



# Chapter 8: Protecting the Network

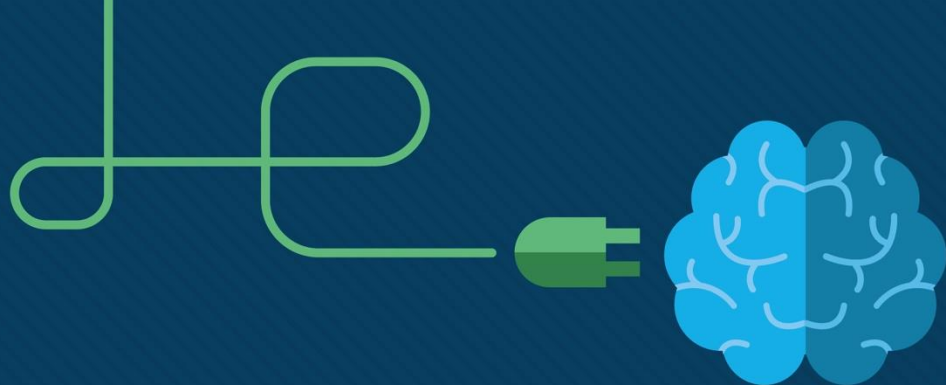
## Instructor Materials

CCNA Cybersecurity Operations v1.1



# Chapter 8: Protecting the Network

**CCNA Cybersecurity Operations v1.1**  
**Planning Guide**



# Chapter 8: Protecting the Network

CCNA Cybersecurity Operations v1.1



# Chapter 8 - Sections & Objectives

## ■ 8.1 Understanding Defense

- Explain approaches to network security defense.
  - Explain how the defense-in-depth strategy is used to protect networks.
  - Explain security policies, regulations, and standards.

## ■ 8.2 Access Control

- Explain access control as a method of protecting a network.
  - Describe access control policies.
  - Explain how AAA is used to control network access.

## ■ 8.3 Threat Intelligence

- Use various intelligence sources to locate current security threats.
  - Describe information sources used to communicate emerging network security threats.
  - Use threat intelligence to identify threats and vulnerabilities.

# 8.1 Understanding Defense

# Assets, Vulnerabilities, Threats

- Cybersecurity risk consists of the following:
  - **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.
  - **Threats** - Any potential danger to an asset.



## Defense-in-Depth

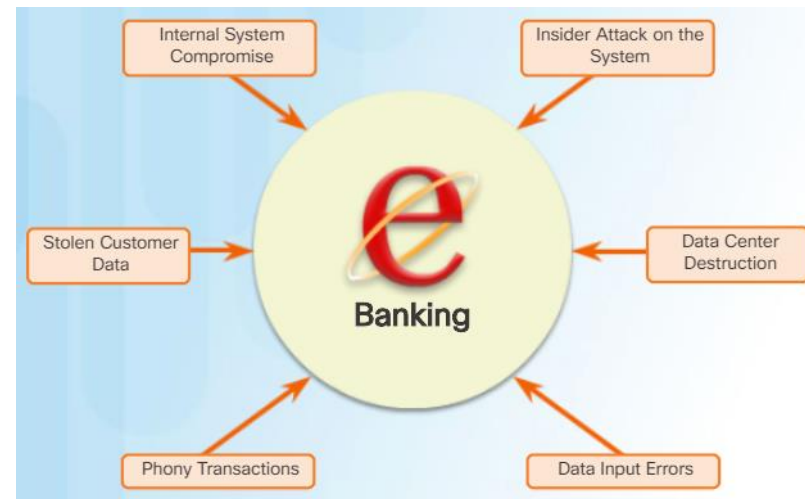
# Identify Assets

- Many organizations only have a general idea of the assets that need to be protected.
- All the devices and information owned or managed by the organization are the assets.
- Assets constitute the attack surface that threat actors could target.
- Asset management consists of:
  - Inventorying all assets.
  - Developing and implementing policies and procedures to protect them.
- Identify where critical information assets are stored, and how access is gained to that information.



# Identify Vulnerabilities

- Identifying vulnerabilities includes answering the following questions:
  - What are the vulnerabilities?
  - Who might exploit the vulnerabilities?
  - What are the consequences if the vulnerability is exploited?
- For example, an e-banking system might have the following threats:
  - Internal system compromise
  - Stolen customer data
  - Phony transactions
  - Insider attack on the system
  - Data input errors
  - Data center destruction

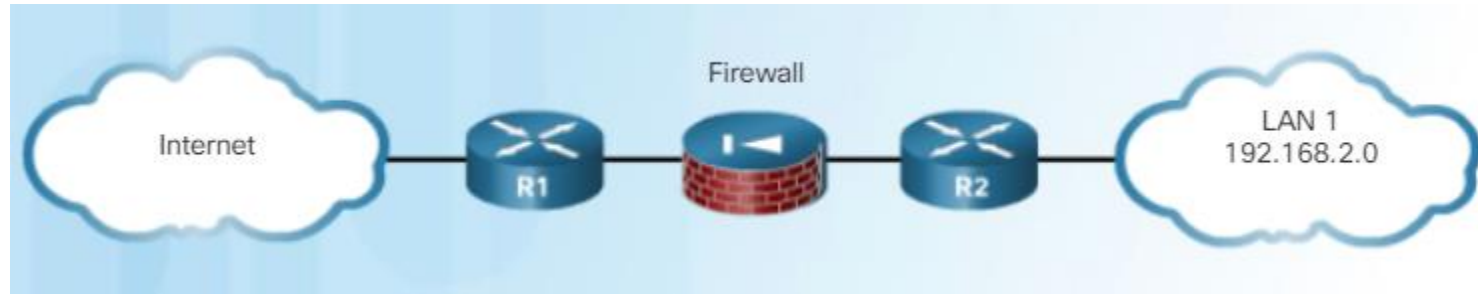




## Defense-in-Depth

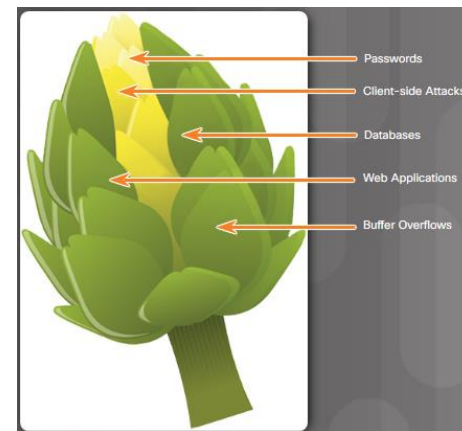
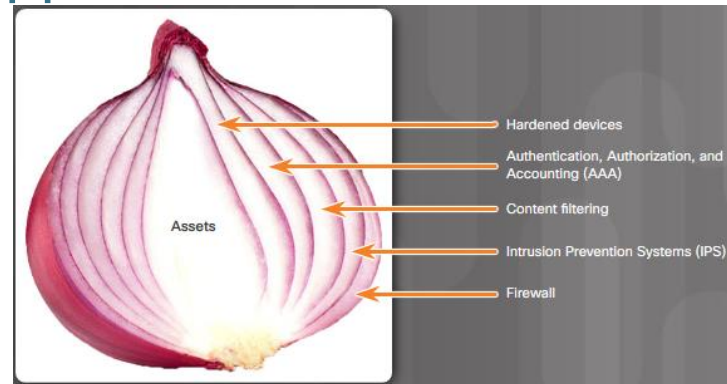
# Identify Threats

- Using a defense-in-depth approach to identify assets might include a topology with the following devices:
  - **Edge router** – first line of defense; configured with a set of rules specifying which traffic it allows or denies.
  - **Firewall** – A second line of defense; performs additional filtering, user authentication, and tracks the state of the connections.
  - **Internal router** – a third line of defense; applies final filtering rules on the traffic before it is forwarded to its destination.



# Security Onion and Security Artichoke Approaches

- The security onion analogy illustrates a layered approach to security.
- A threat actor would have to peel away at a network's defense mechanisms one layer at a time.
- However, with the evolution of borderless networks, a security artichoke is a better analogy.
- Threat actors may only need to remove certain "artichoke leaves" to access sensitive data.
- For example, a mobile device is a leaf that, when compromised, may give the threat actor access to sensitive information such as corporate email.
- The key difference between security onion and security artichoke is that not every leaf needs to be removed in order to get at the data.



# Business Policy

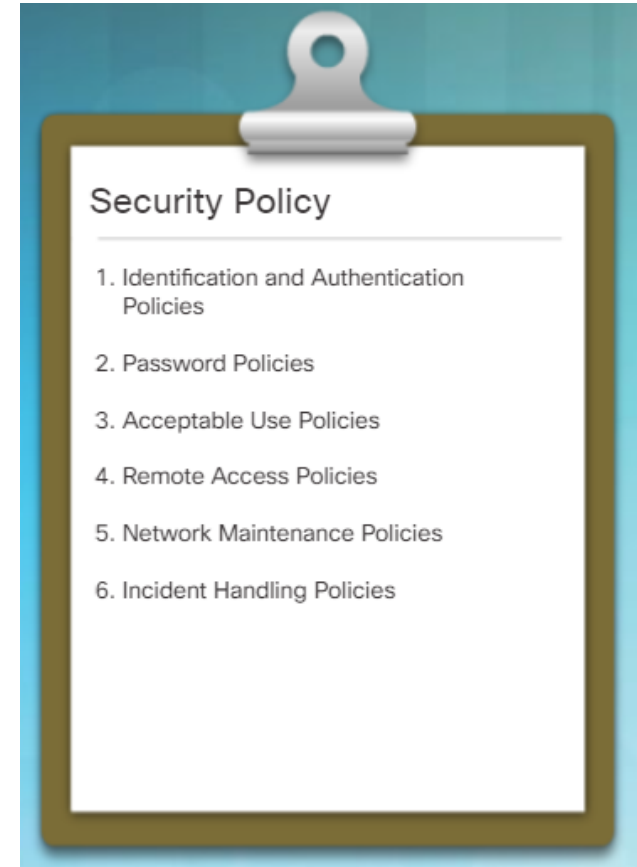
- Policies provide the foundation for network security by defining what is acceptable.
- Business policies are the guidelines developed by an organization that govern its actions and the actions of its employees.
- A organization may have several guiding policies:
  - **Company policies** - establish the rules of conduct and the responsibilities of both employees and employers.
  - **Employee policies** - identify employee salary, pay schedule, employee benefits, work schedule, vacations, and more.
  - **Security policies** - identify a set of security objectives for a company, define the rules of behavior for users and administrators, and specify system requirements.



## Security Policies

# Security Policy

- A comprehensive security policy has a number of 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.
- A security policy may include one or more of the items shown in the figure.
- An Acceptable Use Policy (AUP) is one of the most common policies and covers what users are allowed and not allowed to do on the various system components.



# Security Policies

## BYOD Policies

- Many organizations support Bring Your Own Device (BYOD), which enables employees to use their own mobile devices to access company resources.
- A BYOD policy should include:
  - 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 BYOD security best practices help mitigate BYOD risks:
  - Password protected access for each device and account.
  - Manually controlled wireless connectivity so the device only connects to trusted networks.
  - Keep software updated to mitigate against the latest threats.
  - Back up data in case device is lost or stolen.
  - Enable “Find my Device” locator services that can remotely wipe a lost device.
  - Provide antivirus software.
  - Use Mobile Device Management (MDM) software to enable IT teams to implement security settings and software configurations on all devices that connect to company networks.



## Regulatory and Standard Compliance

- Compliance regulations and standards 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.
- Specific compliance regulations will be discussed later in the course.



# 8.2 Access Control



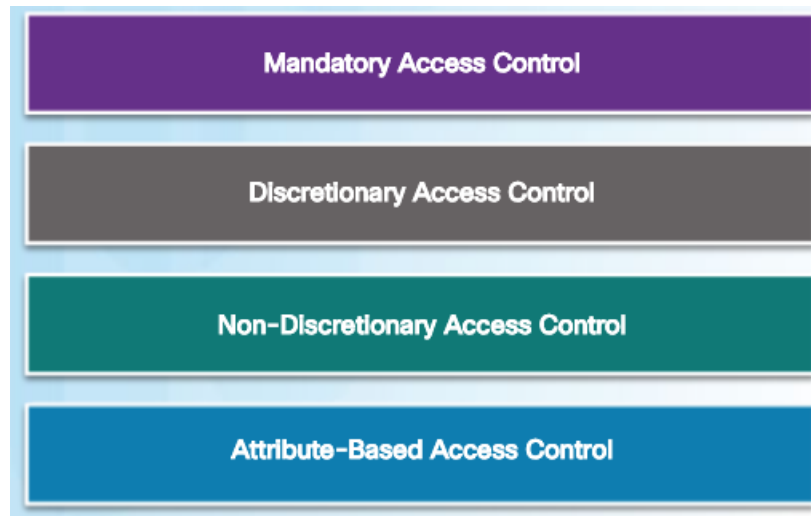
# Communications Security: CIA

- Information security deals with protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.
- The CIA triad consists of:
  - **Confidentiality** - only authorized entities can access information.
  - **Integrity** - information should be protected from unauthorized alteration.
  - **Availability** - information must be available to the authorized parties who require it, when they require it.



# Access Control Models

- Basic access control models include the following:
  - **Mandatory access control (MAC)** – applies the strictest access control, enabling user access based on security clearance.
  - **Discretionary access control (DAC)** – allows users to control access to their data as owners of that data.
  - **Non-Discretionary access control** – access is based on roles and responsibilities; also known as role-based access control (RBAC).
  - **Attribute-based access control (ABAC)** – access is based on attributes of the resource accessed, the user accessing it, and environmental factors, such as time of day.
- Another access control model is the principle of least privilege, which states that users should be granted the minimum amount of access required to perform their work function.



# AAA Usage and Operation

## AAA Operation

- Authentication, Authorization, and Accounting (AAA) is a scalable system for access control.
- **Authentication** - users and administrators must prove that they are who they say they are.
- **Authorization** - determines which resources the user can access and which operations the user is allowed to perform.
- **Accounting** - records what the user does and when they do it.

**Authentication**  
Who are you?

**Authorization**  
How much can you spend?

**Accounting**  
What did you spend it on?

Reference Number	Sold	Posted	Activity Since Last Statement	Amount
43210967	01-03	01-13	Payment, Thank You	-\$74.25
01234567	01-12	01-15	Wings 'N' Things Anytown, USA	\$25.25
78901234	01-14	01-17	Record Release Anytown, USA	\$40.00
45678901	01-14	01-17	Sports Stadium Anytown, USA	\$75.25
3210987	01-22	01-23	Tie Rack Anytown, USA	\$20.75
76543210	01-29	01-30	Electronic World Anytown, USA	\$89.25
2345678		01-30	Transaction Fees	\$3.00
567890		01-01	Annual Fee	\$25.00

# AAA Authentication

- Two common AAA authentication methods include:
  - **Local AAA Authentication** - This method authenticates users against locally stored usernames and passwords. Local AAA is ideal for small networks.
  - **Server-Based AAA Authentication** – This method authenticates against a central AAA server that contains the usernames and passwords for all users. Server-based AAA authentication is appropriate for medium-to-large networks.
- The process for both types are shown on the next slide.

# AAA Usage and Operation

## AAA Authentication (Cont.)

### Local AAA Authentication



1. The client establishes a connection with the router.
2. The AAA router prompts the user for a username and password.
3. The router authenticates the username and password using the local database and the user is provided access to the network based on information in the local database.

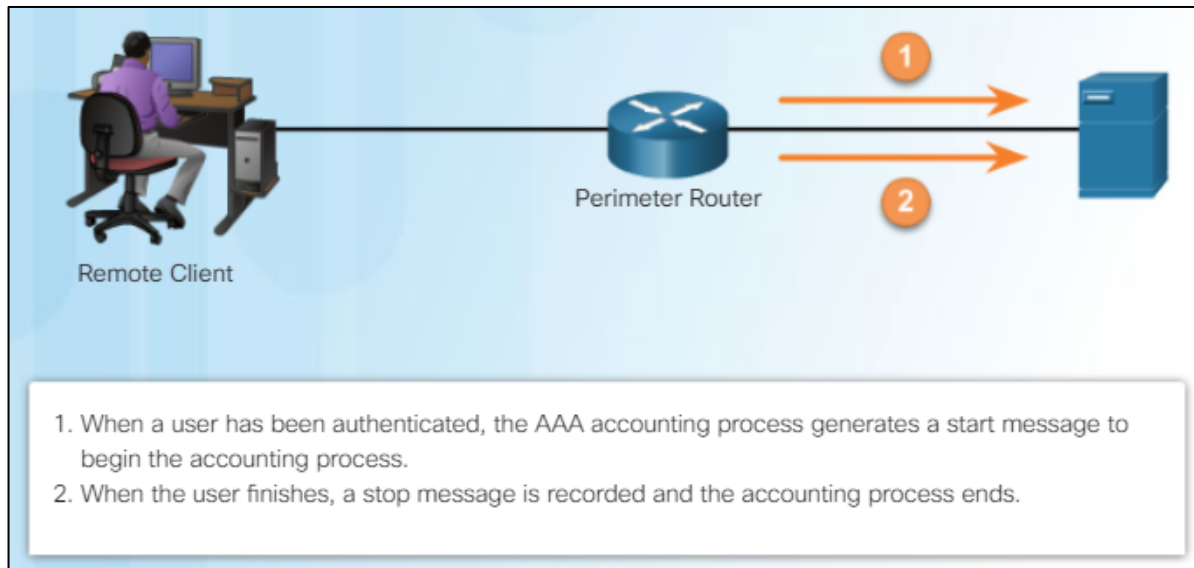
### Server-Based AAA Authentication



1. The client establishes a connection with the router.
2. The AAA router prompts the user for a username and password.
3. The router authenticates the username and password using a remote AAA server.
4. The user is provided access to the network based on information in the remote AAA server.

# AAA Accounting Logs

- Accounting provides more security than just authentication.
- AAA servers keep a detailed log of exactly what the authenticated user does on the device.



# AAA Accounting Logs (Cont.)

- The various types of accounting information that can be collected include:
  - **Network Accounting** - captures information such as packet and byte counts.
  - **Connection Accounting** - captures information about all outbound connections.
  - **EXEC Accounting** - captures information about user shells including username, date, start and stop times, and the access server IP address.
  - **System Accounting** - captures information about all system-level events.
  - **Command Accounting** - captures information about executed shell commands.
  - **Resource Accounting** - captures "start" and "stop" record support for calls that have passed user authentication.



## 8.3 Threat Intelligence



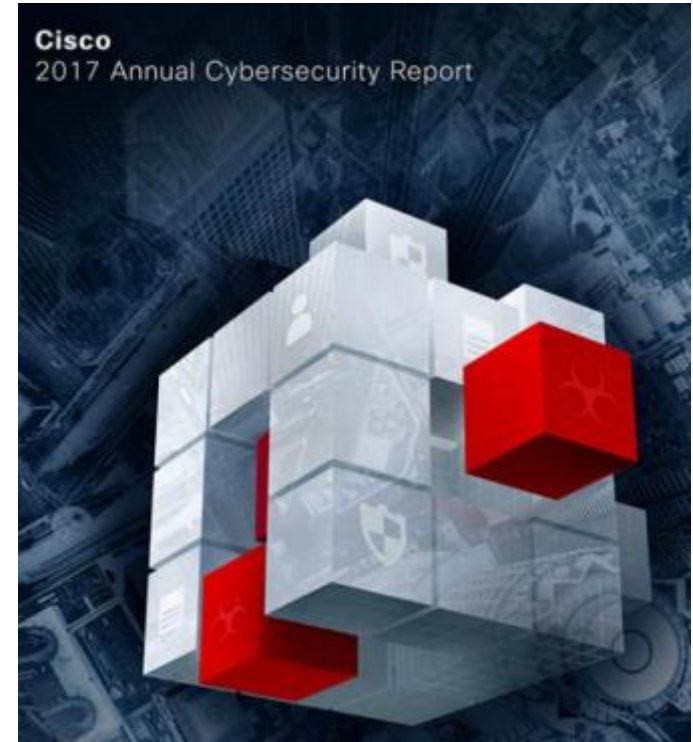
## Network Intelligence Communities

- Threat intelligence organizations such as CERT, SANS, and MITRE offer detailed threat information that is vital to cybersecurity practices.



## Cisco Cybersecurity Reports

- Cisco offers their Cybersecurity Report annually, which provides an update on the state of security preparedness, expert analysis of top vulnerabilities, factors behind the explosion of attacks using adware and spam, and more.



# Security Blogs and Podcasts

- Security blogs and podcasts help cybersecurity professionals understand and mitigate emerging threats.



# Threat Intelligence Services

## Cisco Talos

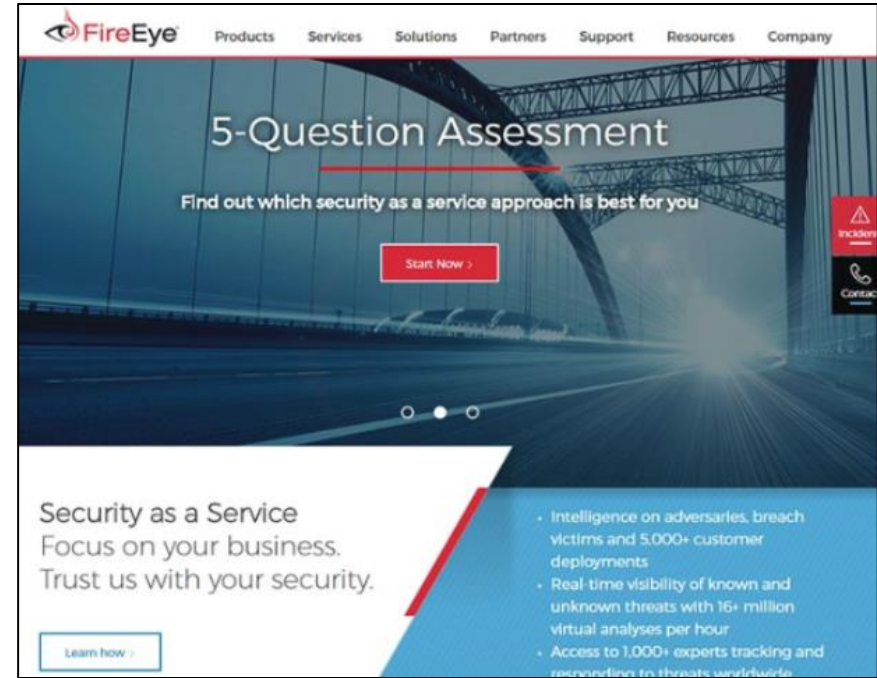
- Threat intelligence services allow the exchange of threat information such as vulnerabilities, indicators of compromise (IOC), and mitigation and detection techniques.
- The Cisco Talos collects information about active, existing, and emerging threats. Talos then provides to its subscribers comprehensive protection against these attacks and malware.



# Threat Intelligence Services

## FireEye

- FireEye is another security company that offers services to help enterprises secure their networks.
- FireEye offers emerging threat information and threat intelligence reports.



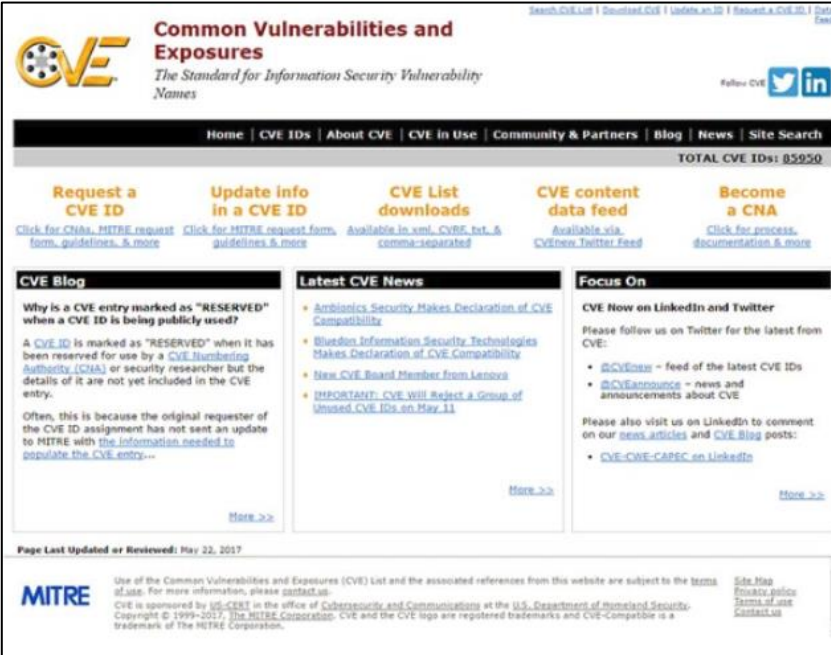
# Automated Indicator Sharing

- Automated Indicator Sharing (AIS) is program which allows the U.S. Federal Government and the private sector to share threat indicators.
- AIS creates an ecosystem where, as soon as a threat is recognized, it is immediately shared with the community.



# Common Vulnerabilities and Exposures Database

- Common Vulnerabilities and Exposures (CVE) is a database of vulnerabilities that uses a standardized naming scheme to facilitate the sharing of threat intelligence.



The screenshot shows the homepage of the Common Vulnerabilities and Exposures (CVE) database. At the top, there is a navigation bar with links for Search, CVE List, Download, CVE, Update, an ID, Request a CVE ID, and Data Feed. The main header features the CVE logo, the title "Common Vulnerabilities and Exposures", and the tagline "The Standard for Information Security Vulnerability Names". Social media links for Twitter and LinkedIn are also present. Below the header is a secondary navigation bar with links for Home, CVE IDs, About CVE, CVE in Use, Community & Partners, Blog, News, and Site Search. A status bar indicates "TOTAL CVE IDs: 85950". The main content area is divided into five columns: "Request a CVE ID" (with a link to the MITRE request form), "Update info in a CVE ID" (with a link to the MITRE request form), "CVE List downloads" (with a link to the CVE list in XML), "CVE content data feed" (with a link to the CVE content data feed), and "Become a CNA" (with a link to the CVE process documentation). Below these columns are three sections: "CVE Blog" (with an article about "RESERVED" CVE IDs), "Latest CVE News" (with a list of recent news items), and "Focus On" (with a section about CVE on LinkedIn and Twitter). The footer contains the MITRE logo, a disclaimer about the use of the CVE list, and links to the Terms of Use, Privacy Policy, and Contact Us.

**Common Vulnerabilities and Exposures**  
The Standard for Information Security Vulnerability Names

Search CVE List | Download CVE | Update an ID | Request a CVE ID | Data Feed

Home | CVE IDs | About CVE | CVE in Use | Community & Partners | Blog | News | Site Search

TOTAL CVE IDs: 85950

**Request a CVE ID**  
[Click for CVEs, MITRE request form, guidelines, & more](#)

**Update info in a CVE ID**  
[Click for MITRE request form, guidelines, & more](#)

**CVE List downloads**  
[Available in xml, CVE list, & comma-separated](#)

**CVE content data feed**  
[Available via CVEnews Twitter Feed](#)

**Become a CNA**  
[Click for process, documentation, & more](#)

**CVE Blog**

Why is a CVE entry marked as "RESERVED" when a CVE ID is being publicly used?

A CVE ID is marked as "RESERVED" when it has been reserved for use by a [CVE Numbering Authority \(CNA\)](#) or security researcher but the details of it are not yet included in the CVE entry.

Often, this is because the original requester of the CVE ID assignment has not sent an update to MITRE with the [information needed to populate the CVE entry](#)...

[More >>](#)

**Latest CVE News**

- [Ambionics Security Makes Declaration of CVE Compatibility](#)
- [Bluelord Information Security Technologies Makes Declaration of CVE Compatibility](#)
- [New CVE Board Member from Lenovo](#)
- [IMPORTANT: CVE Will Reject a Group of Unused CVE IDs on May 11](#)

[More >>](#)

**Focus On**

**CVE Now on LinkedIn and Twitter**

Please follow us on Twitter for the latest from CVE:

- [@CVEnews](#) - feed of the latest CVE IDs
- [@CVEannounce](#) - news and announcements about CVE

Please also visit us on LinkedIn to comment on our [news articles](#) and [CVE Blog](#) posts:

- [CVE-CWE-CAPEC on LinkedIn](#)

[More >>](#)

Page Last Updated or Reviewed: May 22, 2017

**MITRE**

Use of the Common Vulnerabilities and Exposures (CVE) List and the associated references from this website are subject to the [Terms of Use](#). For more information, please [contact us](#).


CVE is sponsored by [US-CERT](#) in the office of Cybersecurity and Communications at the U.S. Department of Homeland Security. Copyright © 1999-2017 The MITRE Corporation. CVE and the CVE logo are registered trademarks and CVE-Compatible is a trademark of The MITRE Corporation.

[Site Map](#)  
[Privacy Policy](#)  
[Terms of Use](#)  
[Contact Us](#)



# Threat Intelligence Communication Standards

- Cyber Threat Intelligence (CTI) standards such as STIX and TAXII facilitate the exchange of threat information by specifying data structures and communication protocols:
- **Structured Threat Information Expression (STIX)** - specifications for exchanging cyber threat information between organizations.
- **Trusted Automated Exchange of Indicator Information (TAXII)** – specification for an application layer protocol that allows the communication of CTI over HTTPS. TAXII is designed to support STIX.



A structured language for cyber threat intelligence


[Read the Latest Specification! \(2.0 CSD 1\)](#)

[STIX 2.0 Public Review -- Frequently Asked Questions](#)


Structured Threat Information Expression (STIX™) is a language and serialization format used to exchange cyber threat intelligence (CTI).

STIX enables organizations to share CTI with one another in a consistent and machine readable manner, allowing security communities to better understand what computer-based attacks they are most likely to see and to anticipate and/or respond to those attacks faster and more effectively.

STIX is designed to improve many different capabilities, such as collaborative threat analysis, automated threat exchange, automated detection and response, and more.



STIX Relationship Diagram with Sighting




A transport mechanism for sharing cyber threat intelligence

[Read the Latest Specification! \(Draft 2\)](#)

Trusted Automated Exchange of Intelligence Information (TAXII™) is an application layer protocol for the communication of cyber threat information in a simple and scalable manner.

TAXII is a protocol used to exchange cyber threat intelligence (CTI) over HTTPS. TAXII enables organizations to share CTI by defining an API that aligns with common sharing models.

TAXII is specifically designed to support the exchange of CTI represented in STIX.



TAXII Collections and Channels

Links:

- [Archive of TAXII 1.x](#)



# 8.4 Summary

## Chapter Summary

# Summary

- Cybersecurity risk consists of assets, vulnerabilities, and threats.
- Assets constitute the attack surface that threat actors could target.
- Vulnerabilities include any exploitable weakness in a system or its design.
- Threats are best mitigated using a defense-in-depth approach.
- The security onion analogy illustrates a layered approach to security.
- The security artichoke analogy better represents today's networks.
- Business policies are the guidelines developed by an organization to govern its actions and the actions of its employees.
- A security policy identifies a set of security objectives for a company, defines the rules of behavior for users and administrators, and specifies system requirements.

# Summary (Cont.)

- A BYOD policy, which enables employees to use their own mobile devices to access company resources, governs which employees are allowed to access what resources using their personal devices.
- All organizations have to comply with regulations specific to the type of organization and the data the organization handles.
- The CIA triad consists of confidentiality, integrity, and availability.
- Basic access control models include the following:
  - Mandatory access control (MAC)
  - Discretionary access control (DAC)
  - Non-Discretionary access control
  - Attribute-based access control (ABAC)
  - Principle of least privilege

# Summary (Cont.)

- AAA access control includes the authentication, authorization, and accounting.
- Two common authentication methods are Local AAA Authentication and Server-based AAA Authentication.
- AAA accounting keeps a detailed log of exactly what the authenticated user does on the device.
- AAA accounting logs include:
  - Network Accounting
  - Connection Accounting
  - EXEC Accounting
  - System Accounting
  - Command Accounting
  - Resource Accounting

# Summary (Cont.)

- Threat intelligence organizations such as CERT, SANS, and MITRE offer detailed threat information that is vital to cybersecurity practices.
- Cisco's Cybersecurity Report provides an update on the state of security.
- Security blogs and podcasts help cybersecurity professionals understand and mitigate emerging threats.
- Threat intelligence services allow the exchange of threat information.
- FireEye offers emerging threat information and threat intelligence reports.
- AIS creates an ecosystem where, as soon as a threat is recognized, it is immediately shared with the community.
- The CVE database uses a standardized naming scheme to facilitate the sharing of threat intelligence.
- The STIX and TAXII standards facilitate the exchange of threat information by specifying data structures and communication protocols.

# New Terms

- Acceptable use policy (AUP)
- asset
- Attribute-based access control (ABAC)
- Authentication, Authorization, and Accounting (AAA)
- Availability
- Bring Your Own Device (BYOD)
- Company policies
- Confidentiality
- Discretionary access control (DAC)
- edge router
- Employee policies
- Integrity
- Mandatory access control (MAC)
- Non-Discretionary access control
- privilege escalation
- security artichoke
- security onion
- Security policies

# Cybersecurity Operations Certification

This chapter covers the following areas in the Cybersecurity Operations Certification:

From 210-250 SECFND - Understanding Cisco Cybersecurity Fundamentals:

- **Domain 2: Security Concepts**

- 2.1 Describe the principles of the defense in depth strategy
- 2.4 Describe the following security terms:
  - Principle of least privilege
- 2.5 Compare and contrast the following access control models:
  - Discretionary Access Control
  - Mandatory Access Control
  - Non-Discretionary Access Control
- 2.7 Describe the following concepts:
  - Asset management
  - Configuration management
  - Mobile device management

- **Domain 6: Attack Methods**

- 6.7 Define privilege escalation

