

Protecting the Network



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.

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.

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.

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

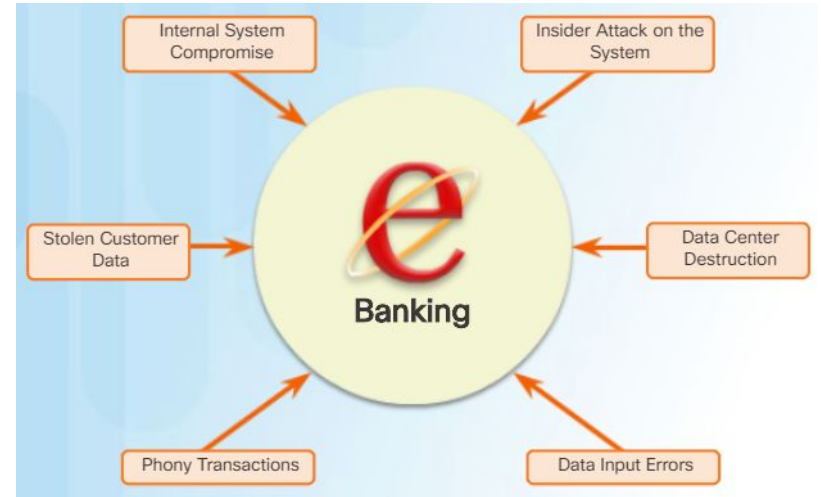
Identify Assets

- 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.



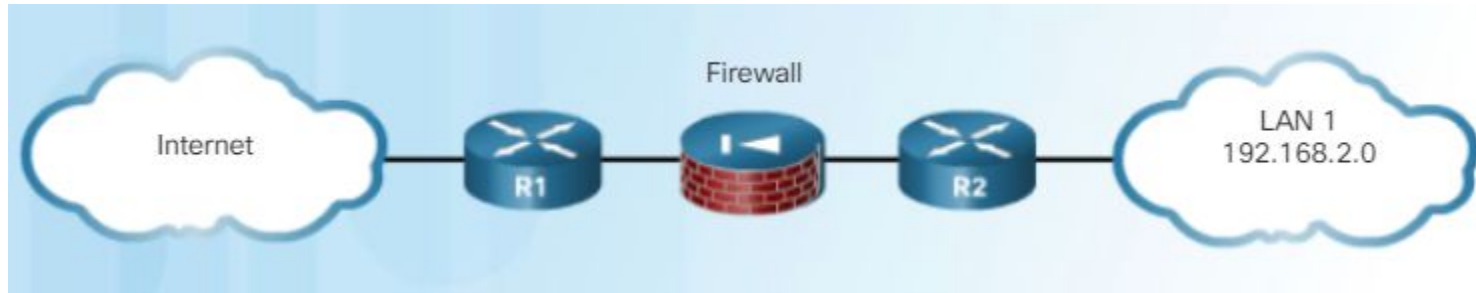
Identify Vulnerabilities

- 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



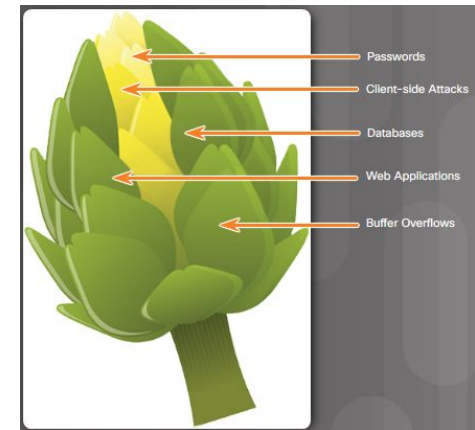
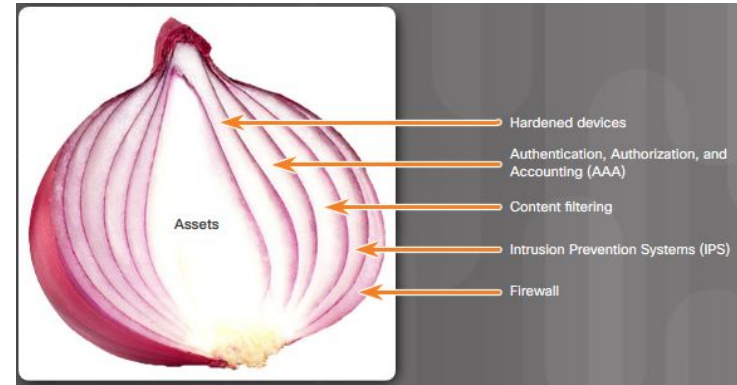
Identify Threats

- 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.



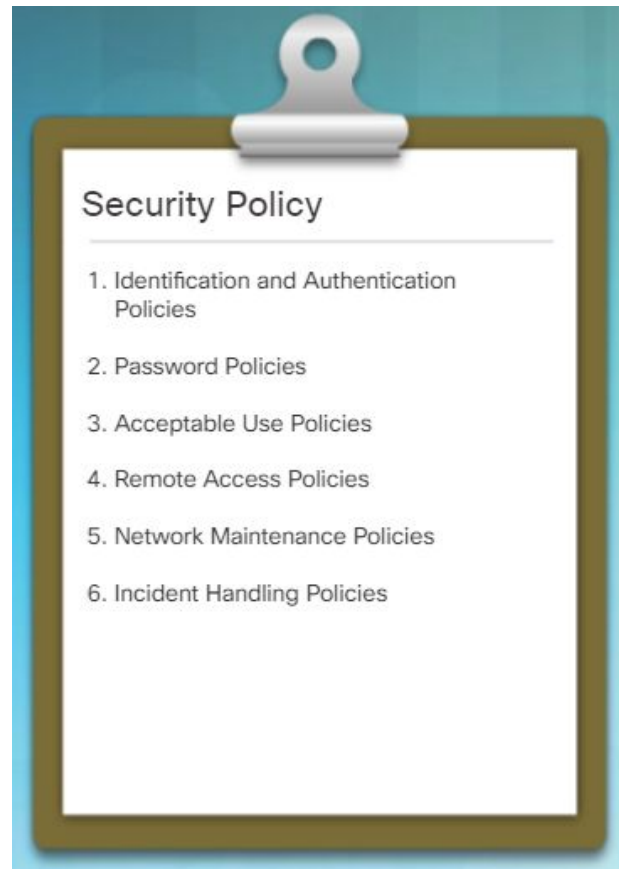
Business Policy

- 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 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.



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.



Access Control

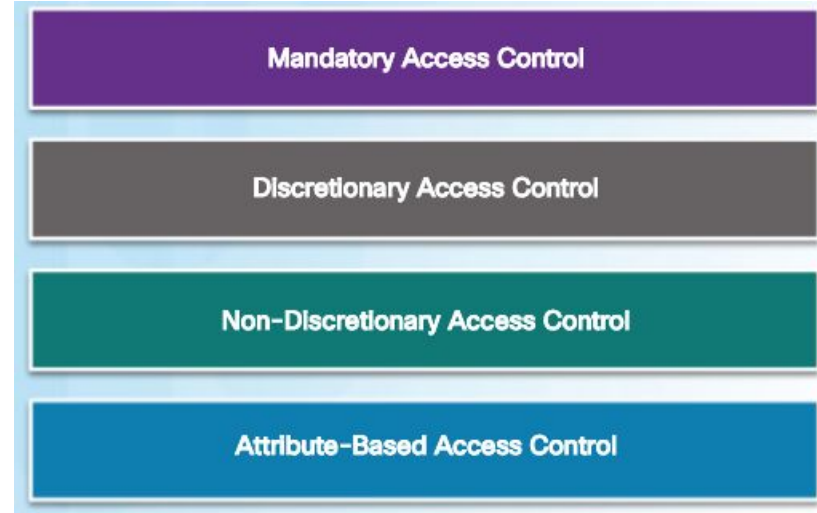
Communications Security: CIA

- 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

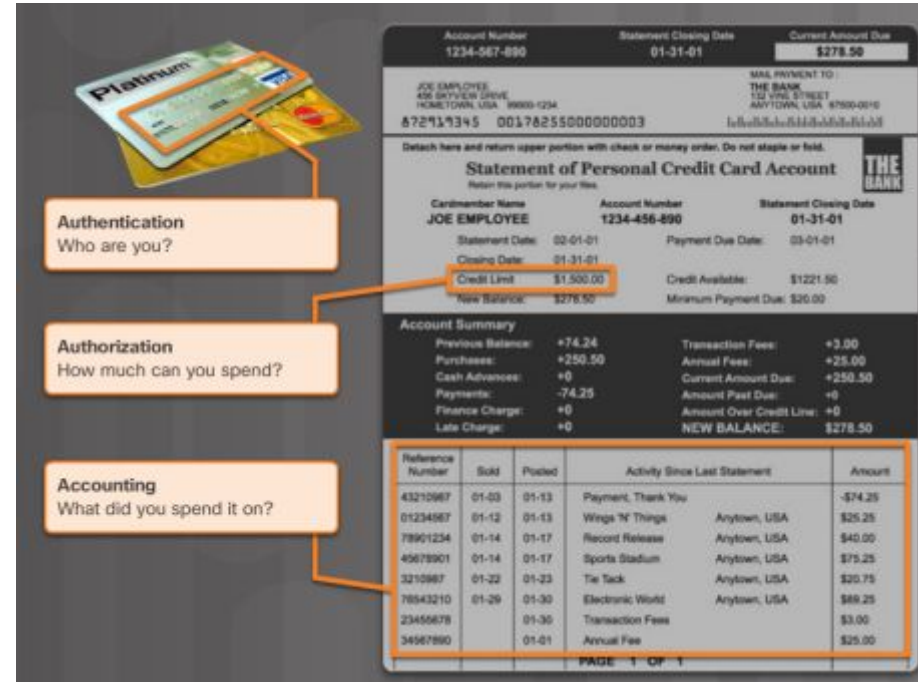
- Basic access control models include the following:
 - **Mandatory access control (MAC)** – applies the strictest access control, enabling user access based on security clearance.
 - **Discretionary access control (DAC)** – allows users to control access to their data as owners of that data.
 - **Non-Discretionary 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.



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.

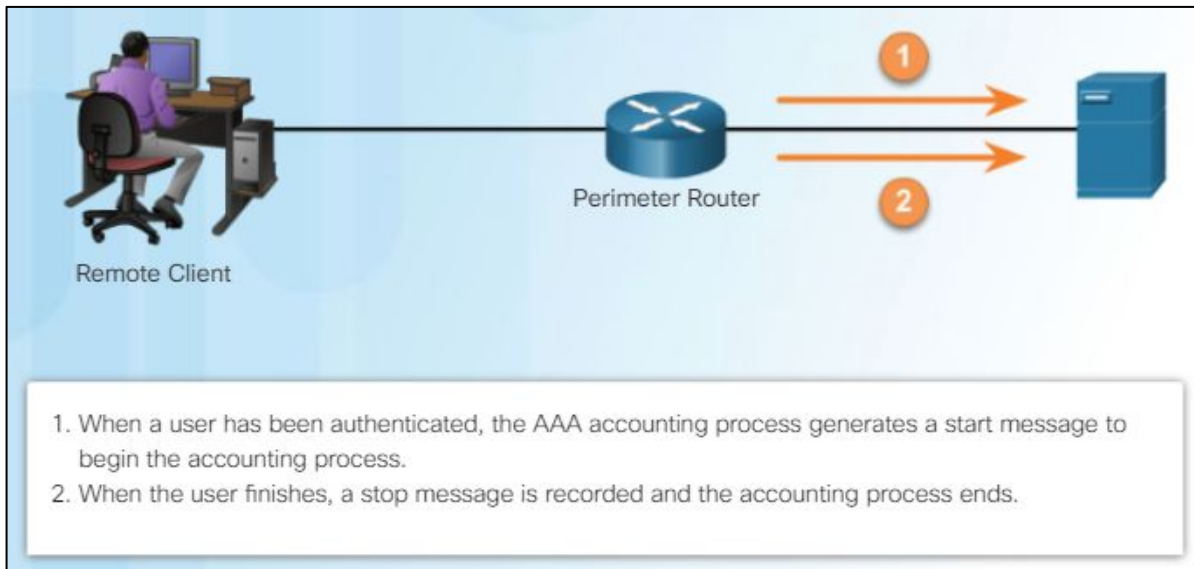
Server-Based AAA Authentication



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.



Threat Intelligence

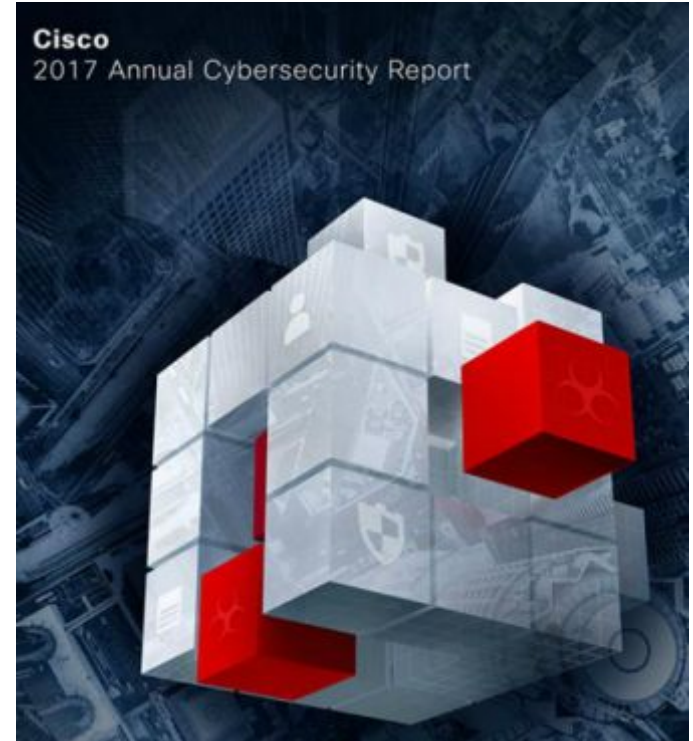
Network Intelligence Communities

- 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.

The screenshot displays the Cisco Blogs website. The top navigation bar includes the Cisco logo, "Cisco Blogs", a search bar, and a "Log In to Cisco.com" button. Below the navigation bar, there are tabs for "All Blogs", "Technologies", "Industries", "Partners", "For the Tech Expert", "Get to Know Cisco", and "Countries and Regions". The main content area is titled "Cisco Blog" and "Security". It features a "Most Recent" tab selected, along with "Most Commented" and "Recommended" options. Two blog posts are visible: "Threat Round-up for May 19 - May 26" by Talos Group and "How to protect against the most advanced email-based attacks" by Lindsay van Gemert. The right sidebar contains a "Let Us Help" section with contact information, a "Subscribe to Security" form, and a "Connect with Security" section with social media icons. At the bottom right, there is a "Cisco Social Rewards" banner.

Cisco Talos

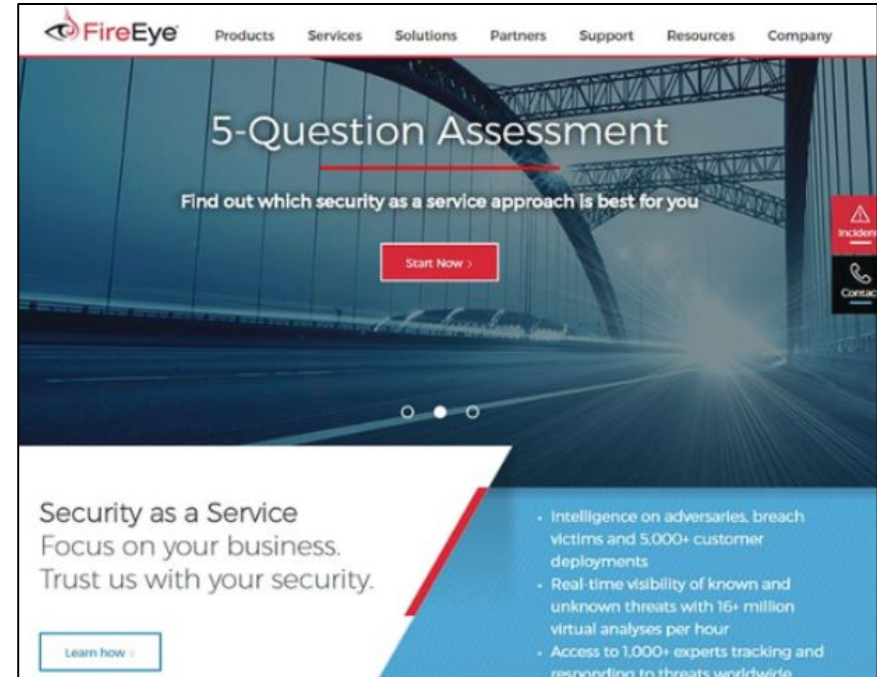
- Threat intelligence services allow the exchange of threat information such as vulnerabilities, indicators of compromise (IOC), and mitigation and detection techniques.
- The Cisco Talos collects information about active, existing, and emerging threats. Talos then provides to its subscribers comprehensive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



The screenshot shows the FireEye website's landing page for a '5-Question Assessment'. The page features a dark blue background with a bridge structure. The main heading is '5-Question Assessment' with a sub-headline 'Find out which security as a service approach is best for you'. A red 'Start Now >' button is prominently displayed. Below this, there is a white section with the text 'Security as a Service Focus on your business. Trust us with your security.' and a 'Learn how >' button. To the right, a list of benefits is provided, including intelligence on adversaries, real-time visibility of threats, and access to experts. The top navigation bar includes links for Products, Services, Solutions, Partners, Support, Resources, and Company. On the right side, there are icons for 'Incident' and 'Contact'.

FireEye Products Services Solutions Partners Support Resources Company

5-Question Assessment

Find out which security as a service approach is best for you

Start Now >

Security as a Service
Focus on your business.
Trust us with your security.

Learn how >

- Intelligence on adversaries, breach victims and 5,000+ customer deployments
- Real-time visibility of known and unknown threats with 16+ million virtual analyses per hour
- Access to 1,000+ experts tracking and responding to threats worldwide

Incident
Contact

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.



The screenshot shows the DHS website page for Automated Indicator Sharing (AIS). The page features a dark blue header with the DHS logo and navigation links. The main content area is white and contains the following text:

Automated Indicator Sharing (AIS)

The Department of Homeland Security's (DHS) free Automated Indicator Sharing (AIS) capability enables the exchange of cyber threat indicators between the Federal Government and the private sector at machine speed. Threat indicators are pieces of information like malicious IP addresses or the sender address of a phishing email (although they can also be much more complicated).

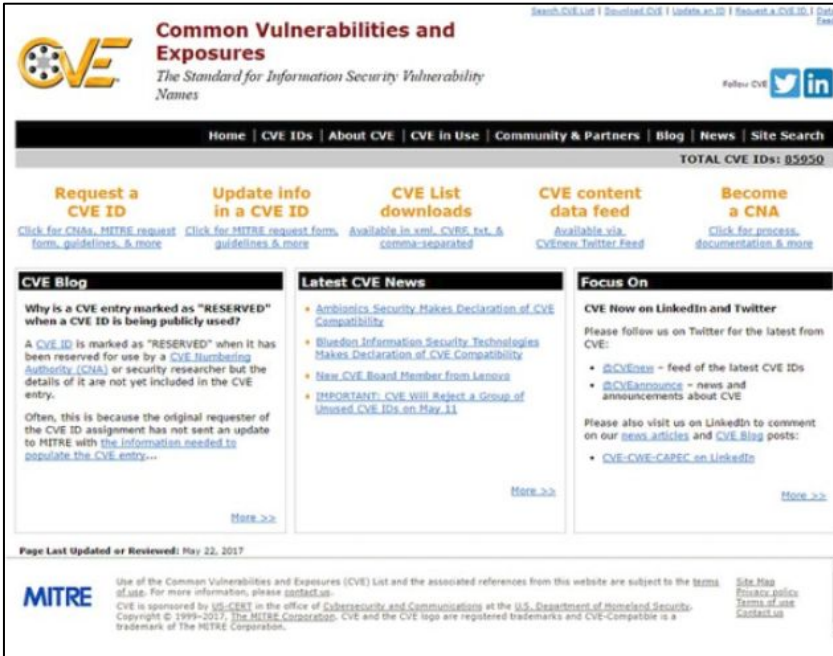
AIS is a part of the Department's effort to create an ecosystem where as soon as a company or federal agency observes an attempted compromise, the indicator will be shared in real time with all of our partners, protecting them from that particular threat. That means adversaries can only use an attack once, which increases their costs and ultimately reduces the prevalence of cyber attacks. While AIS won't eliminate sophisticated cyber threats, it will allow companies and federal agencies to concentrate more on them by clearing away less sophisticated attacks.

Ultimately, the goal is to commoditize cyber threat indicators through AIS so that tactical indicators are shared broadly among the public and private sector, enabling everyone to be better protected against cyber attacks.

[Expand All Sections](#)

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. The header includes the CVE logo, the title "Common Vulnerabilities and Exposures", and the tagline "The Standard for Information Security Vulnerability Names". Navigation links include Home, CVE IDs, About CVE, CVE in Use, Community & Partners, Blog, News, and Site Search. A search bar is located in the top right corner. Below the navigation is a banner for "TOTAL CVE IDs: 85950". The main content area is divided into five columns: "Request a CVE ID", "Update info in a CVE ID", "CVE List downloads", "CVE content data feed", and "Become a CNA". Each column contains a brief description and a link to the relevant page. Below this are three sections: "CVE Blog", "Latest CVE News", and "Focus On". The "CVE Blog" section discusses why a CVE entry is marked as "RESERVED". The "Latest CVE News" section lists recent updates, including a declaration of CVE compatibility by Arbinetica Security and a new CVE Board member from Lenovo. The "Focus On" section encourages users to follow CVE on LinkedIn and Twitter. At the bottom, there is a footer with the MITRE logo, a disclaimer about the use of CVE information, and contact information.

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.

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

TAXII
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](#)

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