Module 11: Understanding Defense

Cybersecurity Essentials 3.0

Module Objectives

Module Title: Understanding Defense

Module Objective: Explain approaches to network security defense.

Topic Title	Topic Objective
Defense-in-Depth	Explain how the defense-in-depth strategy is used to protect networks.
Cybersecurity Operations Management	Explain how an organization monitors cybersecurity threats.
Security Policies, Regulations, and Standards	Explain security policies, regulations, and standards.

11.1 Defense-in-Depth

Assets, Vulnerabilities, Threats

- Cybersecurity analysts must prepare for any type of attack. It is their job to secure the assets of the organization’s network.

- To do this, cybersecurity analysts must first identify:
  - **Assets** - Anything of value to an organization that must be protected including servers, infrastructure devices, end devices, and the greatest asset, data.

  - **Vulnerabilities** - A weakness in a system or its design that could be exploited by a threat actor.

  - **Threats** - Any potential danger to an asset.

Identify Assets

- The collection of all the devices and information owned or managed by an organization are assets.
- The assets constitute the attack surface that threat actors could target.
- As an organization grows, so do its assets. Consider the number of assets a large organization would have to protect.
- Asset management consists of inventorying all assets, and then developing and implementing policies and procedures to protect them.
- Organizations need to identify where critical information assets are stored, and how access is gained to that information.

Asset Classification

- Asset classification assigns an organization’s resources into groups based on common characteristics.
- The most critical information needs to receive the highest level of protection and may even require special handling.
- A labeling system can be used to determine how valuable, how sensitive, and how critical the information is.
- The steps for identifying and classifying assets are:
  Step 1: Determine the proper asset identification category:
  - Information assets
  - Software assets
  - Physical assets
  - Services

Asset Classification (Cont.)

Step 2: Establish asset accountability by identifying the owner of each information asset and each piece of software:

- Identify the owner for all information assets.
- Identify the owner for all application software.

Step 3: Determine the criteria for classification

- Confidentiality
- Value
- Time
- Access rights
- Destruction

Step 4: Implement a classification schema:

- Adopt a consistent way of identifying information to ensure uniform protection and easier monitoring.

Defense-in-Depth

Asset Standardization

- Asset standards identify specific hardware and software products used by an organization.
- When a failure occurs, prompt action helps to maintain both access and security.
  - If an organization does not standardize its hardware selection, personnel may need to scramble to find a replacement component.
  - Non-standard environments require more expertise to manage, and they increase the cost of maintenance contracts and inventory.

Asset Lifecycle Stages

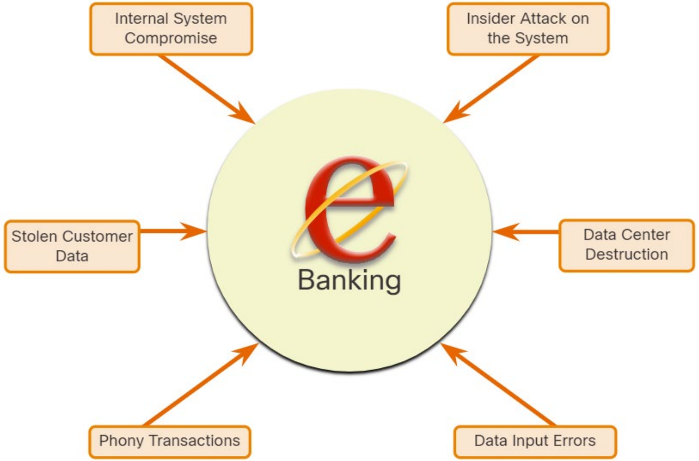
- Part of the cybersecurity specialists’ job is to manage information assets and related systems throughout that asset´s lifecycle. The stages of asset´s lifecycle are:

Procurement	The organization purchases the assets based on the needs identified from data gathered to justify the purchase. The asset is added to the organization’s inventory.
Deployment	The asset is assembled and inspected to check for defects or other problems. Staff perform tests and install tags or barcodes for tracking purposes. The asset moves from inventory to in-use.
Utilization	This is the longest stage of the cycle. The asset’s performance is continuously checked. Upgrades, patch fixes, new license purchases, and compliance audits are all part of the utilization stage.
Maintenance	It helps to extend an asset’s productive life. Staff may modify or upgrade the asset.
Disposal	At the end of the asset’s productive life, it must be disposed of. All data must be wiped from the asset. Disposal may include dismantling an asset for parts. Any parts that can cause an environmental hazard must be disposed of according to local guidelines.

Identify Vulnerabilities

- Threat identification provides an organization with a list of likely threats for a particular environment.

- When identifying threats, it is important to ask several questions:
  - What are the possible vulnerabilities of a system?
  - Who may want to exploit those vulnerabilities to access specific information assets?
  - What are the consequences if system vulnerabilities are exploited, and assets are lost?



Identify Vulnerabilities (Cont.)

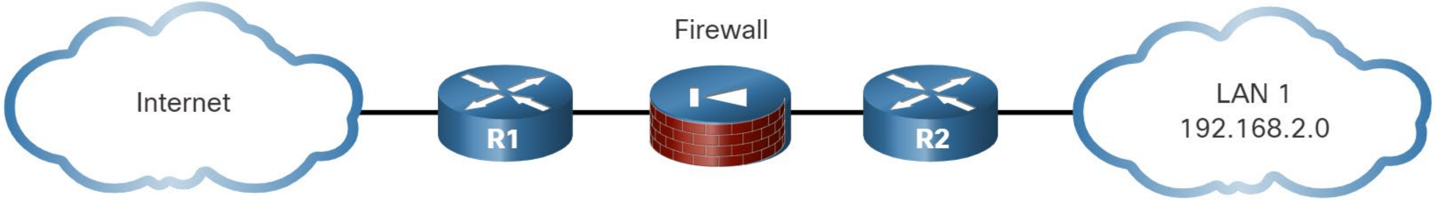
- The threat identification for an e-banking system would include:
  - **Internal system compromise** - The attacker uses the exposed e-banking servers to break into an internal bank system.
  - **Stolen customer data** - An attacker steals the personal and financial data of bank customers from the customer database.
  - **Phony transactions from an external server** - An attacker alters the code of the e-banking application and makes transactions by impersonating a legitimate user.
  - **Phony transactions using a stolen customer PIN or smart card** - An attacker steals the identity of a customer and completes malicious transactions from the compromised account.
  - **Insider attack on the system** - A bank employee finds a flaw in the system from which to mount an attack.
  - **Data input errors** - A user inputs incorrect data or makes incorrect transaction requests.
  - **Data center destruction** - A cataclysmic event severely damages or destroys the data center.

- Identifying vulnerabilities on a network requires an understanding of the important applications that are used, as well as the different vulnerabilities of that application and hardware.

Defense-in-Depth

Identify Threats

- Organizations must use a defense-in-depth approach to identify threats and secure vulnerable assets. It uses multiple layers of security at the network edge, within the network, and on network endpoints.



- Edge router (R1) - The first line of defense is the edge router, that has a set of rules specifying which traffic it allows or denies. It passes all connections that are intended for the internal LAN to the firewall.

- Firewall - The second line of defense is the firewall. It is a checkpoint device that performs additional filtering and tracks the state of the connections.

- Internal router (R2) - Another line of defense is the internal router. It can apply final filtering rules on the traffic before it is forwarded to its destination.

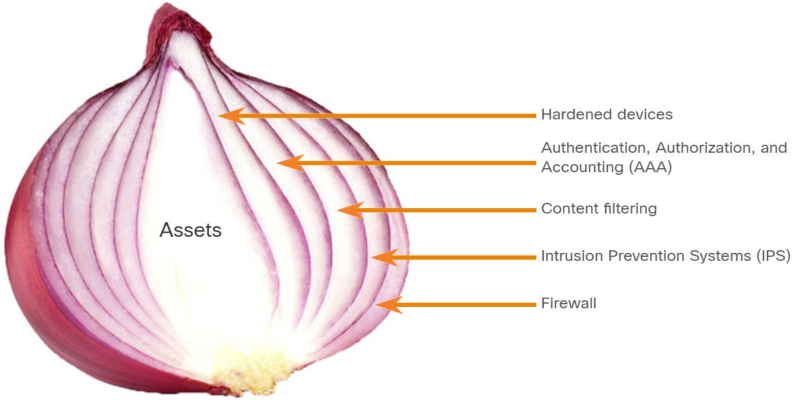
Identify Threats (Cont.)

- Routers and firewalls are not the only devices that are used in a defense-in-depth approach.
- Other security devices include Intrusion Prevention Systems (IPS), Advanced Malware Protection (AMP), web and email content security systems, identity services, network access controls, and more.
- In the layered defense-in-depth security approach, the different layers work together to create a security architecture in which the failure of one safeguard does not affect the effectiveness of the other safeguards.

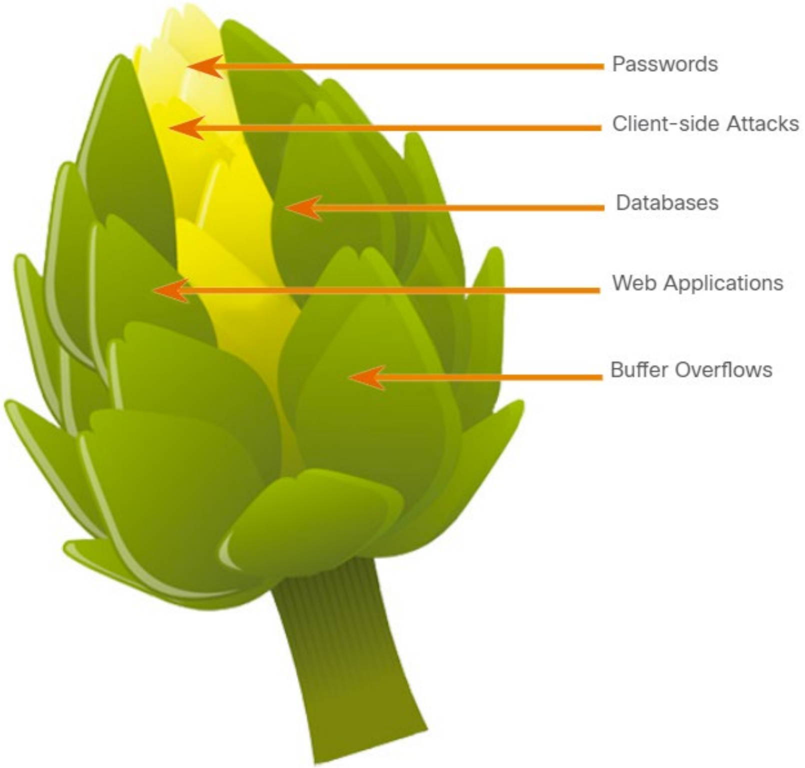
The Security Onion and The Security Artichoke

- **Security Onion**
  - A common analogy used to describe a defense-in-depth approach.
  - A threat actor would have to peel away at a network’s defenses layer by layer in a manner like peeling an onion.
  - Only after penetrating each layer would the threat actor reach the target data or system.

Note: The security onion described on this page is a way of visualizing defense-in-depth. This is not to be confused with the Security Onion suite of network security tools.


Hardened devices
Authentication, Authorization, and Accounting (AAA)
Content filtering
Assets
Intrusion Prevention Systems (IPS)
Firewall

The Security Onion and The Security Artichoke (Cont.)



- The changing landscape of networking, such as the evolution of borderless networks, has changed this analogy to the “security artichoke”, which benefits the threat actor.
- Threat actors no longer peel away each layer.
- They only need to remove certain “artichoke leaves.”
- The bonus is that each “leaf” of the network may reveal sensitive data that is not well secured.
- The hacker chips away at the security armor along the perimeter to get to the “heart” of the enterprise.

Defense in Depth Strategies

- To make sure data and infrastructure remain secure, an organization should create different layers of protection:
  - **Layering:** To make sure data and information remains available, an organization must set up different layers of protection, creating a barrier of multiple defenses that work together to prevent attacks.
  - **Limiting:** Limiting access to data and information reduces the possibility of a security threat. An organization should restrict access so that each user only has the level of access required to do their job.
  - **Diversity:** If all defense layers were the same, it would not be very difficult for cybercriminals to succeed in an attack. The layers must be different so that if one layer is penetrated, the same technique will not work on all the others which would compromise the whole system.

Defense in Depth Strategies (Cont.)

- **Obscurity:** Obscuring information can also protect data and information. An organization should not reveal any information that cybercriminals can use to identify which Operating System (OS) a server is running, or the type or make of equipment or software it uses.
- **Simplicity:** Complexity does not necessarily guarantee security. If employees do not understand how to configure a solution properly, such as setting up their account using an unnecessarily complex process, this may make it just as easy for cybercriminals to compromise those systems.

11.2 Cybersecurity Operations Management

Configuration Management

- Configuration management refers to identifying, controlling, and auditing the implementation and any changes made to a system’s established baseline.

- The baseline configuration includes all the settings that you configure for a system which provide the foundation for all similar systems — like a template of sorts.

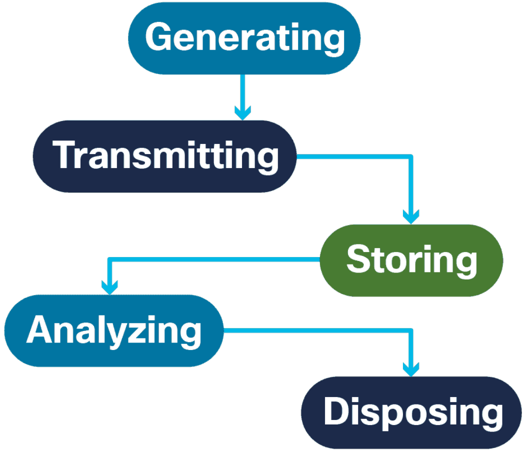
- Documented configuration resources might include:
    - Network maps, cabling and wiring diagrams, application configuration specifications
    - Standard naming conventions used for computers
    - IP schema to track IP addresses

- Hardening the operating system is an important part of making sure that systems have secure configurations.

- Configuring log files along with auditing, changing default account names and passwords, and implementing account policies and file-level access control are all used to create a secure OS.

Log Files

- A log records all events as they occur.
- Log entries make up a log file, with each log entry containing all the information related to a specific event.
- As an increasing number of log files are generated for computer security purposes, organizations should consider a log management process.
- Management of computer security log data should determine the procedures for:
  - Generating log files
  - Transmitting log files
  - Storing log files
  - Analyzing log data
  - Disposing of log data



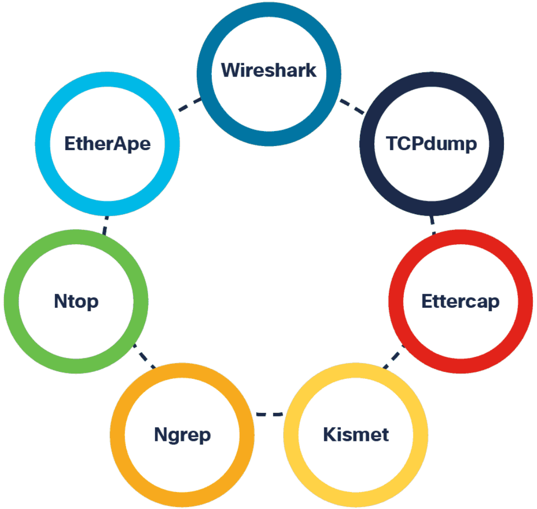
Operating System Logs and Application Security Logs

- **Operating system logs** record events that are linked to actions that have to do with the operating system. System events include:
  - Client requests and server responses such as successful user authentications.
  - Usage information that contains the number and size of transactions in each period.

- **Application Security Logs:** Organizations use network-based and/or system-based security software to detect malicious activity.
  - This software generates a security log to provide computer security data.
  - Logs are useful for performing auditing analysis and identifying trends and long-term problems.
  - Logs also enable an organization to provide documentation showing that it complies with laws and regulatory requirements.

Protocol Analyzers

- Packet analyzers, otherwise known as packet sniffers, intercept and log network traffic.
- The packet analyzer captures each packet, looks at the values of various fields in the packet and analyzes its content.
- It can capture network traffic on both wired and wireless networks.
- Packet analyzers perform the following functions:
  - Traffic logging
  - Network problem analysis
  - Detection of network misuse
  - Detection of network intrusion attempts
  - Isolation of exploited systems



11.3 Security Policies, Regulations, and Standards

Business Policies

- They are the guidelines that are developed by an organization to govern its actions.
- The policies define standards of correct behavior for the business and its employees.
- If behavior that violates business policy (baseline) is detected on the network, it is possible that a security breach has occurred.

An organization may have several guiding policies:

Policy	Description
Company policies	They establish the rules of conduct and the responsibilities of both employees and employers. They protect the rights of workers as well as the business interests of employers.
Employee policies	They are created and maintained by human resources staff to identify employee salary, pay schedule, employee benefits, work schedule, vacations, and more. They are often provided to new employees to review and sign.
Security policies	They identify a set of security objectives for a company, define the rules of behavior for users and administrators, and specify system requirements. These objectives, rules, and requirements collectively ensure the security of a network and the computer systems in an organization.

Security Policy

- A comprehensive security policy has several benefits:
  - Demonstrates an organization's commitment to security
  - Sets the rules for expected behavior
  - Ensures consistency in system operations, software and hardware acquisition and use, and maintenance
  - Defines the legal consequences of violations
  - Gives security staff the backing of management
- Security policies are used to inform users, staff, and managers of an organization's requirements for protecting technology and information assets.
- A security policy also specifies the mechanisms that are needed to meet security requirements and provides a baseline from which to acquire, configure, and audit computer systems and networks for compliance.

Security Policy (Cont.)

Policies in a security policy may include:

Policy	Description
Identification and authentication policy	Specifies authorized persons that can have access to network resources and identity verification procedures.
Password policies	Ensures passwords meet minimum requirements and are changed regularly.
Acceptable Use Policy (AUP)	Identifies network applications and uses that are acceptable to the organization.
Remote access policy	Identifies how remote users can access a network and what is accessible via remote connectivity.
Network maintenance policy	Specifies network device operating systems and end user application update procedures.
Incident handling procedures	Describes how security incidents are handled.

BYOD Policies

- Many organizations must now also support Bring Your Own Device (BYOD), enabling employees to use their own mobile devices to access company systems, software, networks, or information.

- It provides several key benefits to enterprises, including increased productivity, reduced IT and operating costs, better mobility for employees, and greater appeal when it comes to hiring and retaining employees.

A BYOD security policy should be developed to accomplish the following:

- Specify the goals of the BYOD program.
- Identify which employees can bring their own devices.
- Identify which devices will be supported.
- Identify the level of access employees are granted when using personal devices.
- Describe the rights to access and activities permitted to security personnel on the device.
- Identify which regulations must be adhered to when using employee devices.
- Identify safeguards to put in place if a device is compromised.

BYOD Policies (Cont.)

The following are BYOD security best practices to help mitigate BYOD vulnerabilities:

Best Practice	Description
Password protected access	Use unique passwords for each device and account.
Manually control wireless connectivity	Turn off Wi-Fi and Bluetooth connectivity when not in use. Connect only to trusted networks.
Keep updated	Always keep the device OS and other software updated. Updated software often contains security patches to mitigate against the latest threats or exploits.
Back up data	Enable backup of the device in case it is lost or stolen.
Enable “Find my Device”	Subscribe to a device locator service with remote wipe feature.
Provide antivirus software	Provide antivirus software for approved BYOD devices.
Use Mobile Device Management (MDM) software	It enables IT teams to implement security settings and software configurations on all devices that connect to company networks.

Regulatory and Standards Compliance

- There are also external regulations regarding network security.
- Network security professionals must be familiar with the laws and codes of ethics that are binding on Information Systems Security (INFOSEC) professionals.
- Many organizations are mandated to develop and implement security policies.
- Compliance regulations define what organizations are responsible for providing and the liability if they fail to comply.
- The compliance regulations that an organization is obligated to follow depend on the type of organization and the data that the organization handles.

Lab - Document Enterprise Cybersecurity Issues

- In this lab, you will complete the following objectives:

  Part 1: Record your assessment of Athena's cybersecurity issues.
  Part 2: Record the different types of assets owned by Athena.
  Part 3: List the threats for each asset type.
  Part 4: Recommend mitigation techniques to address each threat.

11.4 Understanding Defense Summary

What Did I Learn in this Module?

- Cybersecurity technicians must first identify assets, vulnerabilities, and threats to prepare for an attack.
- The collection of all the devices and information owned or managed by the organization are assets.
- Four steps to asset identification and classification: determine the proper asset identification category, establish asset accountability by identifying the owner of each information asset and each piece of software, determine the criteria for classification, and implement a classification schema.
- The stages of an asset´s lifecycle are procurement, deployment, maintenance, and disposal.
- Organizations must use a defense-in-depth approach to identify threats and secure vulnerable assets.
- Two common analogies to describe a defense-in-depth approach: Security Onion and Security Artichoke.
- To make sure data and infrastructure remain secure, an organization should create different layers of protection including layering, limiting, diversity, obscurity, and simplicity.
- Configuration management refers to identifying, controlling, and auditing the implementation and any changes made to a system’s established baseline.
- Documented configuration resources can include network maps, cabling/wiring diagrams, app configuration standards, naming conventions and an IP schema.
- Configuring log files along with auditing, changing default account names and passwords, and implementing account policies and file-level access control are all used to create a secure OS.

What Did I Learn in this Module? (Cont.)

- Management of computer security log data should determine the procedures for generating, transmitting, and storing log files, as well as analyzing and disposing of log data.
- Operating system logs record events that are linked to actions that have to do with the OS.
- Organizations use network-based and/or system-based security software to detect malicious activity.
- It generates security logs useful for performing auditing analysis and identifying trends and long-term problems and enables an organization to provide documentation showing that it complies with laws and regulatory requirements.
- Packet analyzers intercept and log network traffic, perform traffic logging, network problem analysis, detection of network misuse, detection of network intrusion attempts, and isolation of exploited systems.
- Business policies define standards of correct behavior for the business and its employees and define the activities that are allowed on the network, setting a baseline of acceptable use.
- Most organizations will have company policies, employee policies, and security policies.
- Security policies are made up of identification and authentication, passwords, acceptable use, remote access, network maintenance, and incident handling.
- Best practices for BYOD policies include: password-protected access, manual control of wireless connectivity, updates current including patches and backups, use of antivirus and MDM software, and enabling of "Find my Device".