to the baseline has been made
  - **Attestation Integrity Key**
    - Determines the integrity of a TPM chip

- **Identity Proofing**
  - Identity Proofing relies on a person providing additional proof of who they are

Cryptography

Objectives 1.7

- **OBJ 1.7**: Explain how cryptography and public key infrastructure (PKI) support security objectives and requirements

- **Privacy and Confidentiality**
  - **Privacy**
    - Protects sensitive information about someone's personally identifiable information
  - **Confidentiality**
    - Protects against unintentional, unlawful or unauthorized access, disclosure, or theft of any sensitive information
      - Symmetric
        - 1000X faster than asymmetric encryption
      - Asymmetric

- **Integrity**
  - focuses on the accuracy and completeness of the data
  - Maintains the consistency of and trustworthiness of the data throughout its life cycle
  - **Hash Function**
    - Maps arbitrary sized-data to a fixed-size value
  - **Hash Digest**
    - Unique digital identifies or fingerprint that represents the data received as an input to the function

- **Non-repudiation**
  - Assures that sender of the message cannot deny the validity of the message sent

- **Compliance and Policy**
  - **Compliance**
    - The act of complying with orders, rules or requests
  - **Policy**
    - Sets the standards of behaviors for activities and dictates how to conduct cybersecurity within the organization

- **Gramm-Leach-Bliley Act (GLBA)**
  - Mandates financial services organizations to protect the security and confidentiality of nonpublic personal information
  - Full disk encryption
  - Folder encryption
  - Data encryption
  - VPN encryption
- **Sarbanes-Oxley Act (SOX)**
  - Mandates publicly traded companies to protect sensitive data related to their financial reporting
- **Health Information Technology for Economic and Clinical Health Act (HITECH)**
  - A follow-on legislation to HIPAA that focuses on the use of encryption

- **Data States**
  - **Data at Rest**
    - Data physically stored in a digital format
      - Disk-level
      - Block-level
      - File-level
      - Record-level
  - **Data in Use/Data in Process**
    - Any information currently being processed or about to be processed
      - Intel
        - Software Guard Extensions
      - MS Windows
        - Data-Protection API
  - **Data in Transit**
    - Any information moving across the network
  - **SSL/TLS**
    - Maintains confidentiality of the data while it is in transit from the user's system to the server
  - **Secure Electronic Transaction (SET)**
    - Relied on a system of digital certificates and asymmetric keys
  - **3-D**
    - Provides additional security to payment card transactions over HTTPS
  - **Internet Protocol Security (IPSec)**
    - Create a secure and encrypted tunnel between two devices

- **Cryptographic Use Cases**
  - **Embedded System**
    - Contains both the needed hardware and software to perform a dedicated function
  - **Elliptic Curve Cryptography (ECC)**
    - A form of public key cryptography based upon the algebraic structure of elliptic curves over finite fields

- **PKI Use Cases**
  - **Web Service**
    - Any piece of software that makes itself available over the Internet that uses a standardized XML messaging system
  - **Code Signing**
    - Digitally signing executables and scripts to confirm the software author and guarantee code has not been altered
  - **Federation**
    - Links electronic identity and attributes stored across multiple distinct identity management systems
  - **Trust Model**
    - Informas applications how to decide on the legitimacy of a digital certification
  - **Web of Trust**
    - A decentralized security odel where participants can authenticate identities of other users
  - **Automation/Orchestration**
    - Automated configuration management, and coordination of computer systems, applications and services

Emerging Technology

Objectives 1.8

- **OBJ 1.8**: Explain the impact of emerging technologies on enterprise security and privacy

- **Artificial Intelligence & Machine Learning (AI & ML)**
  - **Artificial Intelligence**
    - Creates machines that develop problem solving and analysis strategies without human direction or intervention
      - There are resource issues involved
      - The data sets used for training can be a big limitation
      - AI is not just used by the defenders, but also by hackers
      - Neural fuzzing is used both for defense and attack
  - **Machine Learning**
    - Allows machines to learn from data without being explicitly programmed

- **Deep Learning**
  - **Artificial Neural Network (ANN)**
    - An artificial of input hidden, and output layers that perform algorithmic analysis of a dataset
  - **Natural LanguageProcessing (NLP)**
    - Gives computers the ability to understand text and spoken words that matches human behavior
  - **Deepfake**
    - A synthetic media where a person in an image or video is replaced with someone else's likeness

- **Big Data**
  - Large or complex data sets that traditional data processing applications cannot sufficiently handle
    - Volume
      - Sheer amount of data
    - Velocity
      - Rapid influx of data
    - Variety
      - Structured/Unstructured nature of data

- **Generation**
  - Active
    - Given to a third party
  - Passive
    - Generated through normal online actions
- **Storage**
  - File-level
  - Database-level
  - Media-level
  - Application-level
    - Attribute-based encryption
    - Homomorphic encryption
    - Storage path encryption
    - Hybrid cloud model
- **Processing**
  - Batch
  - stream
  - Grap
  - Machine Learning
    - Safeguard the information from an inadvertent or unsolicited disclosure
    - Extract meaning information from the big data being processed

- **Blockchain & Distributed Consensus**
  - **Cryptocurrency**
    - Function as a medium of exchange; digital version of money
  - **Blockchain**
    - Allows for the storage of data in blocks that are chained together in a chronological order and are immutable
  - **Distributed Consensus**
    - Process where members of the group collectively achieve agreement without the benefit of a centralized unit
      - proof of work
      - Proof of stake
      - Proof of authority

- **Passwordless Authentication**

- Allows the login to a computer system without entering a password or any other knowledge
  - Ownership Factor
    - Something you have
  - Inherence Factor
    - Something you are
  - Greater security
  - Better user experience
  - Reduced IT costs
  - Better visibility
  - Scalability
- **Biometric Impersonation**
  - The act of pretending to be another user to bypass a biometric-based passwordless authentication system
  - Ensure that the system has a low false positive rate

- **Homomorphic Encryption**
  - Permits users to perform computations on encrypted data
  - **Private Information Retrieval (PIR)**
    - Retrieves an item from a service in a possession of database without revealing which item is retrieved
  - **Secure Function Evaluation (SFE)**
    - Allows two parties to jointly evaluate a publicly known function without revealing their respective inputs
  - **Private Function Evaluation (PFE)**
    - Allows two parties to jointly evaluate a private function without revealing their respective inputs
  - **Secure Multi-Party Computation**
    - Creates methods for parties to jointly compute a function over their inputs while keeping those inputs private

- **Virtual/Augmented Reality**
  - **Virtual Reality**
    - A computer-generated simulation of a 3D image or environment that can be interacted with in a seemingly real or physical wa**y**
      - **Fully immersive VR**
      - **Semi-immersive VR**

        - **Augmented reality**

- **3-D Printing**
    - **3D Printing (Additive Manufacturing)**
        - The construction of a 3D object from a CAD model or a digital 3D model

- **Quantum Computing**
    - Combines physics, mathematics and quantum mechanics to exploit the collective properties of quantum states
        - Quantum
            - Smallest possible discrete unit
        - Qubit
            - Quantum bit
    - **Nanotechnology**
        - The use of matter on an atomic, molecular, and supramolecular scale for industrial purposes
    - **Quantum Cryptography**
        - The science of quantum mechanical properties to perform cryptographic functions and tasks

Enterprise Mobility

Objectives 3.1

- **OBJ 3.1**: Given a scenario, apply secure configurations to enterprise mobility

- **Enterprise Mobility Management (EMM)**
  - **Enterprise Mobility Management (EMM)**
    - Enables centralized management and control of corporate mobile devices
      - Tracking
      - Controlling
      - Securing
  - **EMM**- Policies and tools
  - **MDM** -Technical controls
    - Mobile Administration Common Features
    - Application Control
    - Passwords and passcode functionality
    - MFA requirement
    - Token-based access
    - Patch Management
    - Remote Wipe
  - **Device Certificates**
    - **Trust**
      - Globally identifies a trusted device within an organization
    - **User Specific**
      - Assigned to a device to uniquely identify it on the network
  - **Firmware updates**
    - Updates the baseband of the radio modem used for cellular, Wi-Fi, Bluetooth, NFC, and GPS connectivity

- **WPA3**
  - **Wi-Fi Protected Access 3 (WPA3)**
    - Latest and most secure version of wireless network encryption currently available
  - **Updated Cryptographic protocols**
    - Enterprise – 192-bit
    - Personal – 192-bit or 128-bit

        - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)
        - Galois Counter Mode Protocol (GCMP)
    - **Enhanced open**
        - Opportunistic Wireless Encryption (OWE)
    - **Management protection frames**
    - **Simultaneous authentication of equals (SAE)**
        - A secure password-based authentication and password authenticated key agreement that relies on forward secrecy
            - AP and client use a public key system to generate a pair of long-term keys
            - AP and client exchange a one-time use session key
            - AP sends client messages and encrypts them using the created session key
            - Client decrypts received messages using the same one-time use session key
            - Process repeats for each message being sent, starting at Step 2

- **Connectivity Options**
    - **NFC**
        - Uses radio frequency to send electromagnetic charge containing the transaction data over a short distance
        - Only use card readers from a trusted source
    - **Radio Frequency Identification (RFID)**
        - A form of radio frequency transmission modified for use in authentication systems
    - **Infrared Data (IrDA)**
        - Allows two devices to communicate using line of sight communication in the infrared spectrum
    - **Bluetooth**
        - Creates a personal area network over 2.4 GHz to allow for wireless connectivity
            - **Bluejacking**
                - Sending unsolicited messages to a Bluetooth device
            - **Bluesnarfing**
                - Making unauthorized access to a device via Bluetooth connection

        - **BlueBorne**
            - Allows the attacker to gain complete control over a device without even being connected to the target device
    - **USB Peripherals**
        - Able to connect using the USB or lightning port on a mobile device
    - **Tethering**
        - Shares cellular data Internet connection from a smartphone to multiple other devices
        - Only connect to trusted wireless networks

- **Security Configurations**
    - **Device configurations profiles**
        - Implement settings and restrictions for mobile devices from centralized mobile device management systems
        - Profiles are mainly used for security, but can also provide a vulnerability
        - Download only trusted profiles
    - **Full device encryptions**
        - Data at rest protection for your device's storage
            - iOS -56-bit unique ID
            - Android v6 - 128-bit AES keys
            - Android v7 - File-based encryption
            - Android v9 - Metadata encryption
    - **MicroSD Hardware Security Module (HSM)**
        - stores the cryptographic keys
    - **VPNs**
        - Some Mobile Device Management solutions provide a third-party VPN client
            - **Types of encryptions**
                - Secure socket layer
                - Transport layer security
            - **Mobile device support for VPNs**
                - Operative System Layer – "Always on"
                - Application Layer – Per-app basis
                - Web based – Location Masking (not as secure as OS)
            - **Location Services**

    - Refers to how a mobile device is allowed to use cellular data, Wi-Fi, GPS, and Bluetooth to determine its physical location
    - Geolocation - Uses a device's ability to detect its location to determine if access to a particular resource should be granted
  - **Geofencing**
    - Creates virtual boundaries based on geographical locations and coordinates
  - **Geotagging**
    - Adds location metadata to files or devices

- **DNS Protection**
  - **Custom DNS**
    - Custom DNS services can track requests being sent
    - Can protects your DNS requests
  - **DNS Over HTTPS (DoH)**
    - Encrypts DNS requests by tunneling through a TLS tunnel using the HTTPS protocol
    - Initial request is made on Port 53
    - DNS lookups on port 443
    - Increases privacy but bypasses some corporate restrictions

- **Deployment Options**
  - **Corporate-Owned, Business Only (COBO)**
    - Purchased by the company for use by the employees only for work-related purposes
    - Most Secure
    - Most Restrictive
    - Most Expensive
  - **Corporate-Owned, Personally-Enabled (COPE)**
    - Provides employees with a company procured device for work-related and/or personal use
  - **Choose Your Own Device (CYOD)**
    - Allows employees to select a device from an approved list of vendors or devices
  - **Bring Your Own Device (BYOD)**

        - Allows employees to bring their own devices into work and connect them to the corporate network
        - BYOD is the most difficult to secure
    - **Virtual Mobile Infrastructure (VMI)**
        - Like VDI but utilizes a virtualized mobile operating system

- **Reconnaissance Concerns**
    - **Concerns for mobile devices**
        - Digital Forensics
        - Wearable technology
        - Wireless eavesdropping
    - Ensure devices are setup to encrypt stored data and cloud backups
    - **Wearable Technology**
        - Any type of smart device worn on or implanted in the body
            - Smartwatch
            - Camera
            - Fitness device
            - Glasses
            - Headset
            - Medical sensor
        - Wearables collect a wide range of biometric and health data
        - Consider how to conduct digital forensics on wearable technologies owned by the company

- **Mobile Security**
    - **Key things to avoid**
        - **Jailbreaking (iOS)**
            - Enables a user to obtain root privileges, sideload apps, change or add carriers, and customize the interface of an iOS device
            - Most jailbreaks are Tethered, meaning that they need to be connected to a computer.
        - **Rooting (Android)**
            - Enables a user to obtain root privileges, sideload apps, change or add carriers, and customize the interface of an Android device
            - You can also root via Customr Firmware/Custom Rom which is a new Android OS image that can be applied to a device

        - Another root technique is Systemless Root, which does not modify system partitions or files and is less likely to be detected than a custom ROM
    - **Sideloading**
        - Installs an app on a mobile device directly from an installation package instead of an official store
        - Android and iOS devices block the installation of third-party applications
          by default
    - **Unauthorized app stores**
- **Best practices**
    - **Containerization**
        - Involves segmenting corporate-owned data and resources from personally-enabled mobile devices
    - **Application wrapping**
        - Adds a layer of security over an existing app on the device
    - **Trusted OEM suppliers**
        - Consider an OEM's supply chain management and security reputation
    - **Bootloader security**
        - Device bootloader validation before the device boots.
        - To achieve this, devices will use **eFuse** in which Permanently alters the state of a transistor on a computer chip if the bootloader is modified or altered.

Endpoint Security Controls

Objectives 3.2

- **OBJ 3.2:** Given a scenario, configure and implement endpoint security controls

- **Device hardening**
  - Ensures a device has had any unnecessary applications, services or ports disabled or removed from the host
    - **Only necessary services**
    - **Monitoring software**
    - **Maintenance schedule**
  - **Ensure endpoint security software are installed on the host**
    - **Secure Bios**
      - UEFI
      - TPM
      - HSM
  - **Host hardening**
    - Patch Software
    - Configure Device
    - Remove Unnecessary Applications
    - Block Unnecessary ports and services
    - Control External storage devices
    - Disable unneeded accounts
    - Rename default accounts
    - Change default passwords
  - **Other forms of Host hardening**
    - Standardized Baseline
    - Whitelist/Blacklist apps
    - Security & Group policies
    - CLI restrictions
    - Peripheral restriction
  - **Open the least number of ports and run the least amount of services**
  - **Hardening, What I should be looking at?**
    - Check any network interfaces that provide connectivity to the LAN or WAN
    - Look at the list of services installed and running on the clients and servers
    - Look at the ports being used by different application service ports

        - Utilize disk encryption to harden endpoints
        - Review all accounts on the system
            - **Anything unused or unneeded should be disabled, deleted, or blocked**
    - **Security implementation guides**
        - DoD Cyber Exchange (public)
        - Center for Internet Security
        - Security technical implementation guides (STIGs)
    - **Other Resources for Sec Implementations**
        - Downloadable GPOs
        - DoD SCRAP Compliance Checker
        - CIS Benchmarks
    - Verify Sec Implementation
        - CIS-CAT
        - Nessus Vulnerability Scanner
- Be Aware of Life Cycle of the device
    - End of Life (EOL)
        - The date when a manufacturer will no longer sell a given product
    - End of Support (EOS)
        - The last date that a manufacturer will support a given product

- **Patching**

- **Patch Management**
    - Scans the network for vulnerabilities and ensures systems are updated with proper software patches.
    - Mainly used to automate checking the need for patches

- **Hot Fix**
    - Solves a security issue and should be applied immediately after being tested in a lab environment

- **Update**
    - Provides a system with additional functionality, but does not usually provide any patching of security-related issues

- **Service Pack**

- Several released security patches bundled together

- **Effective Management Program. What does it take?**
  - An individual or a specific team responsible for tracking security patch releases
  - A mechanism to patch operating systems and applications on all systems
  - Cloud-based resources
  - Triage patching
  - A lab or test environment to test patches before deployment
  - Detailed logs of patching activity
  - A mechanism to evaluate, test, and deploy firmware updates
  - A technical process to push urgent patches into production environment
  - An evaluation of non-critical patches

- **Security Settings**
  - Settings you should be aware on your endpoint devices
  - **Local Drive Encryption**
    - Protects the contents of the storage device when the operating system is not running
      - Examples
        - MS Windows – BitLocker
        - Linux – Cryptsetup
        - OS X FileVault
    - **NX bit/XN bit**
      - They are set in the processor of the workstation
      - **NX** – Creates separate areas of memory where data can be placed. Code cannot be run on the areas.
      - **XN** – used specifically for areas of memory that cannot execute code at all.
  - **Disable virtualization support**
  - **Secure Enclave**
    - Provides CPU hardware-level isolation and memory encryption on every endpoint
  - **You can enable shell restrictions on your system**
    - The shell is powerful, but, in the wrong hands, it can also be destructive and harmful to the security of our systems.
      - Shell examples:

        - Bourne Shell
        - Korn Shell
        - C shell
        - Bash shell
    - Cisco router and switches utilize their own command-line environment
- **Address Space Layout Randomization (ASLR)**
    - Provides buffer overflow prevention by making it difficult to guess the location of executable files stored in the RAM

- **Mandatory Access Controls (MAC)**
    - **Mandatory Access Control (MAC)**
        - Uses security labels to determine which users are authorized to access a resource
    - **Security-Enhanced Linux (SELinux)**
        - Provides different modifications and patches to the Linux kernel to ensure higher levels of security
        - Operates as a Linux Securirty module
        - Provides Execution Control
            - Determines additional software or scripts that may be installed or run
              on a host beyond its installed baseline
    - **SEAndroid**
        - Allows for the enforcement of SELinux-type security inside the Android operating system
    - **TrustedSolaris**
        - Provides the same functionality on a Solaris server
    - **Kernel**
        - Is the heart of the operative system.
    - **Middleware**
        - Software that operates in the middle
        - Android uses Middleware Mandatory Access Control (MMAC)
            - Protects the kernel as it moves from the application space to the middleware and then to the kernel space for execution
    - **Least Functionality**
            - Ensures the system only provides access to essential capabilities
    - **Trusted Operating System**

        - Provides sufficient support for multilevel security to meet the requirements set by the government
    - **EAL** – Levels of Assurance 1 being the lowest and 7 being the highest

- **Secure Boot**

- **Security of the pre-OS environment**
    - **BIOS/UEIF**
        - **Basic Input Output System (BIOS)**
            - Initializes hardware for an operating system for it to boot
            - Computer that relies on Bios use Master boot record
        - **Unified Extensible Firmware Interface (UEFI)**
            - Provides support for 64-bit CPU operations, a full GUI and mouse operations, and better boot security
            - Computer that relies on UEFI use GUID partition table
    - **Trusted Platform Module (TPM)**
        - Stores and protects both symmetric and asymmetric encryption keys, hashes, and digital certificates
        - Use the tpm.msc console tool within Windows or via the Group Policy editor
    - **Secure Boot**
        - Prevents unwanted processes from executing during the boot operation
        - Secure Boot process:
            - Computer starts up
            - Firmware boot components load up
            - Boot manager starts
            - Windows loader begins
            - Windows kernel starts up
            - Boot critical driver installations occur
    - **Trusted Boot / Measured Boot**
        - Gathers secure metrics to validate the boot process in an attestation report
        - Check the hashes of key system state data
            - Boot firmware
            - Boot Loader
            - OS Kernel
            - Critical Drivers

- **Hardware Encryption**
  - **Attestation**
    - Ensures a machine meets a certain approved baseline before given access to a given resource
  - **Hardware Security Module (HSM)**
    - Generates and stores cryptographic keys and is less susceptible to tampering and insider threats
      - **Four Main functions**
        - Secure cryptographic key generation
        - Secure cryptographic key storage and management
        - Access to cryptographic and sensitive data
        - Offloading of symmetric and asymmetric cryptographic functions
      - **Downsides of HSM**
        - Costly
        - Lacks standard strength
        - Hard to upgrade
  - **Self-Encrypting Drive (SED)**
    - HDD or SSD with an encryption circuit built into the drive
    - Incorporates FIPS 140-2 and IEEE 1667 encryption standards

- **Endpoint Protections**
  - **Antimalware contains:**
    - Antivirus
    - Antispyware
    - Spam Filter
  - **Best Practices against malware:**
    - Update your antimalware regularly
    - Scan your computer regularly
    - Disable autorun
    - Disable auto preview on e-mail client
  - **Application controls**
    - Application Allow/Block list (formerly known as whitelist/blacklist)
    - Helps control what types of applications can be installed on workstations and servers
  - **Host-based firewall**

        - Accepts or drops packets based on the application or port being targeted by the inbound
        - Some attacks may come from these addresses range, block them:
            - 10..0.0.0/8
            - 172.16.0.0/12
            - 192.168.0.0/16
        - Linux and OS X also include host-based firewalls
            - Linux has Iptables
            - OS X has one integrated in the OS
    - **HIDS/HIPS**
        - Pieces of specialized software installed on the endpoint
        - **HIDS**
            - Detects and logs
        - **HIPS**
            - Detects, logs, and blocks
    - **Endpoint Detection and Response (EDR)**
        - Provides better visibility over endpoints to detect and respond to cyber threats and exploits
            - EDR examples:
                - FireEyE
                - EnCase
                - Symantec
                - RSA
                - Tanium
                - CrowdStrike
    - **User and Entity Behavior Analytics (UEBA)**
        - Provides automated identification of suspicious activity by user accounts and computer hosts

- **Resiliency**
    - Ensure resiliency by ensuring availability
    - Have a mixture of different OSs for resilience
        - **Orchestration**
            - Creates workflows that are fully automated
            - Distribute servers across two or more data centers
        - **Persistent data**
            - Stored on device and not lost on device power off

        - **Non-Persistent**
            - Stored in memory, data is lost on power off
    - **Fault tolerant measures:**
        - Redudant hardware
        - Redudant Power Sources
        - Redudant Network Connecitons
    - Ensure maintenance tasks cause minimal to no downtime
    - Choose hardware that has component redundancy
    - **Self-Healing Hardware**
        - Detects and reacts to component failures
            - Example: Raid Array

Cloud Technologies

Objectives 3.4

- **OBJ 3.4**: Explain how cloud technology adoption impacts organizational security

- **Business Continuity/Disaster Recovery**
  - **Business Continuity Planning**
    - Ensures the organization can recover from a disruptive event or disaster
    - **Business continuity**
      - Response to a disruptive event
    - **Disaster recovery**
      - Used during a disaster
  - Consideration when using the cloud as BCDR:
    - Legacy Application
    - Proprietary Data
  - Primary Provider
    - Cloud platform primarily used for the organization's business operations
    - Example: AWS
    - Multiple Datacenters
  - Contingent Cloud Platform
  - Acts as secondary or alternative provider

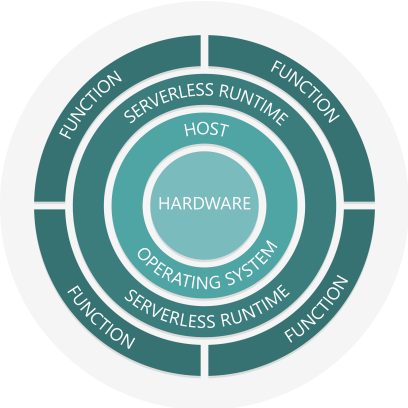
- **Cloud encryption**
  - Enable encryption by default.
  - **Algorithm** – always use a well-known open standard
  - Encryption mechanism Only as secure as the keys and the algorithms used
  - Ensure all keys have owners and bound to an identity
  - Never store data and its keys in the same cloud services
  - Break apart key management and key usage into two separate functions
    - 4 types of Key management System (KMS)
      - **Cloud-native key management system**
        - Configured and operated by the organization's cloud service provider
      - **External key organization**
        - Generated by a key management system not managed by the same cloud provider

- **Cloud service using external key management system**
  - Like external key organization, but using a cloud provider or cloud-based service for key creation
- **Multi-cloud key management system**
  - Incorporates the other three types of KMS into a single system

- **Data Dispersion**
  - Process of storing data across different storage locations
- **Bit/Cryptographic Splitting**
  - Splits encrypted data into parts and then stored in different storage locations where it is encrypted a second time

- **Serverless Computing**

- **FAAS (Function as a service)**



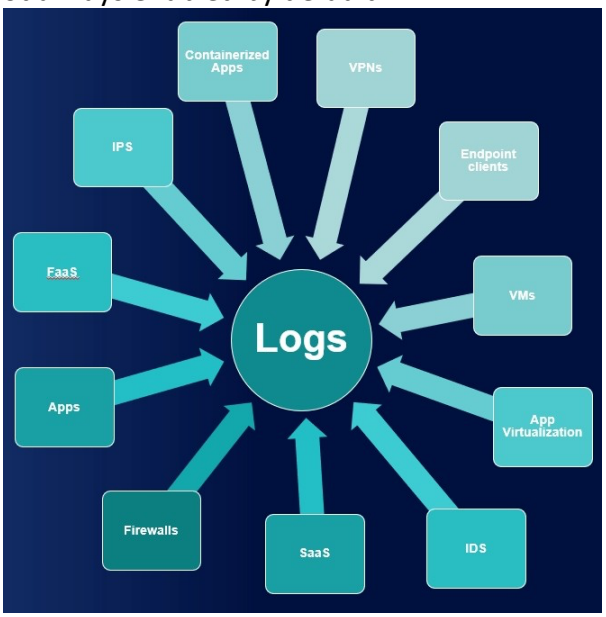
- **Serverless Computing**
  - Runs functions within virtualized runtime containers in a cloud
- **Microservice**
  - Designed to take an input, do some processing, and produce an output
- If demand increases, the FAAS starts up additional containers.
  - Benefits of serverless computing
    - No patching
    - No administration
    - No filesystem monitoring
- Our function in the world of Serverless Computing is to ensure clients accessing the services have not been compromised
  - Risks

- New infrastructure, not much information or best practices
- Fully dependent of the underlying service provider.
- Serverless depends highly on orchestration

- **Software-Defined Networking (SDN)**
  - **SDN**
    - software-based controllers or APIs to communicate with underlying hardware infrastructure and direct traffic on a network
  - **Infrastructure as Code (IaC)**
    - Provisions the architecture in which resource deployment is performed by scripted automation and orchestration
      - 3 portions of a typical network architecture:
        - **Control Plane**
          - Carries the traffic that provides the signals to or from a router
          - Decides how to move data
        - **Data plane**
          - Carries user traffic
          - Actually moves the data
        - **Management plane**
          - Monitors traffic conditions and network status
        - These functions are incorporated into a virtualized or decoupled device
  - **Advantages of SDN**
    - Ability to mix and match products from different vendors
    - Increased choices in network development
    - Increased layers of automation and policy management
    - Fully automated deployments of a network within the cloud
    - Provisioning of network links, appliances, and servers
  - **SDN disadvantages**
    - If we lose connectivity to the SDN controller, then the entire network could go down
    - The use of a centralized controller in SDNs creates a real target for attackers
      - SDN Types
        - **Open SDN**

        - An open-source variant of software defined networking
    - **Hybrid SDN**
        - Employs traditional and SDN protocols to operate
    - **SDN Overlay**
        - Creates virtual connections between different endpoints to provide additional security benefits

- **Log Collection and Analysis**
    - Log review and analysis need to be routinely done
    - Logs contains details of your systems, device, applications etc.
    - Logs are not always enabled by default



    - Logs should be encrypted and use least privilege to protect logs and their data
    - When using the cloud to store your data ensure proper configuration of blob storage
    - Most Cloud services provide detailed log services
        - Third party system example, SPLUNK
            - Can be used to consolidate logs across all cloud platforms
            - It is a SaaS

- Search, Analyze and visualize machine generated data.
- Singles aggregation and analysis platform

- **Cloud Access Security Broker (CASB)**
  - Mediates user access to cloud services across all devices
    - **CASB Vendor examples:**
      - Blue Coat Proxy
      - Skyhigh Networks
      - Forcepoint
    - **CASB Advantages:**
      - Single sign-on authentication
      - Scan malware a rogue device detection
      - Users and resource activity monitoring
      - Data exfiltration mitigation
  - Provide visibility into how clients use cloud services
    - CASB are implemented in 3 different ways:
      - **Forward proxy**
        - Forwards all user traffic to the cloud network if they comply with the organization's policy
        - Inspects all traffic in real time could degrade network performance
        - May be evaded by users
      - **Reverse proxy**
        - Directs traffic to the cloud services if it complies with the organization's policy
        - Only works if the application supports reverse proxy
      - **API**
        - Uses the broker's connections between the cloud service and the cloud consumer to send or receive the information requested
  - Dependent on the API supporting the functions that your policies demand

- **Cloud Misconfigurations**
  - **Insecure APIs**
    - Always use an encrypted channel like HTTPS using SSL or TLS
  - **Improper key management**

        - Keys are used for things like cryptography, authentication and authorization to make our systems more secure
    - **Improper logging and monitoring**
        - When dealing with a software as a service product, you are not going to have any ability to access log files or monitoring tools for that software
    - **Unprotected storage**
        - The most commonly misconfigured ones are buckets and blob
            - A container cannot be nested inside of another container
    - **Cross-Origin Resource Sharing (CORS) Policy**
        - Instructs the browser to treat requests from nominated and listed domains as safe

Operational Technologies

Objectives 3.3

- **OBJ 3.3**: Explain security considerations impacting specific sectors and operational technologies

- **Embedded Systems**
  - Network of appliances and personal devices equipped with sensors, software, and network connectivity
  - Ensure they do not cause interference
  - They should be properly secured
  - These devices should be placed on a separate network
  - Building Automation and Control Network (BACnet)
    - Includes an application, network, and media access layer and can be run over other Layer 2 protocols.
    - **BACnet/IP**
      - Allows support for Internet protocol and routing over traditional business networks
        - **IP video system**
          - QoS
          - Bandwidth
          - Upfront cost
          - Logically separated
        - **4 IoT categories**
          - Hub and control systems
          - Smart devices
          - Wearables
          - Sensor
    - **Microcontrollers**
      - Can perform sequential operations from a dedicated instruction set
      - Field Programmable Gate Array (FPGA)
        - Like a microcontroller but the structure is not fully set at the time of manufacture
    - **System on a chip (SoC)**

        - Contains all the components of a computer system on a single chip

- **ICS and SCADA**
    - **Operational Technology (OT)**
        - Designed to implement an industrial control system rather than business and data networking systems
            - Technology that interacts with the real world
    - **Industrial Control System (ICS)**
        - Provides the mechanisms for workflow and process automation by using embedded devices
            - Interconnected ICSs create a distributed control system (DCS)
    - **Fieldbus**
        - Links different programmable logic controllers together
    - **Programmable Logic Controller (PLC)**
        - Enables automation in assembly lines, autonomous field operations, robotics, and other applications
    - **Human-Machine Interface (HMI)**
        - Input and output controls on a PLC that allow a user to configure and monitor the system
    - **Ladder Logic**
        - Programming language entered into the system through the creation of a graphical diagram used in the PLCs
    - **Data Historian**
        - Aggregates and catalogs data from multiple sources within an ICS by collecting all the event generated from the control loop
    - **Supervisory Control and Data Acquisition (SCADA)**
        - A type of ICS that manages large-scale, multiple-site devices and equipment spread over a geographic region from a host computer
            - Gathers data from and manage plant devices and equipment with embedded PLCs

- **ICS Protocols**
    - **Controller Area Network (CAN)**
        - Designed to allow communications between embedded programmable logic controllers
            - On-Board Diagnostic Module v2 (OBD-II)

        - CAN bus protocol operates like an ethernet network
    - **Modbus**
        - Gives control servers and the SCADA host the ability to query and change configurations of each PLC over a network
        - Modbus looks and functions differently than TCP/IP does
        - Originally known as Modbus RTU and was run over fieldbus networks
    - **Data Distribution Service (DDS)**
        - Provides network interoperability and facilitates the required scalability, performance, and QoS features
    - **Safety Instrumented System (SIS)**
        - Returns an industrial process to a safe state after a predetermined condition was detected
        - Reduces the severity of an emergency by taking quick action

- **Industries and Sectors**
    - **Energy**
        - Focuses on power generation and distribution
    - **Industrial**
        - Includes the mining and refinement of raw materials, including hazardous high heat and pressure processes, presses, centrifuges, and pumps
    - **Manufacturing**
        - Includes the creation of components and assembling them into finished products
    - **Logistics**
        - Focuses on the movement of materials and goods by using embedded technology to control the automated transport and lift systems, as well as embedded sensors for tracking of cargo containers
    - **Facilities**
        - Focuses on site and building management systems. This includes the operating of HVAC systems, lighting systems, and security systems
    - **Healthcare**
        - Focuses on patient health devices, medical equipment, supply management, and building management in hospital and other care facilities
    - **ICS and SCADA are considered defenseless systems**
        - Isolated networks
            - IDS/IPS

- Change control
- Least privilege

- **Information Sharing and Analysis Center (ISAC)**
  - Focuses on sharing sector-specific threat intelligence and security best practices among its members
- **Critical Infrastructure**
  - Security
  - Economic security
  - Public health and safety

Chemical	Financial services
Commercial facilities	Food and agriculture
Communications	Government facilities
Critical manufacturing	Healthcare and public health
Dams	Information technology
Defense industrial base	Nuclear reactors, materials, and waste sector
Emergency services	Transportation systems
Energy	Water and wastewater systems

Hashing and Symmetric Algorithms

Objectives 3.6

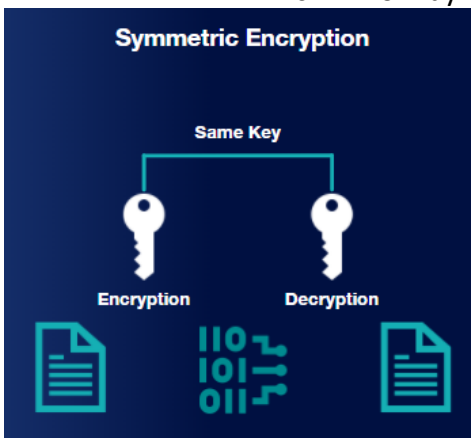
- **OBJ 3.3**: Given a business requirement, implement the appropriate cryptographic protocols and algorithms

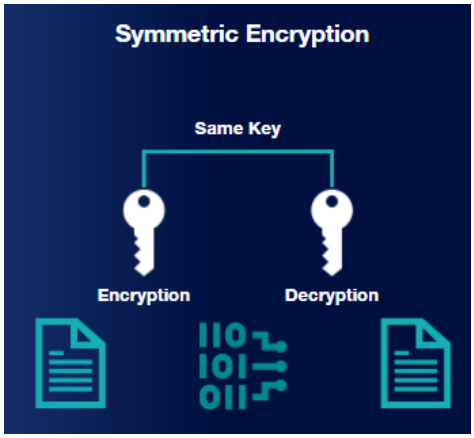
- **Hashing**
  - Takes an arbitrary length string as its input and transforms it into a fixed-length string as its output
    - The output will always be a fixed length
    - The same input will always generate the same output every single time
    - The output of the hashing function cannot be used to recreate the input
  - **Collision**
    - Occurs when the same message digest is created by two different inputs
  - **Message Digest Algorithm (MD5)**
    - Creates a 128-bit hash value
  - **Secure Hash Algorithm v1 (SHA-1)**
    - Uses a 160-bit hash digest
  - **SHA-2**
    - Includes SHA-224, SHA-256, SHA-384, and SHA-512
  - **SHA-3**
    - Uses 120 rounds of computations to create the message digest for each unique file by default
  - **RIPEMD**
    - Can generate outputs of 128-bits, 160-bits, 256-bits, and 320-bits

- **Message Authentication**
  - **Message Authentication Code**
    - Confirms the stated identity of the sender and provides integrity of the message without the need to use any other means
  - **Hash-Based (HMAC)**
    - Combines a cryptographic hash of the message with a secret key
    - Reduces collisions due to the addition of unique outputs
      - HMAC-MD5 or HMAC-SHA
  - **Cipher Block Chaining (CBC-MAC)**
    - Utilizes a block-cipher encryption method

- **Cipher-Based (CMAC)**
  - Works like CBC-MAC but utilizes AES or 3DES for encryption
- **Poly1305**
  - Provides increased speed and efficiency by utilizing alternative encryption algorithms
    - ChaCha20
    - Salsa20

- **Symmetric Algorithms**
  - **Encryption**
    - Converts information or data (plaintext) into an alternative form (ciphertext)
      - **Hashing**
        - One-way function
      - **Encryption**
        - Two-way function





  - Shared secret keys cannot promise non-repudiation
  - Symmetric encryption is 100 to 1000x faster than asymmetric encryption

- **Stream Ciphers**
  - **Steam Cipher**
    - Combines a stream of plaintext bits or bytes with a pseudorandom stream initialized by a secret key
    - Utilizes keystream generators to create a bit stream
    - Created using an initialization vector and a static key value
      - Has low error rate

        - Symmetric
        - Cheaper to utilize
    - **Confusion**
        - Drastically changes the data from its input to its output
    - **Diffusion**
        - Changes many characters of the output when a single character of the input was changed
    - **RC4**
        - Rivest Cipher
        - 40-bits up to 2048-bits
        - Considered to be weak stream cipher in modern networks
    - **Salsa20**
        - Considered fast and was released as a public domain implementation
    - **ChaCha**
        - Adopted by Google and combined with the Poly1305 MAC algorithm

- **Block Ciphers**
    - **Block Cipher**
        - Breaks input into fixed-length blocks of data and then performs encryption on each block
            - Easy implementation
            - More secure
            - Confusion/diffusion
                - **Confusion**
                    - Drastically changes the data from its input to its output
                - **Diffusion**
                    - Changes many characters of the output when a single character of the input was changed
    - **Digital Encryption Standard (DES)**
        - Uses a 64-bit key with 8 bits dedicated to parity
    - **Triple DES (3DES)**
        - Uses three 56-bit keys but is three times slower than DES
    - **Advanced Encryption Standard (AES)**
        - Can be used with 128-bit, 192-bit, or 256-bit blocks
        - AES is the federal government's standard for use on sensitive but unclassified information

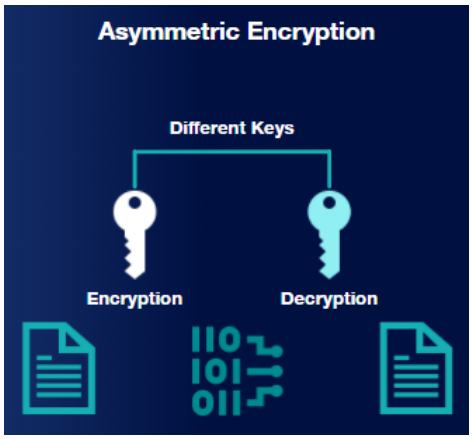
- **International Data Encryption Algorithm (IDEA)**
  - Uses a 128-bit key and is faster and harder to break than DES, but not as widely used as AES
- **Carlisle Adams and Stafford Tavares (CAST)**
  - Replaces IDEA in the PGP suite and its replacement, the GNU Privacy Guard suites
    - CAST-128
    - CAST-256
- **Skipjack**
  - Uses an 80-bit key to encrypt 64-bit blocks
- **Blowfish**
  - Uses 32-bit to 448-bit encryption key to encrypt 64 bits of data
- **Twofish**
  - Uses a 128-bit, 192-bit, or 256-bit encryption key to encrypt 128-bit blocks
- Rivest Ciphers (R1 through R6)
  - **RC5**
    - Uses key sizes up to 2048 bits
  - **RC6**
    - Uses a 128-bit block size and supports 128-bit, 192-bit, and 256-bit key sizes
    - Each symmetric block encryption algorithm operates using different modes of operation

Asymmetric Algorithms

Objectives 3.6

- **OBJ 3.3**: Given a business requirement, implement the appropriate cryptographic protocols and algorithms

- **Using Asymmetric Algorithms**



  - Ensures confidentiality, integrity, authentication, and non-repudiation
  - Ensure confidentiality by encrypting data with the receiver's public key
  - Ensure authentication by encrypting data with the receiver's private key
  - **Digital Signature**
    - Creates a hash digest based on the message being sent and then encrypts it using the sender's private key
    - Asymmetric encryption is 1000x slower than a symmetric algorithm
  - **Key Agreement and Exchange**
    - The process of sending a secret symmetric key using an asymmetric algorithm
  - **Diffie-Hellman (DH)**
    - Relies on a complicated math problem using discrete logarithms that utilize a common secret
      - Logjam
      - On-path
  - **Elliptic-Curve Diffie-Hellman (ECDH)**
    - Uses math based on the shape of elliptic curves

- **Rivest, Shamir, Adleman (RSA)**
  - Uses the difficulty of factoring the product of two large prime numbers to protect its public and private key pairs
  - Can support key sizes between 1024-bit and 4096-bit
- **Digital Signature Algorithm (DSA)**
  - Federal standard for digital signatures based on module exponentiation and discrete logarithm problems
- **El Gamal**
  - Utilizes discrete logarithms for its key strength and was used for key exchange, encryption, and digital signatures
  - DSA is faster at generating digital signatures but slow at verifying them
- **Elliptic Curve Cryptography (ECC)**
  - Relies on an elliptic curve's size to define the keys
- **Elliptic Curve Digital Signature Algorithm (ECDSA)**
  - Uses the power of elliptic curves to provide security

- **SSL/TLS and Cipher Suites**
  - **SSL/TLS**
    - Creates a secure connection to send data over an untrusted network
      - Secure Sockets Layer (SSL)
        - SSL
        - SSL 2
        - SSL 3
    - Should not be utilized due to its weakness and vulnerabilities
    - Outdated and should never be utilized
  - **Transport Layer Security (TLS)**
    - Utilize at least TLS 1.2 or above, preferably TLS 1.3
    - Newer and more secure
  - **Cipher Suite**
    - Defines the algorithm supported by the client and server when requesting to use encryption and hashing
  - As a cybersecurity professional, you need to understand how to read one of these cipher suites

- **S/MIME and SSH**
  - **Secure/Multipurpose Internet Mail Extensions (S/MIME)**
    - Allows non-text-based emails to pass securely over the Internet

- Uses the public key cryptography standards (PKCS)
- S/MIME can encrypt emails and their contents, including malware

- **Secure Shell (SSH)**
  - Allows remote access to another computer or server through a secure encrypted tunnel
    - SSH requires a server (daemon) to be run on one device and a client on another device
    - SSH can also be used as an encrypted tunnel for other protocols
      - **Host Key Pair**
        - Used to identify the SSH server
      - **User Key Pair**
        - Used by the client to login to the SSH server
  - Use a good SSH key management solution or rely on PKI infrastructure
    - SSH 1
    - SSH 1.5
    - SSH 2

- **Extensible Authentication Protocol (EAP)**
  - Replaces some of the older authentication protocols like PAP and CHAP
    - **Password Authentication Protocol (PAP)**
      - Provides authentication but the user credentials are not encrypted during transit
    - **MS-CHAP**
      - Microsoft's proprietary version of CHAP
  - Uses mechanisms of authentication including simple passwords, digital certificates, and PKI
    - **EAP-MD5 CHAP**
      - Utilizes simple passwords and the challenge handshake authentication process to provide remote access authentication
    - **EAP Transport Layer Security (EAP-TLS)**
      - Uses public key infrastructure with a digital certificate being installed on both the client and the server
  - EAP-TLS uses mutual authentication
    - **Protected EAP (PEAP)**
      - Uses server certificates and Microsoft's Active Directory databases to authenticate a client's password
        - CHAP v2

        - Generic token card
    - **EAP Tunnel Transport Layer Security (EAP-TTLS)**
        - Requires a digital certificate on the server and a password on the client for its authentication
    - **EAP Flexible Authentication via Secure Tunneling (EAP-FAST)**
        - Uses a protected access credential to establish mutual authentication between devices
  - Use EAP-TLS which uses mutual authentication

- **IP Security (IPSec)**
  - Provides authentication and encryption of data packets to create a secure and encrypted communication path between two computers

Protection	Method
Confidentiality	Using data encryption
Integrity	Ensuring data is not modified in transit
Authentication	Verifying parties are who they claim to be
Anti-Replay	Checking sequence numbers on all packets prior to transmission

  - **Main Mode**
    - Conducts three two-way exchanges between the peers, from the initiator to the receiver

First Exchange	Agrees upon which algorithms and hashes will be used to secure the IKE communications throughout the process
Second Exchange	Uses a Diffie-Hellman exchange to generate shared secret keying material so that the two parties can prove their identities
Third Exchange	Verifies the identity of the other side by looking at an encrypted form of the other peer's IP address

        - Authentication methods used
        - Encryption and hash algorithms used
        - Diffie-Hellman groups used
        - Expiration of the IKE SA
        - Shared secret key values for
        - the encryption algorithms
    - **Aggressive Mode**
        - Uses fewer exchanges, resulting in fewer packets and faster initial connection than main mode
            - Diffie-Hellman public key
            - Signed random number
            - Identity packet
                - Negotiate the IPSec SA parameters
                - protected by an existing IKE SA
                - Establish IPSec SA
                - Periodically renegotiate IPSec SAs to maintain security
                - Perform additional Diffie-Hellman exchanges, if needed
    - **Quick Mode**
        - Only occurs after IKE already established the secure tunnel in Phase 1 using either main or aggressive mode
            - Diffie-Hellman Key Exchange

    - Allows two systems that don't know each other to be able to exchange keys and trust each other
        - PC1 sends traffic to PC2 and then RTR1 initiates creation of IPSec tunnel
        - RTR1 and RTR2 negotiate Security Association (SA) to form IKE Phase 1 tunnel (ISAKMP tunnel)
        - IKE Phase 2 tunnel (IPSec tunnel) is negotiated and set up
        - Tunnel is established and information is securely sent between PC1 and PC2
        - IPSec tunnel is torn down and the IPSec SA is deleted
  - **Transport Mode**
    - Uses packet's original IP header and used for client-to-site VPNs
    - By default, maximum transmission unit (MTU) size in most networks is 1500 bytes
  - **Tunneling Mode**
    - Encapsulates the entire packet and puts another header on top of it
    - For site-to-site VPNs, you may need to allow jumbo frames
      - **Authentication Header (AH)**
        - Provides connectionless data integrity and data origin authentication for IP datagrams and provides protection against replay attacks
      - **Encapsulating Security Payload (ESP)**
        - Provides authentication, integrity, replay protection, and data confidentiality
    - In transport mode, use AH to provide integrity for the TCP header and ESP to encrypt it
    - In tunneling mode, use AH and ESP to provide integrity and encryption of the end payload

- **Elliptic Curve Cryptography (ECC)**
  - A form of public key cryptography based upon the algebraic structure of elliptic curves over finite fields
  - Six times more efficient than the RSA algorithm
  - Provides faster key agreement
    - **Elliptic Curve Diffie-Hellman**

        - ECC version of the popular Diffie-Hellman key exchange protocol
    - **Elliptic Curve Diffie-Hellman Ephemeral**
        - Uses a different key for each portion of the key establishment process inside the Diffie-Hellman key exchange
    - **Elliptic Curve Digital Signature Algorithm**
        - Used as a public key encryption algorithm by the US Government in their digital signatures under the name Digital Signature Algorithm or DSA
            - Elliptic Curve Cryptography key sizes
                - **P256**
                - **P384**
  - Part of NSA's Commercial National Security Algorithm Suite (CNSA)
  - ECC is more efficient and requires less processing power

- **Forward Secrecy**
  - Assures the session keys will not be compromised even if the long-term secrets used in the session key exchange have
  - A compromised private key could cause an attacker to decrypt secure messages
  - Forward secrecy uses frequently changing unique session keys
    - Simultaneous Authentication of Equals (SAE)
        - A secure password-based authentication and password authenticated key agreement that relies on forward secrecy
            - AP and client use a public key system to generate a pair of long-term keys
            - AP and client exchange a one-time use session key
            - AP sends client messages and encrypts them using the created session key
            - Client decrypts received messages using the same one-time use session key
    - Process repeats for each message being sent, starting at Step 2

- **Authenticated Encryption with Associated Data (AEAD)**
  - Checks the integrity and authenticity of the data it is encrypting
    - Authenticated Encryption with Associated Data
        - Checks the integrity and authenticity of associated data that is not encrypted
  - Advanced Encryption Standard in Galois/Counter Mode (AES-GCM)

- Checks the integrity and authenticity of the plaintext message being sent and received

- **Key Stretching**
  - Increases the security of a potentially weak key by increasing its effectiveness to resist a brute force attack
  - Simply increases the time to brute force a password or key
    - Password-Based Key Derivation Function 2 (PBKDF2)
      - Applies a pseudorandom function such as the HMAC to the inputted password or passphrase
        - **PBKDF2-HMAC-SHA256**
          - 310,000 iterations
        - **PBKDF2-HMAC-SHA512**
          - 120,000 iterations

- **Bcrypt**
  - A password-hashing function designed to conduct stretching using a salt
  - Resistant to rainbow table attacks
    - **Salting**
      - Adds random data into a one-way cryptographic hash
      - Defends against attacks that use precomputed tables
      - Doesn't have any negative effects on users
      - Salts are pseudorandom

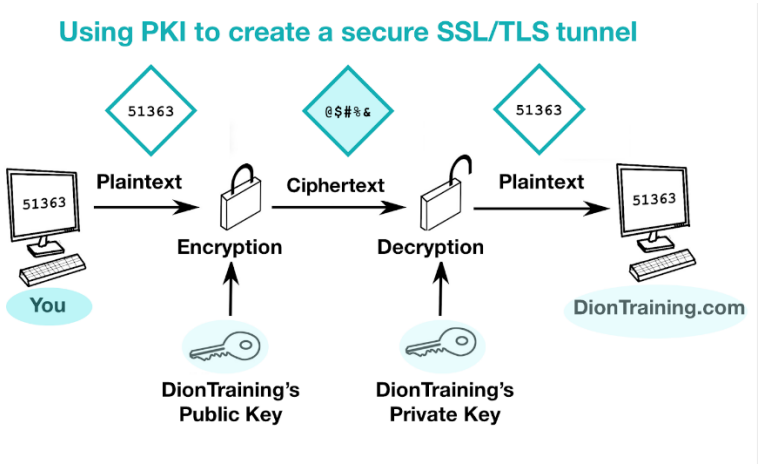
Public Key Infrastructure

Objectives 3.5 and 3.7

- **OBJ 3.5**: Given a business requirement, implement the appropriate PKI solution
- **OBJ 3.7**: Given a scenario, troubleshoot issues with cryptographic implementations

- **PKI Components**

- **Public Key Infrastructure (PKI)**
  - Software, services, and hardware that support the generation of digital certificates and capabilities of public-key encryption
  - Using PKI to create a secure SSL/TLS Tunnel



  - **Public Key Infrastructure**
    - System that creates and manages key pairs
  - **Public Key Cryptography**
    - Encryption and decryption process using key pairs

- **Certificate Authority (CA)**
  - Issues and guarantees signed digital certificates
  - A CA can be either private or public
    - Provide certificate services to users
    - Ensure validity of certificates and the identities of those applying for a certificate

- Establish trust in the CA from users, government, regulatory authorities, and enterprises
- Manage servers and repositories that store and administer the certificates
- Perform key and certificate lifecycle management, from generation to revocation

- **Certificate Chaining (Chain of Trust)**
  - Validates a certificate by tracing each CA that signs the certificate

- **Registration Authority (RA)**
  - Accepts requests for digital certificates and performs additional steps to validate an authorization

- **Certificate Signing Request (CSR)**
  - A Base64 ASCII file sent to a CA containing the information it needs to create a certificate
    - Organization info

    - Public key
    - Key type and length

- **Digital Certificates**
  - A digitally signed electronic document that bind a public key with a user's identity
  - Requests a digital certificate from a registration authority (RA)
  - RA requests identifying information from the user and forwards the certificate request to the certificate authority (CA)
  - CA creates the digital certificate, including the user's public key and their identity information, and then passes it to the user.
  - CA maintains a publicly accessible copy of the user's public key too
    - **X.509**
      - Standard in the public key infrastructure

- Different types of Digital certificates
  - General Purpose or Domain Validation known as DV
  - Granted to prove the ownership of a particular domain
  - Extended Validation or EV
  - Check the subject's legal identify and control over the domain or software being signed
    - **Wildcard certificates**
      - Allow all of the subdomains to use the same public key certificate and have it displayed as valid
      - If one of your servers is compromised and the certificate needs to be revoked
      - Wildcards can only be used for a subdomain of a domain name, not for a different domain name
    - **Load Balancer or Content Switch**
      - allows you to create a single wildcard certificate that will protect any number of subdomains being delivered
    - **Single-sided Certificate**
      - Does not require to have your own digital certificate to be authenticated back
    - **Dual-sided Certificate**
      - Requires twice the processing power on the server
  - **X.690**
    - Know as BER, CER, and DER
      - **BER**

- The Basic Encoding Rules and is the original ruleset governing the encoding of data structures for certificates

- **CER**
  - The Canonical Encoding Rules which is a restricted version of the BER that only allows the use of only one encoding type
- **DER**
  - The Distinguished Encoding Rules, which is another restricted version of the BER and only allows one encoding type and has more restrictive rules for length, character strings, and how the particular elements of a digital certificate are stored
    - **.pem format**
      - Used for Privacy-enhanced Electronic Mail and uses the DER encoding method. Sometimes, this is also stored as a .cer, .crt or .key file
    - **.p12 format**
      - Used to store a server certificate, intermediate certificate, and private key in one encrypted file
    - **.pfx file**
      - The Personal Information Exchange and is used by Microsoft for release signing. This file contains both the private and public keys in it
    - **.p7b file**
      - Used as the basis for S/MIME (secure email) and single sign on. It is called the P7B because it is based on PKCS #7

- **Using Digital Certificates**
  - **Client Authentication**
    - Used by a server to verify a connection request comes from a preauthorized endpoint
  - **Server Authentication**
    - Used by a client device to verify a server as genuine and not a forgery
  - **Cross-Certification**
    - A trust relationship that allows CAs to validate the digital certificates from each other's certificate authority
    - An attacker can access every resource a user has access to
  - **802.1x**
    - Authenticates each network device attempting to connect to a LAN/WLAN
  - **Digital Signature**
    - Created by hashing the file then taking the resulting hash digest and encrypting it with a user's private key from their digital certificate
  - **Code Signing**
    - Uses digital signature to ensure the source and integrity of a programming code

- **Trust Models**
  - **Trust Model**
    - Informs applications how to decide on the legitimacy of a digital certification
  - **Single Certificate Authority**
    - Issues, manages, and validates certificates
  - **Hierarchical**
    - Requires a centralized root node as the starting point for all trust in the PKI system
      - **Root CA**
        - A single point of failure
  - **Cross-Certification**
    - Establishes a trust relationship between two different Cas
  - **Bridge Certificate Authority**
    - Supports PKI applications across various enterprises
  - **Hybrid**
    - Combines two or more trust models
  - **Trusted Providers**
    - A set of root CAs that are trusted to validate identity

- **Certificate Profile**
  - A combination of the certificates used for digital signing

- **Certificate Management**
  - **Generate**
    - Certificate requests
  - **Provision**
    - Certificate issuance
  - **Discover**
    - Certificate scanning and identification
  - **Inventory**
    - Certificate documentation
  - **Monitor**
    - Change identification
  - **Protect**
    - Technical controls
  - **Renew**
    - Replacement of expiring certificates
    - Incorporate automation instead of relying on manual intervention
  - **Revoke**
    - Revocation case identification
    - During revocation, the certificate is added to the CRL

- **Certificate Validity (CRL and OCSP)**
  - When a digital certificate is issued in the PKI system, it has a listed expiration data within the certificate
  - Digital certificates work the same basic way, in that they will automatically expire on a certain date, but they can also be revoked any time before their expiration by the certificate authority for a number of reasons
    - **Reasons for a revocation**
      - Cessation of Operation
      - CA Compromise
      - Key Compromise
      - Superseded
      - Unspecified
  - A digital certificate can also be suspended instead of revoked, if needed
  - A suspension can be reinstated, but a revocation cannot

        - **Certificate revocation list**
            - A full list of every certificate ever revoked by that certificate authority
        - **Validating a digital certificate**
            - Check the expiration date of the certificate
            - Use the Online Certificate Status Protocol, also known as the OCSP
                - **Online Certificate Status Protocol (OCSP)**
                    - A protocol that allows us to determine the revocation status of a digital certificate using its serial number

- **Protecting Web Traffic**
    - **Certificate pinning**
        - A method of trusting digital certificates that bypasses the certificate authority hierarchy and chain of trust to minimize on-path or man-in-the-middle attacks
        - The first method used to try and mitigate this vulnerability
    - **Certificate Stapling**
        - Allows a webserver to performance certificate status checking instead of the browser
        - This method resolves the issues of certificate pinning by having the webserver obtain a time-stamped OCSP response from the certificate authority
    - **HTTP Strict Transport Security (HSTS)**
        - The webserver is configured to notify web browsers that are connecting to it that they should only request the website using HTTPS and not HTTP
        - Prevents on-path or man-in-the-middle attacks by exploiting the HTTP website connection

- **Troubleshooting Certificates**
    - **Validity dates**
        - Each digital certificate is issued for a defined period of time, from its issuance to its expiration
    - **Wrong certificate types**
        - Certificates are created for different purposes
    - **Revoked certificates**

        - Once a certificate is revoked, it is invalidated and will appear on the certificate revocation list
    - **Incorrect names**
        - The Common Name, or CN, field on the digital certificate must match the fully qualified domain name of the system that is using that certificate
    - **Chain issues**
        - A certificate is only deemed valid if it is verified as valid all the way through the trust chain, from the user to the server to the subordinate or intermediate certificate authority up to the root certificate authority
    - **Self-signed certificates**
        - A digital certificate independently generated without using a CA
    - **Weak signing algorithms**
        - The hashing algorithms used by digital signatures can become weak or vulnerable as computers get more powerful and cryptanalysts find ways to exploit the algorithms
    - **Weak cipher suites**
        - Occurs when using an older encryption algorithm with a web server
    - **Incorrect permissions**
        - Occur when you are trying to register a new digital certificate for enrollment, but the template has incorrect permission causing an "operation failed" or "cannot enroll for this type of certificate" error
    - **Cipher mismatches**
        - Occurs when a web browser and server cannot support the same type of cipher

- **Troubleshooting Keys**
    - **Mismatched keys**
        - Used the wrong public/private key pair to decrypt the received data
    - **Improper key handling**
        - Ensure keys are properly secured during storage
    - **Embedded Keys**
        - Stored on specialized read-only cryptographic storage chips
    - **Rekeying**
        - Renegotiates a session key during communication
    - **Crypto Shredding**
        - Destroys a decryption key in order to destroy the data that the encryption protects

- **Cryptographic Obfuscation**
  - Transforms protected data into an unreadable format
- **Key Rotation**
  - Changes keys on a periodic basis to mitigate against the possibility of a brute force attack of an unidentified key breach
- **Compromised or exposed keys**
  - This means there is unauthorized access to a symmetric key or private key

Threat and Vulnerability Management

Objectives 2.1 and 2.3

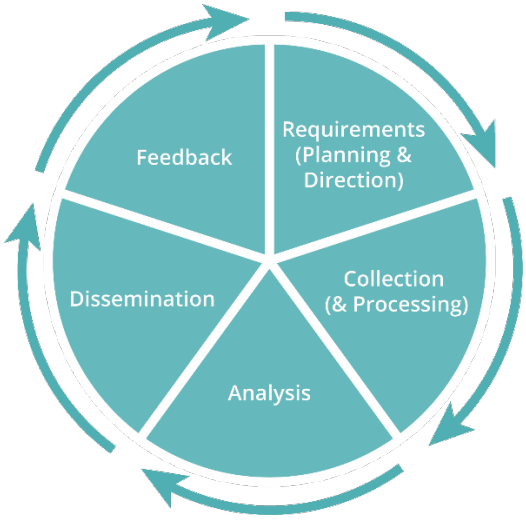
- **OBJ 2.1:** Given a scenario, perform threat management activities.
- **OBJ 2.3**: Given a scenario, perform vulnerability activities.

- **Threat Intelligence**
  - **Threat Intelligence**
    - A continual process used to understand the threats faced by an organization
    - Focused on evidence-based knowledge analysis
    - Threat intelligence provide us the:
      - Context
      - Mechanisms
      - Indicators
      - Implications
      - Actionable Information
  - **Types of Attacks**
    - Server-side attacks
    - Client-side attacks
      - Focus on targeting vulnerabilities in the client's applications
        - Device not hardened
        - No proper patches
        - Additional software
  - Types of Threat Intelligence
    - **Tactical**
      - Focused on the tactics, techniques, and procedures of a given threat actor
    - **Strategic**
      - Focused on the motivations, capabilities, or intentions of a given threat actor
    - **Operational**
      - Collected from the organization's own infrastructure and includes data from SIEM logs
        - **Threat Emulation**
          - Uses known TTPs to a real-world attack against a network

    - **Adversary Emulation**
        - Uses known adversary TTPs in a realistic way to mimic the actions of a specific threat actor or group

- **Threat Hunting**
    - **Threat Hunting**
        - Detects the presence of threats that have not been discovered by normal security monitoring
    - **Establishing a Hypothesis**
        - Derived from threat modeling and is based on potential events with higher likelihood and higher impact
    - **Profiling Threat Actors and Activities**
        - The creation of scenarios on how a potential attacker might attempt an intrusion as well as their objectives
        - Also uses tools for regular security monitoring and incident response
        - With threat hunting, we assume existing rules have failed
    - **Advisories and Bulletins**
        - Published by vendors and security researchers when new TTPs and vulnerabilities are discovered
    - **Intelligence Fusion and Threat Data**
        - Use of a SIEM and threat analysis platform to efficiently identify items of concern
            - Analyze network traffic
            - Analyze the executable process list
            - Analyze other infected hosts
            - Identify how the malicious process was executed

- **Intelligence Collection**
    - Security intelligence is a 5-step process



- **Requirements (Planning & Direction)**
  - Sets out the goals for the intelligence gathering effort
  - Figure out exactly what to collect and measure
  - Consider any potential constraints during collection
- **Collection (& Processing)**
  - Implemented by software tools like SIEMs and all data collected is saved and processed for later analysis
    - Consolidate
    - Aggregate
    - Correlate
- **Intelligence Feeds**
  - Provides information about ongoing attack campaigns that are being observed by threat researchers
    - DHS CISA AIS
    - Mandiant
    - FireEye
- **Open-Source Intelligence (OSINT)**
  - The use of publicly available information sources to collect and analyze data
- **Human Intelligence (HUMINT)**
  - The collection of intelligence through interactions with other people
- **Analysis**

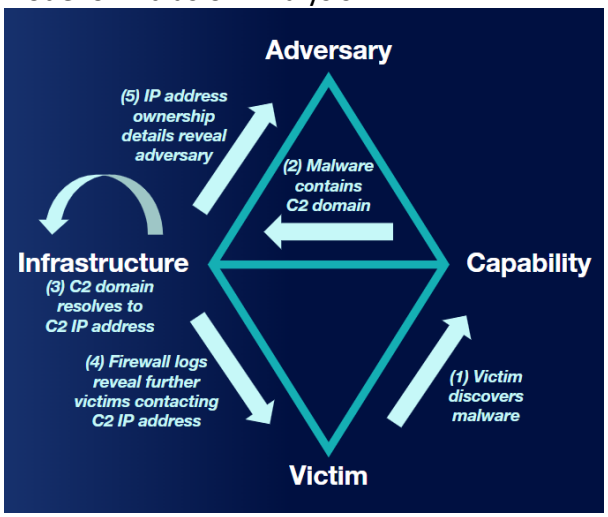
        - Performed using the given use cases and requirements from the initial requirements and planning phase
            - Automated analysis
            - Artificial intelligence
            - Machine learning
        - Three categories of collected data
            - Known good
            - Known bad
            - Unknown
        - Focus the analysis on answering the questions from the requirements phase
    - **Dissemination**
        - Publishing analysis results to consumers who need to act on the insights developed
    - **Feedback**
        - Clarifies requirements and improves the collection, analysis, and dissemination of information
            - Lessons learned
            - Measuring success
            - Modifying requirements

- **Threat Actors**
    - **Threat Actor**
        - Describes those who wish to harm networks or steal secure data
    - **Hacker vs cracker**
        - A hacker was simply a computer enthusiast, and not a criminal
        - Crackers were hackers with malicious intent, they were the criminals
            - Social media profiling
            - Social engineering
            - Network scanning
            - Fingerprinting
            - Service discovery
            - Packet capture
    - **Script Kiddie**
        - Uses other people's tools to conduct their attacks as they do not have the skills to make their own tools
        - Script kiddies often don't understand what they're doing

- **Insider Threat**
  - People who have authorized access to an organization's network, policies, procedures, and business practices
    - Data loss prevention
    - Internal defenses
    - SIEM search
- **Competitor**
  - A rogue business attempting to conduct cyber espionage against an organization
- **Organized Crime**
  - Focused on hacking and computer fraud to achieve financial gains
- **Hacktivist**
  - Politically-motivated hacker who targets governments or individuals to advance their political ideologies
- **Nation-State/ Advanced Persistent Threat (APT)**
  - A group of attackers with exceptional capability, funding, and organization with an intent to hack a network or system
  - Conducts highly covert hacks over long periods of time

- **Threat Management Frameworks**
  - **Lockheed Martin Cyber Kill Chain**
    - Describes the stages by which a threat actor progresses a network intrusion
  - **Reconnaissance**
    - Attacker determines the methods to use to complete the phases of the attack
    - Open source and passive information gathering techniques
  - **Weaponization**
    - Attacker is going to do couple payload code to enable access with exploit code to exploit a vulnerability on a target system
  - **Delivery**
    - Attacker identifies a vector to transmit the weaponized code to the target environment
  - **Exploitation**
    - Weaponized code is executed on the target system
  - **Installation**

        - Enables weaponized code to run a remote access tool and achieve persistence on the target system
    - **Command and Control (C2)**
        - Weaponized code establishes an outbound channel to a remote server
    - **Action on Objectives**
        - Attacker collects information from target systems and transfer it to a remote system or achieve other goals and motives
            - **6 Ds**
                - Detect
                - Deny
                - Disrupt
                - Degrade
                - Deceive
                - Destroy
        - **MITRE ATT&CK Framework**
            - Adversarial
            - Tactics
            - Techniques
            - &
            - Common
            - Knowledge
    - Diamond Model of Intrusion Analysis



- **Vulnerability Management Activities**

- **Vulnerability Assessment**
  - Defines, identifies, and classifies vulnerabilities within a system
    - What is the value of the information?
    - What is the threat the system is facing?
    - What is the mitigation that could be deployed?
  - Vulnerability assessments are only a snapshot in time
    - Credentialed vs non-credentialed
      - **Credentialed**
        - With username and password
      - **Non-Credentialed**
        - Without username and password
    - Agent vs agentless
      - **Agent-Based**
        - Installs local agents to perform the scans
      - **Agentless**
        - Relies on a centralized vulnerability scanner
    - Active vs passive
      - **Active**
        - Probes each individual target on the network
      - **Passive**
        - Relies on indirect methods
- **Criticality ranking**
  - Provides a standardized score associated with each vulnerability found
- **Advisory**
  - Provides specific information about an identified vulnerability
- **Bulletin**
  - Contains a listing of advisories across a wide range of products
- **News**
  - Can be useful as a tipper but does not contain enough details
- **Information Sharing and Analysis Centers (ISACs)**
  - Share sector-specific threat intelligence and security best practices among its members

- **Security Content Automation Protocol (SCAP)**
  - **Security Content Automation Protocol (SCAP)**
    - Standardizes the formatting and naming conventions used for software flaws, misconfigurations, and vulnerabilities

- **Open Vulnerability and Assessment Language (OVAL)**
  - An XML schema for describing system security states and querying vulnerability reports and information
- **Extensible Configuration Checklist Description Format (XCCDF)**
  - An XML schema for developing and auditing best-practice configuration checklists and rules
  - With XCCDF, scanning tools and automation can be used to check our systems
- **Asset Reporting Format (ARF)**
  - An XML schema for expressing information about assets, and the relationships between assets and reports
- **Common Configuration Enumeration (CCE)**
  - A scheme for provisioning secure configuration checks across multiple sources
  - Provides unique identifiers for different system configuration issues
- **Common Platform Enumeration (CPE)**
  - A scheme for identifying hardware devices, OSs, and applications
- **Common Vulnerabilities and Exposures (CVE)**
  - A list of records where each item contains a unique identifier used to describe publicly known vulnerabilities
- **Common Vulnerability Scoring System (CVSS)**
  - Provides a numerical score to reflect the severity of a given vulnerability

Rating	CVSS Score
None	0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

Vulnerability Assessments

Objectives 2.4

- **OBJ 2.4:** Given a scenario, use the appropriate vulnerability assessment and penetration testing methods and tools.

- **Penetration Test**
  - **Penetration Test (PenTest)**
    - Simulates an attack on a network, its systems, or applications
      - **Vulnerability Assessment**
        - Credentialed
      - **Penetration Test**
        - Non-credentialed
  - **Blind Test**
    - Provides the attackers with limited knowledge of the network and the devices that it contains
  - **Double-Blind Test**
    - Much like the blind test, except the defenders are not informed about when the attack may occur
  - **Target Test**
    - Both attackers and defenders have the maximum amount of knowledge about the network and its devices
  - **Unknown Environment Testing**
    - Provides attacker with no prior knowledge of the network
  - **Partially-Known Environment Testing**
    - Provides attacker with some prior knowledge of the network
  - **Known Environment Testing**
    - Provides attacker with complete knowledge of the network

- **PenTest Steps**
  1. Get permission and document information about the target network
  2. Gather information about the target through reconnaissance
  3. Enumerate the target to identify known vulnerabilities
  4. Exploit the network to gain user or privileged access
  5. Document the results of the test and report them to the organization

  - **Reconnaissance (Footprinting)**

        - Systematic attempt to locate, gather, identify, and record information about the target network or systems
    - **Enumeration (Fingerprinting)**
        - Scans a network to identify systems running, as well as available services and applications
            - **Reconnaissance**
                - Passive
            - **Enumeration**
                - Active and passive
        - The attacker gains more in-depth information about the systems during enumeration
    - Exploitations can be:
        - Client-side or remote exploitation
        - Social engineering
        - Unsecure/unpatched system vulnerabilities
        - Open wireless connections
        - Web application vulnerabilities
        - Backdoors
        - Trojans
        - Buffer overflows

- **PenTest Requirements**
    - Three major factors for any assessment
        - Time
        - Cost
        - Quality
    - **Scope of Work (SOW)**
        - Details the tasks to be performed which will include all the rules of engagement that will be followed
    - **Rules of Engagement (ROE)**
        - The ground rules both parties must abide by
            - Timeline
            - Location
            - Time restrictions
            - Transparency
            - Boundaries
            - Test Invasiveness

        - Refers to the type of actions you can perform on a target
        - Any limitations or constraints must be understood during the planning phase

- **Code Analysis**
    - **Types of Security Assessments**
        - Vulnerability assessments
        - Physical security
        - Malware analysis
        - Penetration testing
        - Internal and external audits
        - Self-assessments
        - Code reviews
    - **Static Analysis**
        - The analysis of computer software code that is performed without actually executing the program
        - Can be done manually or using automated tools
    - **Dynamic Analysis**
        - The analysis of computer software code that is performed while executing the program
    - **Side-channel Analysis**
        - An inspector of a system or software as it operates
    - **Reverse Engineering**
        - Process of analyzing the structure of a piece of hardware or software to reveal more about its functions
    - **Decompiler**
        - Specialized piece of software that displays the low-level programming language representation of the malware
    - **Debugger**
        - Specialized piece of software that runs the malware sample step-by-step through its program
        - Reverse engineering can also be used on hardware devices
    - **Software Composition Analysis**
        - The assessor inspects the source code to try to identify any open source component
    - **Fuzz Testing**

    - Form of dynamic analysis where the assessor uses a specialized toolset to purposely input or inject malformed data into an application
    - Can test large sample sets of data in a very short period of time

- **Protocol Analysis**
    - **Wireless Vulnerability Scanner**
        - It is used to identify the configuration and signal coverage of a given organization's wireless network
    - **Protocol Analyzer**
        - It is specific type of software that collects raw packets from the network
    - **Network Traffic Analyzer**
        - Samples the network packets and allows us to conduct flow analysis
    - **Port Scanner**
        - Used to discover what access points are open into a given host or server
    - **HTTP Interceptor**
        - Excellent tool when testing web applications that rely on the HTTP or HTTPS protocols

- **Analysis Utilities**
    - **SCAP Scanner**
        - Tool designed to use the SCAP to compare a target computer or software configuration and patch level against pre-determined settings
    - **Vulnerability Scanner**
        - Discovers security weaknesses in a host, system, or across the enterprise network
            - Critical
            - High
            - Medium
            - Low
            - Informational
    - **Exploitation tools and Frameworks**
        - Is a grouping of software that are used to exploit security holes in an enterprise network
        - These tools are used by both security analysts and attackers
        - The Browser Exploitation Framework Project
    - **Password Cracker**

- Used to attempt to break a user's password by using either brute force techniques or a dictionary attack

- **Dependency Management**
  - Tools are used to identify what dependencies are met on a given system for a piece of software or which libraries may be missing

Risk Reduction

Objectives 2.6

- **OBJ 2.6:** Given a scenario, use processes to reduce risk.

- **Deceptive Technologies**
  - **Deceptive Technology**
    - Any technology that appears to be legitimate target, but they do not contain any sensitive files or data
  - **Decoy File**
    - Contains data that would be appealing to an adversary, such as user credentials, email address, account numbers, or other sensitive data
  - **Honeypot**
    - Host or server that mimics a genuine system, is configured to monitor and log any interactions with this host or server
    - A honeypot can also install a honeynet
  - **Honeynet**
    - Contains a network of several honeypots in a tightly controlled and heavily monitored network
  - **Simulator**
    - A software application that is configured to simulate a common server or service
  - **Dynamic Network Configurations**
    - Allows to integrate your detection techniques with an automated network reconfiguration capability based on software-defined network
    - Observed malicious activity can quickly be put into quarantined environment

- **Security Data Analytics**
  - **Security Data Analytics**
    - Collects, aggregates, correlates, and analyzes large amounts of data to identify security incidents and perform threat detection
  - **Normalization**
    - Data reformatting or restructuring to facilitate indexing, searching, and analysis
  - **Processing Pipeline**
    - Method and sequence used to process the collected data

        - Was called data processing pipeline that uses batching
        - Data may be waiting a while before it reaches the centralized repository
    - **Indexing**
        - Minimizes number of disk accesses required when a query or search is being processed
    - **Searching**
        - Finds a given value in a list of values or data
        - Collecting everything is a waste of time, money, and resources
        - Identify what is important, and then only collect those
    - **Database Activity Monitoring (DAM)**
        - Identifies changes or specific activities within a database management system
            - **Interception-Based**
                - Client-server communication
            - **Memory-Based**
                - SQL statements
            - **Generation-Based Log-Based**
                - Transaction logs
            - Not designed to track responses to SQL queries
            - Route database traffic to the DAM before reaching the database
            - Data classification and discovery
            - Data loss protection
            - Data integrity
            - SQL query monitoring
            - Network sniffing
            - Memory scraping
            - Reading system tables
            - Analyzing DB audit logs

- **Preventative Controls**
    - **Antivirus**
        - Detects and removes virus infections
        - Ensure frequent updates to signature and scanning engine
    - **HIDS/HIPS**
        - Monitors system for unexpected behavior and drastic changes to the system state on a given endpoint

- **Immutable System**
  - Any workstation or server that is never modified after deployment
    - Lower cost
    - Faster deployment
    - Reduced errors
    - Less configuration changes
    - Less vulnerabilities
- **Hardening**
  - Reduces a system's attack surface and eliminates vulnerabilities
  - The less code or options available on a system, the less vulnerable it will be
- **Sandbox Detonation**
  - Identifies malicious actions using observed behavior for a suspicious file or program

- **Application Controls**
  - **Allow List**
    - What can be run
  - **Block List**
    - What cannot be run
  - **Unlicensed software can't get updates and can cause compliance issues**
  - **Ensure proper licensing for any installations on workstations and servers**
  - **Time of Check vs Time of Use (TOCTOU)**
    - Occurs when there is a change between when an app checks a resource and when the app uses the resource
      - Record transaction in the sales history
      - Find next available voucher in the inventory and assign to student
      - Copy voucher code to the voucher ledger
      - Mark voucher in the inventory as sold
      - Ensure to lock or block the state of critical elements until the app can complete their task
  - **Atomic Execution**
    - A task's capability to run with exclusive access to a resource

- **Security Automation**
  - **Script**
    - Automates the execution of tasks for or shell environment

- **Bash**
  - A scripting language and command shell for Unix-like systems that is the default shell for Linux and macOS
  - Scripts are constrained by the permissions assigned to them
- **cron daemon**
  - A background service that is used to manage scheduled tasks known as cron jobs
    - **crontab**
      - Controls the cron daemon
- **PowerShell**
  - Serves as an advanced command shell for Windows desktop and server systems
- **cmdlet**
  - Performs an action and returns a Microsoft .NET object to the next command in the pipeline
    - **Linux**
      - cron jobs
    - **Windows**
      - Task Scheduler
- **Windows Task Scheduler**
  - Allows for the creation of new tasks to run an application or script at a predefined time
- **Python**
  - A cross-platform scripting language that can operate on any operating system
  - Widely used by cybersecurity analysts and penetration testers

- **Physical Security**
  - **Detection Mechanisms and Detective Controls**
    - Security controls used during an event to find out whether something malicious may have happened
  - **Ultrasonic**
    - A type of surveillance camera that uses sound-based detection
    - Ensure adequate coverage of the critical areas
      - **Open** (General use)
      - **Confined (**Classified or sensitive)

Analyzing Vulnerabilities

Objectives 2.5

- **OBJ 2.5:** Given a scenario, analyze vulnerabilities and recommend risk mitigations

- **Race Conditions**
  - **Race Condition**
    - Occurs when a computer tries to race itself in the processing of certain data
    - Found where multiple threads attempt to write to a variable or object at the same memory location
  - **Dereferencing**
    - Occurs when the code attempts to remove the relationship between a pointer and the thing it points to
    - Race conditions often happen outside the normally logged processes in a system
  - **TOCTOU**
    - Occurs when there is a change between when an app checks a resource and when the app uses the resource
  - **Mutually Exclusive Flag (Mutex)**
    - Acts as a gatekeeper to a section of code so that only one thread can be processed at a time
  - **Deadlock**
    - Occurs when a lock cannot be removed from the resource
    - Properly design and test any locks or mutexes

- **Buffer Overflows**
  - **Buffer Overflow**
    - Occurs when a process stores data outside the memory range allocated by the developer
  - **Buffer**
    - A temporary storage area that a program uses to store data
    - Over 85% of data breaches were caused by a buffer overflow
  - **Stack**
    - Reserved area of memory where the program saves the return address when a function call instruction is received
  - **"Smashing the Stack"**

- Occurs when an attacker fills up the buffer with NOP instructions

- **Non-Operation (NOP) Instruction**
  - Tells the system to do nothing and simply go to the next instruction
  - Maintain a good patch management program
  - Always use secure coding practices
    - **Boundary checking**
    - **Input validation**
  - Use Address Space Layout Randomization
    - **Address Space Layout Randomization (ASLR)**
      - Prevents an attacker's ability to guess where the return pointer for a non-malicious program has been set to call back to
  - Use Data Execution Protection
    - **Data Execution Protection (DEP)**
      - Blocks applications that attempt to run from protected memory locations
      - Executable code stored in the user data location will be marked as non-executable
- **Integer Overflow**
  - Occurs when a computed result from an operation is too large to fit into its assigned variable type for storage
  - Integer overflows and buffer overflows can lead to arbitrary code execution, and in turn, privilege escalations

Integer	Bounds
8-bit, signed	256 (-128 to +127)
8-bit, unsigned	256 (0 o 255)
16-bit	65,535
32-bit	4.2 million
64-bit	18 quadrillion

    - Size variable bounds appropriately to avoid wasting resources

- **Authentication and References**
    - **Broken Authentication**
        - Insecure authentication mechanisms that can allow an attacker to gain entry
            1. Utilize multi-factor authentication
            2. Never use default credentials
            3. Verify passwords are strong and not found on published password exploitation lists
            4. Use limits or delays to slow failed login attempts and brute force attempts
            5. Use server-side session management and long and randomized session identifiers
            6. Never pass a session identifier as a URL parameter
            7. Implement session timeouts and expiring session identifications
    - **Insecure Direct Object Reference**
        - Used to manipulate URLs to gain access to a resource without requiring proper authentication
            1. Always use secure coding practices
            2. Always implement proper access control techniques to verify a user's authorization

- **Ciphers and Certificates**
    - **Cipher**
        - An individual algorithm used for the encryption or decryption of data
            - Key exchange
            - Digital signature
            - Bulk encryption
            - Hashing algorithm
    - **Cipher Suite**
        - Defines the algorithm supported by the client and server when requesting to use encryption and hashing
        - As a cybersecurity professional, you need to understand how to read one of these cipher suites
            - Validity dates
            - Wrong certificate types

- Incorrect names
- Revoked certificates
- Self-signed certificates
- Chain issues
- Weak signing algorithms
- Weak cipher suites
- Cipher mismatches
- Incorrect permissions

  - Device and user certificates are issued for different purposes
  - The CN field on the digital certificate must match the system's FQDN
- **Self-Signed Certificate**
  - A digital certificate independently generated without using a CA
- **Weak Cipher Suite**
  - Occurs when using an older encryption algorithm with a web server
- **Incorrect Permission**
  - Occurs when trying to register a new digital certificate but the template has incorrect permissions
- **Cipher Mismatch**
  - Occurs when a web browser and server cannot support the same type of cipher

- **Improper Headers**
  - Cross site request forgery
  - Cross site scripting
  - Downgrade attack
  - Cookie hijacking
  - User impersonation
  - Clickjacking
  - **HTTP Strict Transport Security (HSTS)**
    - Allows a web server to notify web browsers to only request using HTTPS and not HTTP
  - **HTTP Public Key Pinning (HPKP)**
    - Allows HTTPS websites to resist impersonation by attackers using mis-issued or fraudulent certificates
  - **X-Frame-Options**
    - Prevents clickjacking from occurring

- **X-XSS-Protection**
  - Enables cross site scripting filter in the web browser
- **X-Content- Type-Options**
  - Prevents the browser from interpreting files as something other than what they are
- **Content-Security-Policy (CSP)**
  - Impacts how web browsers render pages
- **X-Permitted-Cross-Domain-Policies**
  - Sends a cross-domain policy file to the web client and specifies if the browser has permission to handle data across domains
- **Referrer-Policy**
  - Governs which referrer information should be included with requests made
- **Expect-CT**
  - Indicates browsers to evaluate connections to the host emitting the header for Certificate Transparency compliance

- **Software Composition**
  - **Software Composition Analysis**
    - A process by which software can be analyzed for open-source components
    - "A vulnerability in a third-party dependency becomes a vulnerability in your application"
    - When using third-party dependencies, you are responsible for the code you write and did not write
      - Apache Struts
      - Microsoft .NET
      - Ramaze
      - Ruby on Rails
      - Hibernate
      - Django
      - web.py
      - Twisted
  - **Poor Exception Handling**
    - Occurs when a program is not written to anticipate problems or errors
  - **Security Misconfiguration**

        - Any issue related to poorly implemented or documented security controls
    - **Weak Cryptography Implementation**
        - Occurs when an out-of-date algorithm or cipher is being used in a modern system
        - Utilize a well-known and documented encryption standard
    - **Information Disclosure**
        - The act of stealing information from an application or during the communication process between two applications
            - **End of Life**
                - No longer sold
            - **End of Support**
                - No longer updated
    - **Code Injection**
        - An exploitation technique that runs malicious code with identification of a legitimate process
        - Ensure applications provide input and output validation
    - **Regression Issues**
        - Occur when a source code is changed which may have introduced a new vulnerability or have broken some existing functionality
    - **Regression Testing**
        - Validates any software change does not produce any unintended consequences

- **Vulnerable Web Applications**
    - Client-side processing puts the load on the end user's machine instead of the server
    - JavaScript Object Notation/Representational State Transfer (JSON REST)
    - **Represented State Transfer (REST)**
        - A client/server model for interacting with content on remote systems over HTTP
    - **JavaScript Object Notation (JSON)**
        - A text-based message format used with RESTful web service
            - **REST and JSON**
                - Mobile devices
            - **SOAP and XML**
                - Security/transactional services

- **Simple Object Access Protocol (SOAP)**
  - Used for exchanging structural information for web services
  - Conduct inspection and sanitization of inputs and outputs to the application
- **Browser Extensions**
  - Provides expanded functionality or features to a web browser
- **Asynchronous JavaScript and XML (AJAX)**
  - A grouping of related technologies used on the client side to create asynchronous web applications
  - AJAX is considered more secure than some other methods
- **Machine Code**
  - Basic instructions written in machine language that can be directly executed by the CPU
  - Specific to a type of processor and can only be run on the processor for which it was compiled
- **Bytecode**
  - An intermediate form of code produced by a compiler that can be translated into machine code

Attacking Vulnerabilities

Objectives 2.5

- **OBJ 2.5:** Given a scenario, analyze vulnerabilities and recommend risk mitigations

- **Directory Traversals**
  - **Directory Traversal**
    - Allows access to files, directories, or commands that may or may not be connected to the web document root directory
    - In a directory traversal, an attacker tries to navigate upwards and out of the web document root directory
      - **Unix/Linux**
        - ../
      - **Windows running IIS**
        - ..\
    - Directory traversals may be used to access any file on a system with the right permissions
    - Attackers may try to use **%2E%2E%2F** instead of **../**
  - **File Inclusion**
    - Allows an attacker to download a file from an arbitrary location or upload an executable or script file to open a backdoor
      - **Remote File Inclusion**
        - Executes a script to inject a remote file into the web app or the website
      - **Local File Inclusion**
        - Adds a file to the web app or website that already exists on the hosting server

- **Cross-Site Scripting (XSS)**
  - **Cross-Site Scripting (XSS)**
    - Injects a malicious script into a trusted site to compromise the site's visitors
    - Cross-site scripting (XSS) is a powerful input validation exploit
      1. Attacker identifies input validation vulnerability within a trusted website
      2. Attacker crafts a URL to perform code injection against the trusted website

3. The trusted site returns a page containing the malicious code injected
4. Malicious code runs in the client's browser with permission level as the trusted site

- XSS breaks the browser's security and trust model
  - **Non-Persistent XSS**
    - Happens once
  - **Persistent XSS**
    - Embedded code

- **Document Object Model (DOM) XSS**
  - Exploits the client's web browser using client-side scripts to modify the content and layout of the web page
  - DOM XSS runs with the logged in user's privileges of the local system

- **Cross-Site Request Forgery (CSRF)**
  - **Session Management**
    - Enables web applications to uniquely identify a user across several different actions and requests
  - **Cookie**
    - Text file used to store information about a user when they visit a website
      - **Non-Persistent**
        - Reside in memory
      - **Persistent**
        - Stored in browser cache
  - **Session Hijacking**
    - Disconnects a host and then replaces it with his or her own machine by spoofing the original host IP address
      - Session cookie theft
      - Nonrandom tokens
  - **Session Prediction**
    - Predicts a session token to hijack the session
    - Session tokens must be generated using non-predictable algorithm and must not reveal any info about the session's client
  - **Cross-Site Request Forgery (CSRF)**
    - Exploits a session that was started on another site and within the same web browser
      1. Ensure user-specific tokens are used in all form submissions

2. Add randomness and prompt for additional information for password resets
3. Require users to enter their current password when changing it

- **SQL Injections**
  - **Select**
    - Read
  - **Insert**
    - Write
  - **Delete**
    - Remove
  - **Update**
    - Overwrite
  - **Code Injection**
    - Inserts additional information or code through a data input form from a client to an application
  - **SQL Injection**
    - Injects an SQL query through the input form a client uses to send data to a web application
      - URL parameters
      - Form fields
      - Cookies
      - POST data
      - HTTP headers
  - Use input validation and sanitize any data received from users

- **XML Injections**
  - **Extensible Markup Language (XML)**
    - Used by web apps for authentication, authorization, and other types of data exchange
    - Conduct input validation and input sanitization of the data received
      - Spoofing
      - Request forgery
      - Code injection
  - **XML Bomb (Billion Laughs Attack)**
    - XML encodes entities that expand to exponential sizes, consuming memory on the host and potentially crashing it

- **XML External Entity (XXE) Attack**
  - Attempts to embed a request for a local resource
  - To prevent XML vulnerabilities from being exploited, use proper input validation
    - XML vulnerability
    - XML exploitation
    - XML injection
  - Unlike XML, HTML or JavaScript use defined keywords for each bracketed entry

- **Other Injection Attacks**
  - **Lightweight Directory Access Protocol (LDAP)**
    - An open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol network
  - **LDAP injection**
    - An application attack that targets web-based applications by fabricating LDAP statements that are typically created by user input
      - **STAR**
        - a wildcard character inserted as the search parameter to display all the users to the screen
    - use input validation and input sanitization as protection against an LDAP injection attack
  - **Command Injection**
    - Occurs when a threat actor is able to execute arbitrary shell commands on a host via a vulnerable web application
  - **Process Injection**
    - A method of executing arbitrary code in the address space of a separate live process
    - There are many different ways to inject code into a process
      - Injection through DLLs
      - Thread Execution Hijacking
      - Process Hollowing
      - Process Doppel ganging
      - Asynchronous Procedure Calls
      - Portable Executable Injections

    - Use endpoint security solutions that are configured to block common sequences of attack behavior

- **Authentication Bypass**
  - **Authentication bypass attack**
    - Any attack that exploits how user logins are obtained or processed within a web application
  - **Spoofing**
    - A software-based attack where an attacker attempts to assume the identity of a user, a process, address, or other unique identifier in order to bypass authentication mechanisms
  - **On-path Attacks**
    - An on-path attack is an attack where the attacker sits between two hosts during communication
    - Formerly known as man-in-the-middle attacks
    - When a password is stored in the web application's database, it isn't the actual password itself that is stored, but instead it is a **hash** of that password
  - **Password spraying**
    - A form of brute force password guessing that focuses on using the same few commonly used passwords across multiple accounts
  - **Credential stuffing**
    - A type of brute-force attack in which stolen user account names and passwords are tested against multiple websites in an effort to bypass their authentication
  - **Broken authentication system**
    - Any system that has a software vulnerability where the authentication mechanisms allow the attacker to gain entry
    - A broken authentication system, this can lead to credential exposure

- **VM Attacks**
  - **VM Escape**
    - Occurs when a threat actor attempts to get out of an isolated VM and directly sends commands to the underlying hypervisor
    - Easier to perform on a Type II hypervisor then a Type I hypervisor
    - Ensure guest OS, host OS, and hypervisor are patched and up-to-date
  - **VM Hopping**

        - Occurs when a threat actor attempts to move from one VM to another on the same host
            - **VM Hopping**
                - VM to VM
            - **VM Escape**
                - VM to hypervisor or host OS
        - Ensure guest OS and hypervisor are patched, up-to-date, and securely configured
    - **Sandbox**
        - Separates running programs to mitigate system failures or software vulnerabilities from spreading
    - **Sandbox Escape**
        - Occurs when an attacker circumvents sandbox protections to gain access to the protected OS or other privileged processes
    - **Live Migration**
        - Migration of a VM from one host to another even while it is running
        - VM images should be encrypted prior to being sent from one server to another over the network
    - **Data Remnants**
        - Leftover pieces of data that may exist in the hard drive which are no longer need
        - Always encrypt VM storage locations and ensure encryption key is destroyed

- **Network Attacks**
    - **BGP Route Hijacking**
        - Occurs when the IP addresses associated with an autonomous system are improperly announced
            - DV-LINK-AS (AS-39523)
    - **IP Prefix Filtering**
        - Only allows IP address announcements to be sent and accepted from a small set of well-defined autonomous systems
    - **Virtual Local Area Network (VLAN)**
        - Used to partition any broadcast domain and isolate it from the rest of the network
    - **VLAN Hopping**

        - A technique exploiting a misconfiguration to direct traffic to a different VLAN without proper authorization
    - **Double Tagging**
        - Attacker tries to reach a different VLAN using the vulnerabilities in the trunk port configuration
            - Change default config
            - Never add user devices
    - **Switch Spoofing**
        - Attacker attempts to conduct a Dynamic Trunking Protocol (DTP) negotiation
        - Disable dynamic switch port modes by default
    - **Interception Attack**
        - Any attack that provides unauthorized access to network traffic
    - **On-Path Attack**
        - Attacker puts themselves between the victim and the intended destination
    - **Denial of Service (DoS) Attack**
        - Attempts to make a computer or service resources unavailable
    - **Distributed Denial of Service (DDoS) Attack**
        - Uses multiple machines to launch an attack against a single server or domain to force it offline
            - Redundancy
            - Resiliency
            - Network segmentation
            - Mirroring
            - Failover
            - Sinkholing
            - Rate limiting
            - Web application firewalls

- **Social Engineering**
    - **Social Engineering**
        - Any attempt to manipulate users to reveal confidential information or perform actions detrimental to a system's security
        - The weakest link is our end users and employees
    - **Phishing**
        - Sending an email in an attempt to get a user to click a link

        - Captures most people and doesn't really target any particular person or group
    - **Spearphishing**
        - More targeted form of phishing
    - **Whaling**
        - Focused on key executives within an organization or other key leaders, executives, and managers in the company
    - **Tailgating**
        - Entering a secure portion of the organization's building by following an authorized person into the area without their knowledge or consent
    - **Piggybacking**
        - Similar to tailgating, but occurs with the employee's knowledge or consent
    - **Shoulder Surfing**
        - Coming up behind an employee and trying to use direct observation to obtain information
    - **Dumpster Diving**
        - Scavenging for personal or confidential information in garbage or recycling containers

Indicators of Compromise

Objectives 2.2

- **OBJ 2.2:** Given a scenario, analyze indicators of compromise and formulate an appropriate response.

- **Types of IoCs**

- **PCAP Files**
  - Network traffic must be captured and its data frames decoded before it can be analyzed
  - **Switched Port Analyzer (SPAN)**
    - Allows for the copying of ingress and/or egress communications from one or more switch ports to another
  - **Packet Sniffer**
    - A piece of hardware or software that records data from frames as they pass over network media using methods such as a mirrored port or tap device
    - A **network sniffer** should be placed inside a firewall or close to an important server
  - **tcpdump**
    - A data-network packet analyzer computer program that runs under a command line interface and allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached
  - **Wireshark**
    - A free and open-source GUI-based packet analyzer that is used for network troubleshooting, analysis, software and communications protocol development, and education

- **NetFlow**
  - **Full Packet Capture (FPC)**
    - Captures the entire packet, including the header and the payload for all traffic entering and leaving a network
  - **Flow Analysis**
    - Relies on a flow collector, which records metadata and statistics rather than recording each frame that passes through the network

        - Flow analysis does not provide the actual content
    - **NetFlow**
        - A Cisco-developed means of reporting network flow info to a structured database
            - Protocol interface
            - IP version/type
            - Source/destination IP
            - Source/destination port
            - IP service type
    - **Zeek**
        - Passively monitors a network like a sniffer, but only logs full packet capture data of potential interest
        - Performs normalization of the data and stores it as a tab-delimited or JSON-formatted text files
    - **Multi Router Traffic Grapher (MRTG)**
        - Creates graphs showing traffic flows through the network interfaces of routers and switches by polling the appliances using SNMP

- **Logs**
    - Log files allow for the reconstruction of an event after it occurs
    - Ensure logs are not saved on the same device being logged
    - Network Log
        - Generated by network appliances like routers, switches, access points, and firewalls
    - Vulnerability Log
        - Documented results from a vulnerability scan or assessment
    - Access Log
        - Records authentication attempts for each host, server, or web application
        - Review access logs to determine patterns of activity
    - Operating System Log
        - Created within the particular operating system running in your environment
            - Application
                - Record of any events generated by applications and services on the system
            - Security

        - Record of audit events on the system, such as any failed logon or file access attempts that are denied
    - System
        - Record of events on the system and its services that involve its resources
    - Setup
        - Used to record events generated during the installation of the operating system
    - Forwarded event
        - Used to record events that are received from other hosts

- **IoC Notifications**
    - **File Integrity Monitoring (FIM)**
        - A host-based IDS that creates a hash digest for every file being monitored on the given system
            - PCI-DSS
            - Sarbanes-Oxley
            - FISMA
            - HIPAA
    - **Critical Security Functions**
        - Security Information and Event Management (SIEM)
        - Combines data, logs, and notifications from multiple systems across the network into a single repository
            - Trigger
            - Alert
            - Notify
    - **Data Loss Prevention (DLP)**
        - Configured to monitor and prevent data leakage from devices
            - **Network DLP**
                - At network boundary
            - **Endpoint DLP**
                - As a software agent
    - **Precise Method**
        - Registers all content that should be considered sensitive by the DLP
    - **Imprecise Method**
        - Relies on keywords, regular expressions, metadata tags, Bayesian analysis, and statistical analysis

- **Intrusion Detection System (IDS)**
  - Logs and alerts
- **Intrusion Prevention System (IPS)**
  - Logs, alerts, takes action Signature-Based

- Analyzes traffic based on defined signatures and can only recognize attacks based on previously identified attacks in its database

- **Anomaly-based/ Behavioral-based IDS**
  - Analyzes traffic and compares it to a normal baseline of traffic to determine whether a threat is occurring
- **Antivirus/Antimalware**
  - Detects and stops software problems such as adware, spyware, viruses, worms, and other destructive types of software
  - Keep antimalware signatures up-to-date and conduct routine system scans

- **Response to IoCs**
  - Severity or priority rating of the alert is defined y the type of alert or notification received
  - **Functional Impact**
    - Scope of the impact the incident would have on the organization's daily operations
  - **Information Impact**
    - Degree to which the confidentiality, integrity, and availability of the organization's data is affected
  - **Recoverability**
    - Amount of time and resources that will be required to recover from an incident
      - Firewall rules
      - IPS/IDS rules
      - ACL rules
      - Endpoint protection rules
      - Scripts/regular expressions

Incident Response

Objectives 2.7

- **OBJ 2.7:** Given an incident, implement the appropriate response.

- **Triage**
  - **Triage**
    - Quickly analyzing a given event or alert and categorizing it based on some predefined factors in the organization
      - Scope
      - Impact
      - Cost
      - Downtime
      - Legal ramification
  - The more machines that are affected, the larger the scope
  - Automatically categorize and prioritize events and alerts based on signature patterns and rules
      - True positive
      - True negative
      - False positive
      - False negative
  - False positives can overwhelm security analysts with too many alerts to investigate
  - Triage inputs by severity and determine if they are true positives or false positives

- **Communication Plan**
  - **Communication Plan**
    - An outline of how your organization will communicate during an incident
    - Should account for the time difference involved between your headquarters and the local site that is affected by the incident
      - **VOIP systems**
        - Cannot be trusted during an incident involving a potential network compromise
        - Corporate email can also have been compromised by an attacker if they have gotten into the network
    - **Out-of-band communication system**

- Any system where your signals are being sent between two parties or two devices using a path or method that is different from your primary communication path
- Use a different set of digital signatures and encryption keys in their encryption process
    - **Up-to-date contact list**
        - A printed out contact list with all the proper names and numbers that you might need

- **Escalation procedures**
    - Identify at what point you will call in personnel or an incident response team
    - Procedures to notify the right individuals and key stakeholders in the organization
        - Chief Information Officer
        - On-call incident response team members
        - System owners
        - System administrators
        - Human resources
        - Legal department representative
        - Public affairs
        - Law enforcement
    - Methods of notifying individuals can include
        - Email
        - Internal web portals
        - Telephone calls
        - In-person update
        - Leaving a voicemail
        - Writing a formal report
        - Any other form of notification that your company decides is desirable and effective
        - **Medium priority incident**
            - Email, Direct message, or possibly even a phone call
        - **Low priority incident**
            - Daily or weekly report or by posting it to our internal portal that key stakeholders could review at their leisure

    - Communications plan should identify who is authorized to release information to those outside of the incident response team and the key stakeholders
    - Communication plan should dictate who is authorized to receive privileged information

- **Stakeholder Management**
    - **Senior leadership**
        - The executives and managers who are responsible for business operations and various functional areas within your company
            - Chief Executive Officer
            - Chief Operations Office
            - Chief Financial Officer
            - Chief Information Officer
            - Director of Information Technology
            - Director of Human Resources
            - Marketing Director
        - Incident responders are extremely technical people and they will look to solve an incident as quickly as possible
    - **Regulatory bodies**
        - Governmental organizations that oversee the compliance with specific regulations and laws
    - **Legal counsel**
        - Involves the lawyers who work for your business or organization in order to mitigate risk from civil or criminal lawsuits
    - **Law enforcement**
        - A stakeholder external to your organization who may provide some services to assist in your incident handling efforts or can help you prepare for legal action against the attacker
        - Involving law enforcement, is a decision that should only be made by senior executives with guidance from your organization's legal counsel
    - **Human resources**
        - Provides guidance and counsel to ensure there is not a breach of any employment laws or employee contracts during your incident response
    - **Public Relations team**
        - Manage the negative publicity from a serious incident during your response

        - Public relations should always be involved with larger breaches that could garner media interest

- **Incident Response Process**
    - **Incident**
        - An act of violating an explicit or implied security policy
    - NIST Computer Security Incident Handling Guide special publication number 800-61
        - **Preparation**
            - The phase where cybersecurity practitioners try to make the system resilient to attack by hardening their systems and networks
            - Focused on doing everything needed to get ready for some kind of future incident
        - **Detection and analysis**
            - Determine if an incident has actually taken place, and if so, how severe is that incident
        - **Containment**
            - Limits the scope and magnitude of the incident by securing data and minimizing the impact to business operations and your organization's customers and business partners
        - **Eradication and recovery**
            - Begins once the incident is contained and is focused on removing the malicious activity and restoring the system back to a secure state
        - **Post-incident activity**
            - Occurs after the system has been contained, the malicious activity was eradicated, and the system was fully recovered and restored to operation
            - **Root Cause Analysis**
                - A systematic process to identify the initial source of the incident and how to prevent it from occurring again
                    - Define/scope the incident
                        - Determine the causal relationships to led to the incident
                    - Identify an effective solution

        - Implement and track the solutions to ensure the incident is fully solved
    - **Lessons Learned Process**
        - A formalized method to document the things we experienced during the incident
        - Identify what could be improved
    - **After-action Report**
        - A formalized report that collects information about what happened
        - Should have the root cause analysis and the recommendations for improvements from your lessons learned
- Organizations should utilize a team of professionals
    - **Large organizations**
        - Have dedicated incident responses teams where the members perform this role full-time
    - **Smaller organizations**
        - Create temporary teams that are brought together for a specific incident
- **Leadership and management teams**
    - Responsible for ensuring the team has the funding, resources, and expertise needed to conduct the incident response
    - Other method that some organizations have taken to handle incident responses is to outsource the incident response teams

- **Playbooks**
    - **Playbook**
        - Acts as a checklist of actions that should be performed to detect and respond to a specific type of incident
        - Preparing for an incident response ahead of time and creating these playbooks to ensure documented procedures for response when an incident occurs
        - Serve as a standard operating procedure
        - Details how to automate responses, detect and analyze it
            - Preparation Phase
            - Detection Phase
            - Analysis Phase

        - Containment Phase
        - Eradication Phase
        - Recovery Phase
        - Post-incident Activity Phase
- **SOAR**
    - A class of security tools that helps facilitate incident response, threat hunting, and security configurations by orchestrating and automating runbooks and delivering data enrichment
    - Can Automate a playbook
        - Runbook
            - An automated version of a playbook that can partially or fully automate the incident response process
            - Free up analysts for higher level work without wasting their time on minor things that could easily automated
- **Ransomware Playbook**
    - Used to describe the people, process, and tools to be employed during a ransomware event
    - Determining which systems are impacted
    - Methods used to impact those systems
    - How to isolate those systems
    - Which key stakeholders to work with
- **Data Exfiltration Playbook**
    - Used to describe the specific and necessary tasks needed to stop or mitigate an ongoing data exfiltration
    - The playbooks and runbooks should focus on mitigating known instances and protecting the data stores first, then identifying any other potential compromises in the network
- **Phishing Playbook**
    - Involve the necessary responses to identifying the phishing emails, determining which uses clicked or opened the links or files in those emails, and identifying the extent of the exploitation
    - Focus on identifying all users who have received the email, identifying how many have open, read, or clicked on the email, and then resetting their passwords and reimaging their workstations

Digital Forensics

Objectives 2.8

- **OBJ 2.8:** Explain the importance of forensic concepts.

- **Forensic Process**
  - **Conducting a Criminal Investigation**
    - The forensic investigator must be qualified to the standards set forth by your jurisdiction and conduct all of their investigations using sound digital forensic procedures and techniques
  - **Conducting Forensic Analysis**
    - Internal organizational requirements are not as strict
  - **Identification Phase**
    - Ensures the scene is safe, the evidence is not going to be contaminated, and the scope of the evidence to be collected is properly identified
  - **Collection Phase**
    - Ensure that we have authorization to collect the evidence
    - Evidence being collected must be documented to prove integrity
  - **Analysis Phase**
    - Involves creating a copy of the evidence for analysis, because we never want to perform analysis on the primary evidence source, such as the original laptop or hard drive
  - **Reporting or Presentation Phase**
    - Used to create a report of the methods and the tools used in the investigation and then to present detailed findings and conclusions based on the analysis performed in phase 3
    - If you are dealing with an internal organizational investigation, you may not use a formal report, but instead you may be asked to provide a presentation on your finding

- **Chain of Custody**
  - **Chain of custody**
    - The record of evidence handling from its collection to it eventually presentation in court
    - Evidence must be put into a specialized evidence bag
  - **Specialized Evidence Bags**

- Used for electronic media to ensure that they cannot be damaged or corrupted by **electrostatic discharge or ESD**
  - **Faraday bag**
    - Used to shield devices from outside signals to prevent data from being altered, deleted, or added to a device
- The lifecycle for a piece of evidence can extend over a very long time
- Each piece of evidence collected, should be identified, bagged, sealed, labeled, and stored
- It is important to ensure that the evidence is properly store with the right humidity and temperature controls in place
- The amount of evidence collected can become extremely large
- Use metadata, or data about the data for cataloging the evidence

- **Legal Hold**
  - A process designed to preserve all the relevant information when litigation is reasonably expected to occur. Litigation is just a fancy word for lawsuit
  - Your computer or server can be seized as evidence inside of some kind of criminal conspiracy
  - If you are subject to a legal hold, ensure your business operations by having have a spare hardware and good backups of your systems

- **Order of Volatility**
  - **Data acquisition**
    - The method and tools used to create a forensically sound copy of the data from a source device such as system memory or a hard disk
    - **"Do I have the right to search or seize this legally?"**
  - **Bring-your-own-device policies**
    - Complicate data acquisition because you may not legally be able to search or seize that device because the employee owns it
    - Evidence without the proper authority or permission can be inadmissible in court
    - Some evidence can be lost if you shut down a computer or it is powered off
  - **Order of Volatility**
    - You should always collect evidence that could be modified or destroyed the easiest first
    - **Guidelines for Evidence Collection and Archiving" in RFC 3227**

- **Registers and cache**
    - This type of data can also only be collected when the computer is powered on
- **Routing tables, ARP Caches, Process Tables, and Kernel Statistics, and memory**
    - These can all be altered by the system when it is in operation. Additionally, if you remove power to the system, all of this data will also be lost
- **Temporary file systems**
    - Often overwritten during system operation, and some are deleted when the system is shutdown or rebooted
- **Disks**
    - These types of devices do allow for frequently updates and changes to their contents, but not nearly as rapidly as processor registers and cache, RAM, and temporary file systems
- **Remote logging and monitoring data**
    - This data is less likely to change as quickly as the other evidence collected so far, since it is not on the same system that is the subject of our investigation, making it a lower collection priority
- **Physical configurations and network topologies**
    - This data also doesn't change frequently, but it is good to collect to gather the details of the network at the time evidence collection
- **Archival media**
    - Most of this data is offline and not likely to change quickly, such as backup tapes, CDs, DVDs, and external hard drives
    - When you are dealing with the Windows registry, remember that some of its contents are actually in RAM and not stored fully on the hard drive
        - **HKLM\Hardware hive**
            - You need to collect this part of the registry using a memory dump
            - It captures a record of every single disk or thumb drive that has been connected to or removed from the computer

- **Forensic Analysis**
  - **Media Analysis**
    - The most common form of digital forensics
  - **Disk Imaging**
    - A technique that creates a bit-by-bit copy of a hard disk or USB drive, including the slack space and the unallocated space on the drive
    - Document the chain of custody and create hash digests of the disk image to ensure integrity of the data collected
  - **Forensic Image**
    - Used for analysis purposes and is created from the original evidence
  - **Forensic Clone**
    - A copy of that forensic image and is used as a working copy during analysis that could modify or change the data in the working copy
  - **Memory Snapshot or Memory Dump**
    - The process of conducting memory capture and forensics is very similar to the processes used in disk imaging
    - Incident responders must be very careful when conducting memory captures because memory is extremely volatile
    - Incident responders can also analyze the page files
  - **Content Analysis**
    - Where the files and configurations of the hard disk are analyzed, and a detailed report is generated
    - The empty space of the disk image is analyzed to determine if the perpetrator may have deleted the evidence
  - **Cryptanalysis**
    - The art and science of cracking cryptographic schemes
    - Small bits of the data can be recovered or observed, and this can still help the forensic investigator with their case
  - **Steganalysis**
    - The process of identifying files that use steganography to hide data within them
    - The practice of concealing data within another file, message, image, or video
  - **LSB Steganography**
    - Allows you to hide text messages inside an image file
    - It is very easy to hide information in these files in plain sight because it doesn't add to the file size or change the file much at all

- **Software Analysis**
  - A specialized type of analysis that requires an expert on the particular software code being considered
- **Network Analysis**
  - Conducted to determine the path a particular piece of traffic may have taken on the network by conducting path tracing, or by analyzing the network logs
- **In Hardware or Embedded Device Analysis**
  - Specialized tools are used to determine the actions that have occurred on devices

Digital Forensic Tools

Objectives 2.9

- **OBJ 2.9**: Given a scenario, use forensic analysis tools.

- **Forensic Workstations**
  - **Digital forensic kits**
    - Contain the software and hardware tools required to acquire and analyze evidence from system memory captures or dumps, and mass storage file systems
      - **Encase**
        - Provides built in pathways or workflow templates that help analysts follow the key steps in many different types of investigation
        - Provides a simple to use graphical user environment and it runs on Windows systems
        - Can be used for data acquisition, as well as data analysis
        - Powerful tool that can be used to read bit by bit copies of the hard drive
      - **Forensic Toolkit (FTK)**
        - Allow for faster searching and analysis by using data indexing during the evidence importation process
      - **Sleuth Kit**
        - An open-source digital forensics suite that is built on top of different command line tools and programming libraries for disk imaging and file analysis
      - Autopsy
        - A graphic user interface front-end for the Sleuth Kit that makes it look and feel more like Encase or FTK
  - **Forensic Workstation**
    - A powerful desktop unit that can have multiple processors with multiple cores in each one
    - The forensic workstation should also have a wide variety of drive host bus adapters
      - EIDE
      - SATA
      - SCSI

        - SAS
        - USB
        - FireWire
        - Thunderbolt
    - The system should also have optical storage drives
        - CD
        - DVD
        - Blu-ray drives
        - Multi-format memory card reader
    - If you wanted to collect the potential evidence on my cloud-based server, that is another 40 to 60 terabytes of data to collect
    - Forensic Workstation needs to be well secured and protected since it will be processing sensitive files and evidence
    - The forensic workstation should be prohibited from accessing the internet because we don't want it to get infected with any malware or suffer from any kind of exploitation
    - Forensic workstation should remain air gapped from the internet as a method of protecting it from an attacker who may be seeking to damage or modify the evidence you are analyzing

- **File Carving Tools**
    - **File carving**
        - A process used in digital forensics to extract data from a disk drive or other media when the file system is unavailable
        - When a file is deleted from a hard drive or storage device by a user, it isn't actually erased from the drive
            - **Forensic Analyst**
                - Finds deleted files and restore them to contain evidence of a crime
            - **Files Recovery**
                - Data is extracted as raw data without any specific formatting by the system
    - **Foremost**
        - A forensic data recovery programs that is commonly used to conduct file carving to extract deleted or corrupted data from a disk partition
            - **EnCase and FTK**

        - Both have the ability to recover deleted files and perform basic file carving
    - **Autopsy and the Sleuth Kit**
        - Have this capability using the command-line tool known as Scalpel
  - Another form of file carving involves extracting portions of a file for analysis
    - **sudo strings /dev/mem**
        - used to collect data from the system's memory for Linux System

- **Binary Analysis Tools**
  - **Hexdump**
    - A cross-platform tool that can be used to extract data from binary files and display their contents to the screen in hexadecimal, decimal, octal, or ASCII formats
      - **Hexdump –canonical option**
        - Display the date of creation, date of access, and MIME type for a given file to the screen
  - **Binwalk**
    - A binary firmware image inspection tool that can be used to understand the components, characteristics, and composition of a binary firmware image
    - Used when analyzing a file to determine if it is compressed, obfuscated, or encrypted by displaying a graph of the amount of entropy in the file's contents
  - **Ghidra**
    - An open-source, cross-platform java-based utility used to conduct software reverse engineering
      - IDA Pro
        - Used to generate assembly language source code from a machine-executable binary
    - Supports debugging functionality, like GNU Project Debugger for Linux and OllyDbg for Windows
  - **GNU Project Debugger**
    - A Unix and Linux tool that can be used to identify what is occurring within an application while it is running

        - A text-based program that can be used to analyze how code runs at a low level, identify shared libraries loaded by the program, and to understand how address space is memory is being used
        - Useful in reverse engineering
    - **Ollydbg**
        - A graphical debugger alternative to GDB that is used with the Windows operating system
        - Used to convert the binary code of 1s and 0s back into something like assembly language
    - **Readelf**
        - A Linux utility that can read the Executable and Linkable Format in an object file, which is known as ELF
        - Contains the different structures that make the program operate properly
    - **Objdump**
        - A utility that is used to analyze object files, similar to readelf, but it also includes a disassembler to reveal the assembler commands used by the binary or program
    - **Strace**
        - A Linux utility that can identify the interactions made between different processes and the Linux kernel
    - **Ldd**
        - A Linux utility that is used to display a program's dependencies
        - Useful during a forensic malware analysis
    - **File**
        - A Linux utility that is used to display the type of file being inspected
        - Uses the first two hexadecimal bytes to determine the file type known as the "magic bytes"

- **Forensic Analysis Tools**
    - **Exiftool**
        - A cross-platform utility written in Perl that can be used to read and write metadata from different file formats
        - Used to read metatdata
    - **Nmap**
        - A cross-platform tool used to discover hosts and services on a computer network by sending packets and analyzing the responses it receives

- Can also be configured to conduct fingerprinting of the services
  - **Aircrack-ng**
    - A suite of utilities that is designed for the assessment and analysis of wireless network security
  - **Airodump-ng**
    - Used to list the wireless networks in range of your antenna
    - Used to conduct wireless packet capture of the networks
  - **Airmon-ng**
    - Used to put your wireless network adapter into monitor mode to inspect all the wireless traffic being sent or received to any network in-range of your antenna, without joining or authenticating to those access points
  - **Airbase-ng**
    - Used to mimic an access point and can be used to create an evil twin as part of your investigation or incident response
  - **Aireplay-ng**
    - Used to introduce packets into a wireless network in order to perform a deauthentication attack against network clients

- **Volatility Framework**
  - An open-source memory forensics tool that has many different modules for analyzing specific elements of memory
  - Volatility is a text-based command line interface tool that allows you to take a memory dump of a system
- **Sleuth Kit**
  - A collection of command line tools and a C library that allows you to analyze disk images and recover files and evidence from them during an investigation or incident response
  - It can be paired with Autopsy
- **Statically linked library**
  - Describes a compiled process where the application's required libraries are identified at the time of compilation and are included within the resulting executable binary file
  - Contain all of the code in one place
- **Dynamically linked library**

    - Describes an architecture where the application will call upon the required library when the application is run by the user
    - Allow the application to execute functions from a library dynamically at run-time

- **Imaging Tools**
    - Creating a forensically-sound disk image requires a bit-by-bit copy of the original drive
    - Use either a forensically-sound software imaging tool, or a hardware forensic drive duplicator to create your disk images
    - **FTK Imager**
        - Known as the Forensic Toolkit Imager
        - A forensically-sound software tool that can be used to create a disk image
        - Only works on a Windows laptop or desktop to capture the contents of a hard drive
        - Documents the chain of custody
        - Uses graphical user interface like most Windows programs
        - The image can be read and analyzed by FTK, EnCase, or the Sleuth Kit
    - **dd Utility**
        - Found in all versions of the Linux and Unix operating system
        - Used to create a bit-by-bit copy of a hard drive from the command line or shell environment in Linux
        - Does not automatically create a chain of custody
        - Requires a proper syntax at the command line
    - **Forensic Drive Duplicators**
        - Works fast and efficient
        - Conduct the hashing and create the chain of custody like the FTK Imager does
        - Heavily used by law enforcement due to their ease of use in creating new images fast
            - PATA
            - SATA
            - USB
            - FireWire
    - **Write Blocker**

- Any tool that permits read-only access to data storage devices without compromising the integrity of the data and guarantees the protection of the original evidence
- **Sha256sum**
  - A Linux utility that is designed to generate a SHA-2 hash with a 256-bit hash digest for any given input
- **Ssdeep**
  - Another hashing utility, but it not used to create a hash of the evidence or disk image
  - Used for recursive computing and matching of Context Triggered Piecewise Hashing, also known as Fuzzy Hashing
    - **Fuzzy hashing**
      - Used to compare similar, but not identical files
  - Useful when searching for indicators of compromise
  - It looks for not just the exact matching file's hash, but also minor variations of the file too

- **Collection Tools**
  - **Netstat**
    - A very powerful command-line tool used to view the network connection information on a machine
      - **netstat -ano**
        - Provides the protocol, the local IP address, the remote IP, the state of the port, and the process that is using that particular network connection
    - Used on Windows, Linux, Unix, and Mac systems
  - **Nbtstat**
    - A utility that provides protocol statistics and current connections using the NetBIOS over TCP/IP
    - Only used on Windows systems
  - **Process Status (PS)**
    - A utility that gives us the process status for any currently running processes on a Linux system
    - Only used in Linux, Unix, and Mac systems
  - **Vmstat**

- A Linux command line utility that is used to collect and display summary information about the operating system's memory, processes, interrupts, paging, and block input outputs
- Used on a Linux, Unix, or Mac system

- **Ldd**
  - A Linux utility that is used to display a program's dependencies
  - Identify all of the shared libraries that are required by the particular program or binary
- **Lsof**
  - A Linux utility that is used to display a list of open files and the name of associated processes using those files
  - Can identify any files and processes
- **Netcat**
  - A networking utility that can read or write raw data to network connections using either TCP or UDP
  - Used in Unix, Linux, and Windows
  - Performs port scanning, file transfers, port listener, and can even be used as backdoor to a system
- **Conntrack**
  - A Linux command line utility that allows an investigator to interact with the connection tracking system in Linux
  - Can show, delete, and update tablet entries or listen to different traffic flow events
- **TCPdump**
  - A cross-platform packet analysis program that runs from the command-line
  - Relies on another program to capture packets, and then display the contents on the screen or write them to a file
  - Used with Linux, Unix, Mac, or Windows
- **Wireshark**
  - A cross-platform packet analyzer that works on many operating systems, including Windows, OS X, Unix, Solaris, and Linux
  - Makes searching, sorting, and filtering very easy
    - **PCAP**
      - Uses a remote machine to conduct packet capture and send the file

CASP+ (CAS-004) Conclusion

- **Take lots of practice exams before the official certification**
  - Did you score at least 90% or higher?
  - If you need more practice, take additional practice exams to hone your skills before attempting the exam

- **If you would like to save 10% or more on your exam voucher, please visit diontraining.com/vouchers to purchase your official exam voucher at a discount**