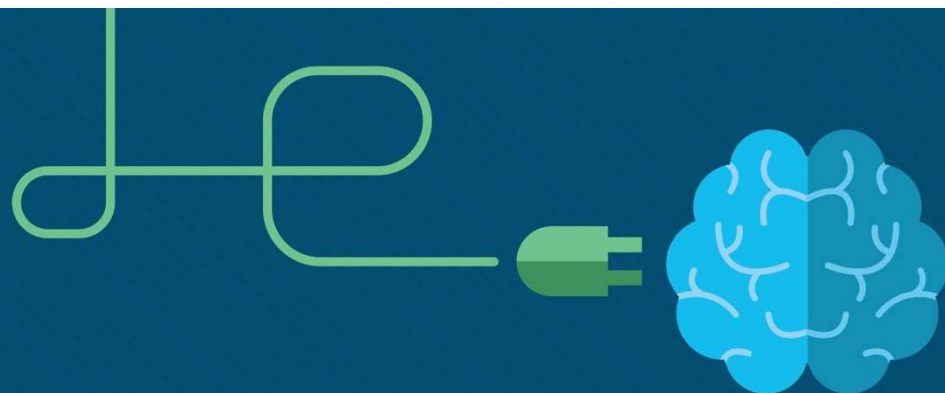




# DIGITAL TALENT SCHOLARSHIP 2019





# 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

## Defense-in-Depth

# 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

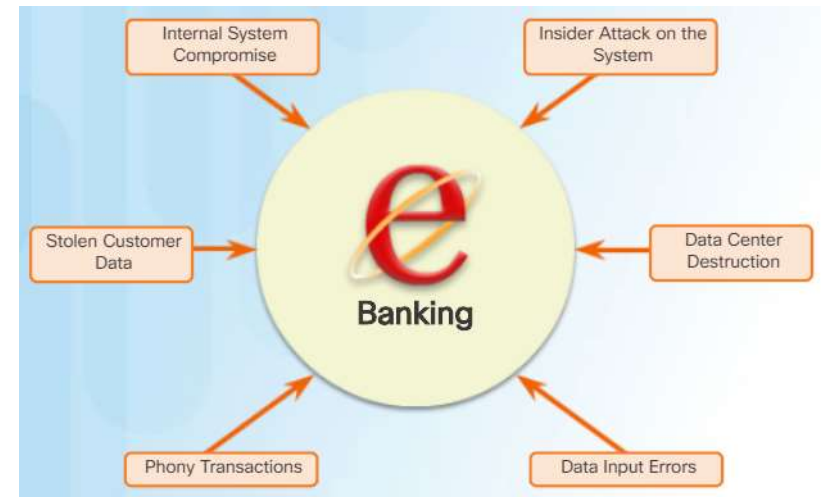
- Many organizations only have a general idea of the assets that need to be protected.
- All the devices and information owned or managed by the organization are the assets.
- Assets constitute the attack surface that threat actors could target.
- Asset management consists of:
  - Inventorying all assets.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



## Defense-in-Depth

# Identify Vulnerabilities

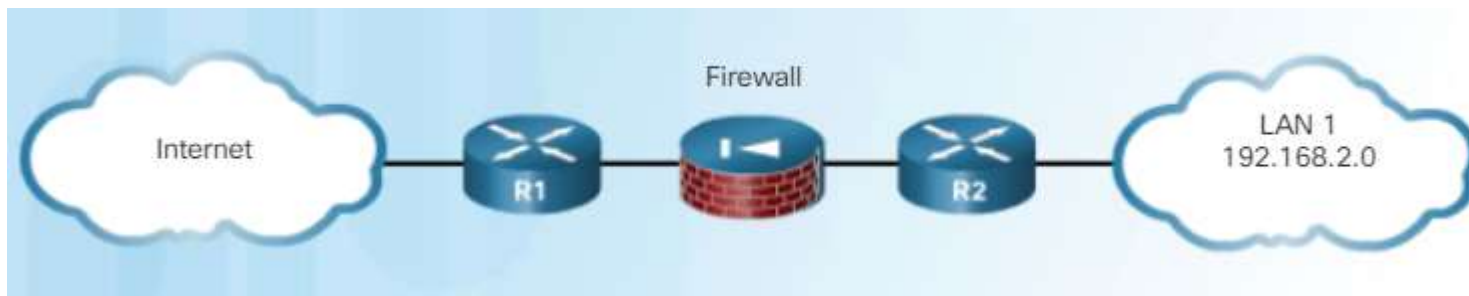
- Identifying vulnerabilities includes answering the following questions:
  - What are the vulnerabilities?
  - Who might exploit the vulnerabilities?
  - What are the consequences if the vulnerability is exploited?
- For example, an e-banking system might have the following threats:
  - Internal system 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.

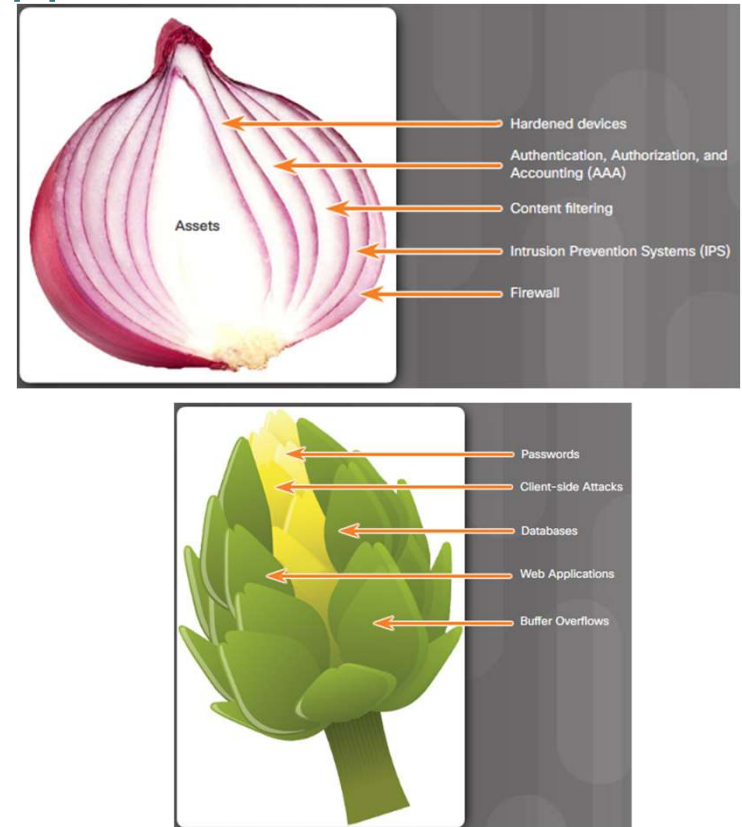




## Defense-in-Depth

# 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.



## Security Policies

# Business Policy

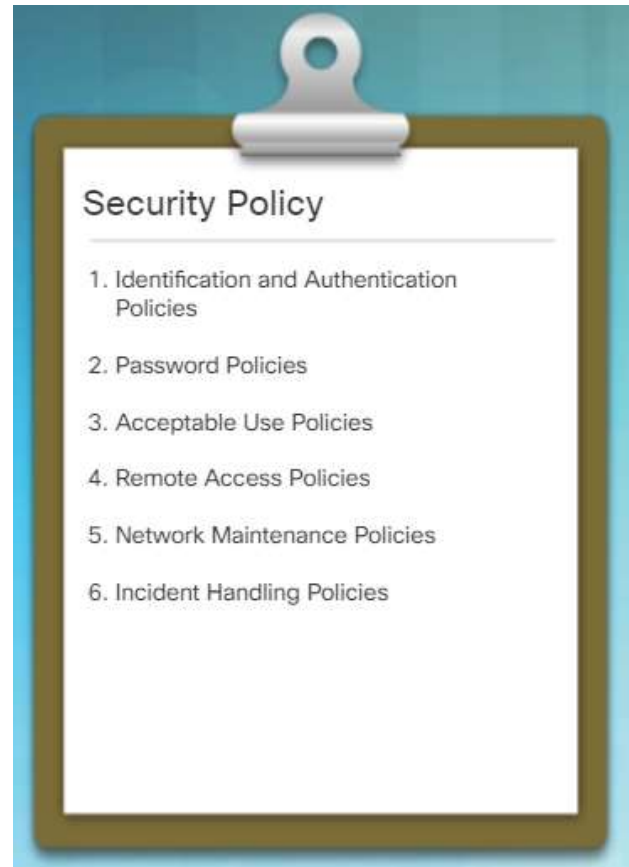
- Policies provide the foundation for network security by defining what is acceptable.
- Business policies are the guidelines developed by an organization that govern its actions and the actions of its employees.
- A organization may have several guiding policies:
  - **Company policies** - establish 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.



## Security Policies

# 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.



## Security Policies

# 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.

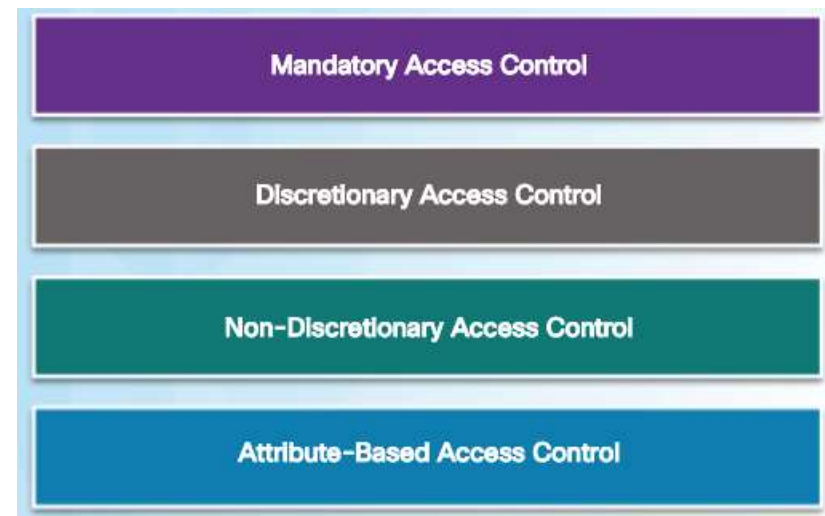




## Access Control Concepts

# 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?

Account Number: 1234-567-890 Statement Closing Date: 01-31-01 Current Account Due: \$278.50

JOE EMPLOYEE  
400 SKYVIEW DRIVE  
HUNTSVILLE, USA 35890-1234  
872519345 000782550000000003

MAIL PAYMENT TO:  
THE BANK  
100 VINE STREET  
HUNTSVILLE, USA 35890-1234

Detach here and return upper portion with check or money order. Do not staple or fold.

**Statement of Personal Credit Card Account**  
Return this portion for your file.

Cardmember Name: JOE EMPLOYEE Account Number: 1234-456-890 Statement Closing Date: 01-31-01

Statement Date: 02-01-01 Payment Due Date: 03-01-01

Closing Date: 01-31-01

Credit Limit: \$1,500.00 Credit Available: \$1,221.50

Next Billing: \$278.50 Minimum Payment Due: \$25.00

**Account Summary**

Previous Balance:	+74.34	Transaction Fee:	+3.00
Purchases:	+258.58	Annual Fee:	+25.00
Cash Advances:	+0	Current Amount Due:	+258.58
Payments:	-74.25	Amount Past Due:	+0
Finance Charge:	+0	Amount Over Credit Limit:	+0
Late Charge:	+0	<b>NEW BALANCE:</b>	<b>\$278.50</b>

Reference Number	Sold	Posted	Activity Since Last Statement	Amount
43210987	01-08	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
43878901	01-14	01-17	Sports Stadium Anytown, USA	\$75.25
3210987	01-23	01-23	Tie Tack Anytown, USA	\$20.75
78543210	01-26	01-30	Electronic Music Anytown, USA	\$68.25
23456789	01-30	01-30	Transaction Fees	\$3.00
34567890	01-01	01-01	Annual Fee	\$25.00

PAGE: 1 OF 1

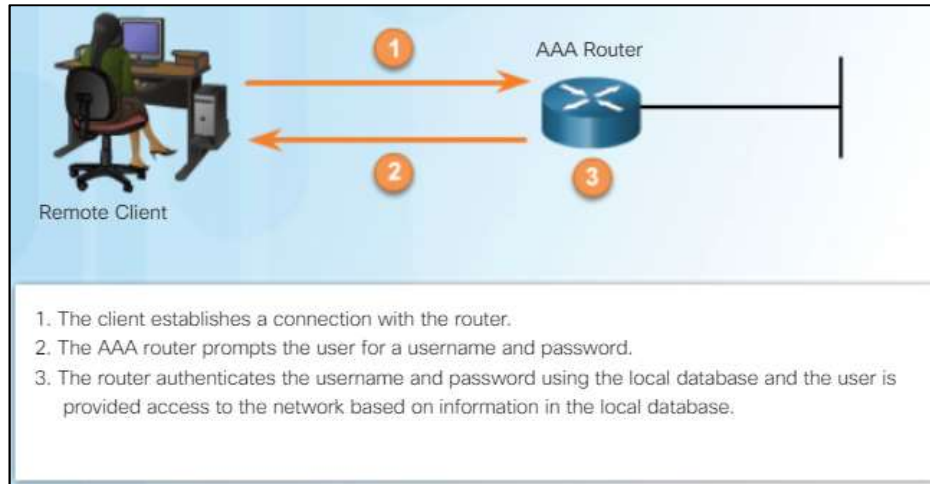
## AAA Authentication

- 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.

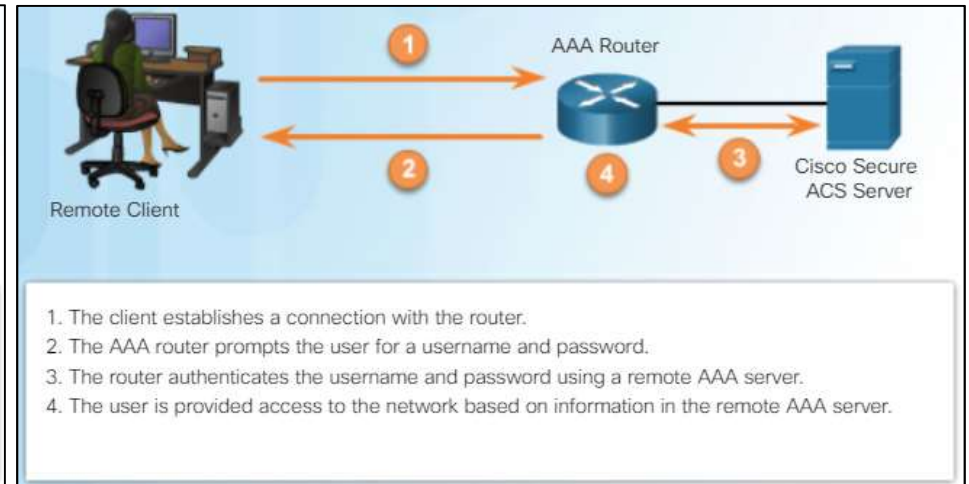
## AAA Usage and Operation

### AAA Authentication (Cont.)

#### Local AAA Authentication



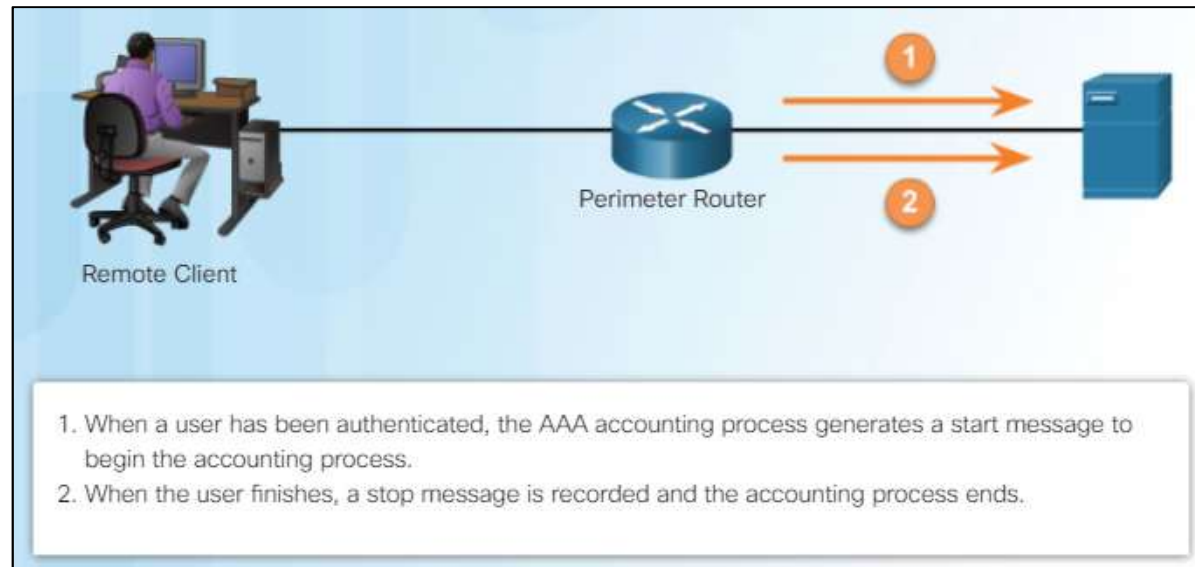
#### Server-Based AAA Authentication



## AAA Usage and Operation

# 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 Usage and Operation

# 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

## Information Sources

# Network Intelligence Communities

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

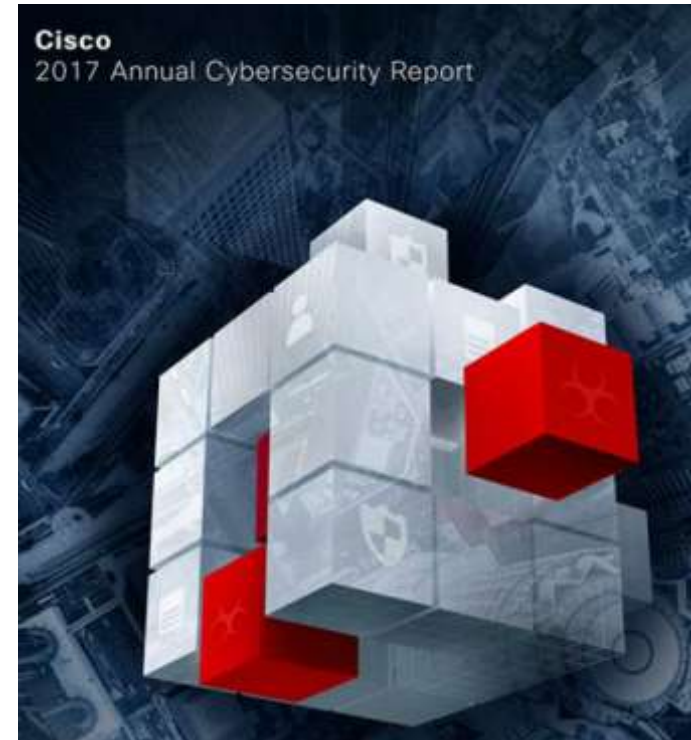




## Information Sources

# 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.



## Information Sources

# Security Blogs and Podcasts

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



## Threat Intelligence Services

# Cisco Talos

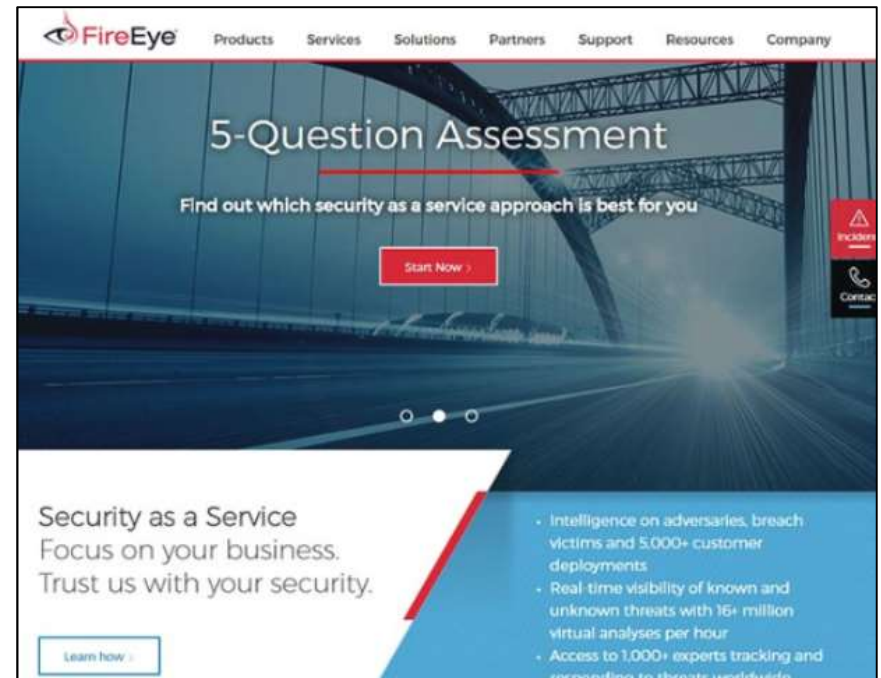
- Threat intelligence services allow the exchange of threat information such as vulnerabilities, indicators of compromise (IOC), and mitigation and detection techniques.
- The Cisco Talos collects information about active, existing, and emerging threats. Talos then provides to its subscribers comprehensive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



## Threat Intelligence Services

# Automated Indicator Sharing

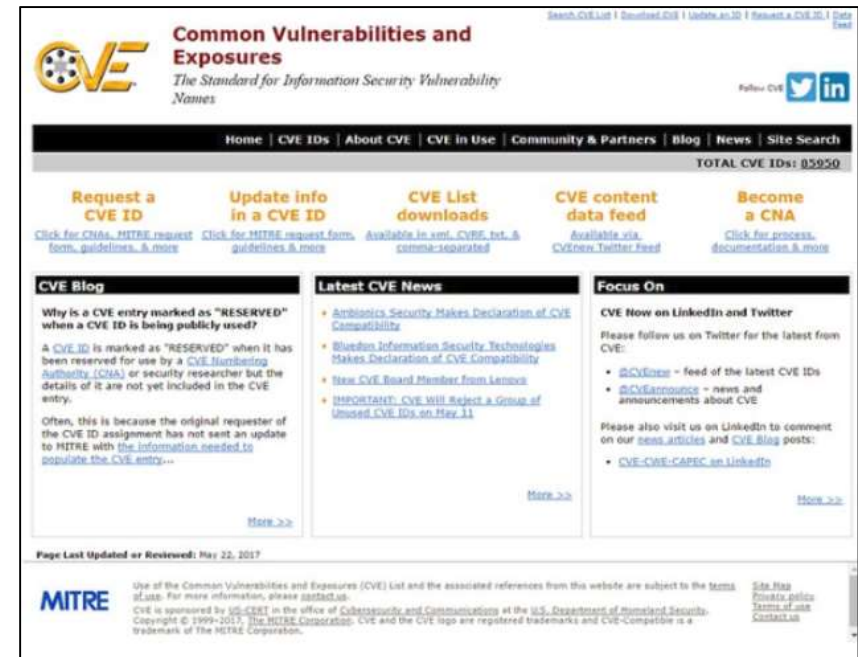
- Automated Indicator Sharing (AIS) is program which allows the U.S. Federal Government and the private sector to share threat indicators.
- AIS creates an ecosystem where, as soon as a threat is recognized, it is immediately shared with the community.



## Threat Intelligence Services

# 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.



## Threat Intelligence Services

# 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.

## Chapter Summary

### 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

## Chapter Summary

### 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

## Chapter Summary

### 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.

## Chapter 8

# 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



IKUTI KAMI



- digitalent.kominfo
- digitalent.kominfo
- DTS\_kominfo
- Digital Talent Scholarship 2019

Pusat Pengembangan Profesi dan Sertifikasi  
Badan Penelitian dan Pengembangan SDM  
Kementerian Komunikasi dan Informatika  
Jl. Medan Merdeka Barat No. 9  
(Gd. Belakang Lt. 4 - 5)  
Jakarta Pusat, 10110

