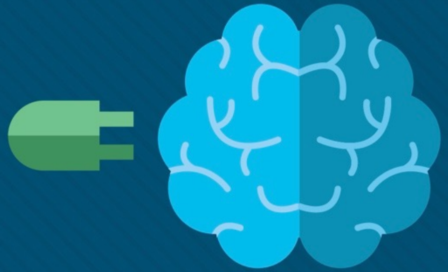


Chapter 8: Protecting the Network

Information Security

Dr. Ayman Aljarbouh

8.2 Access Control

Module Objectives

Module Title: Access Control

Module Objective: Explain access control as a method of protecting a network.

Topic Title	Topic Objective
Access Control Concepts	Explain how access control protocols network data.
AAA Usage and Operation	Explain how AAA is used to control network access.

Communications Security: CIA

Information security deals with protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

CIA Triad

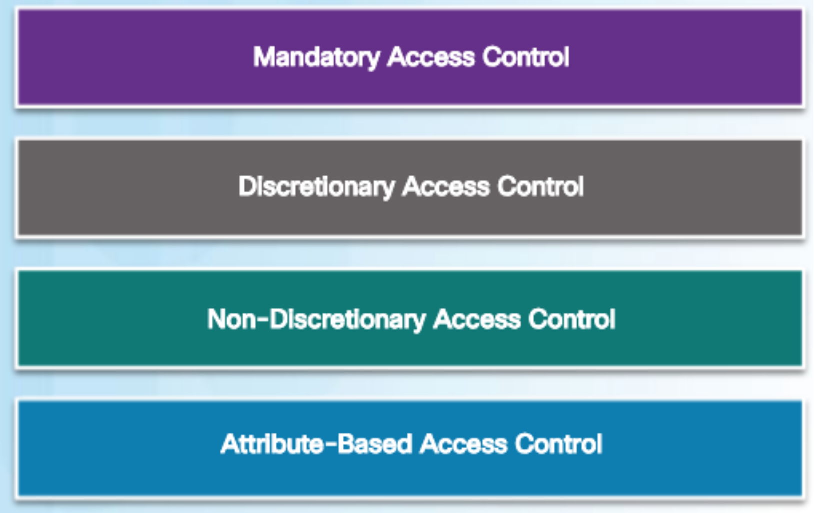
The CIA triad consists of three components of information security:

- **Confidentiality -** Only authorized individuals, entities, or processes can access sensitive information.
- **Integrity -** This refers to the protection of data from unauthorized alteration.
- **Availability -** Authorized users must have uninterrupted access to the network resources and data that they require.

Confidentiality
Integrity
Availability

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.


Mandatory Access Control

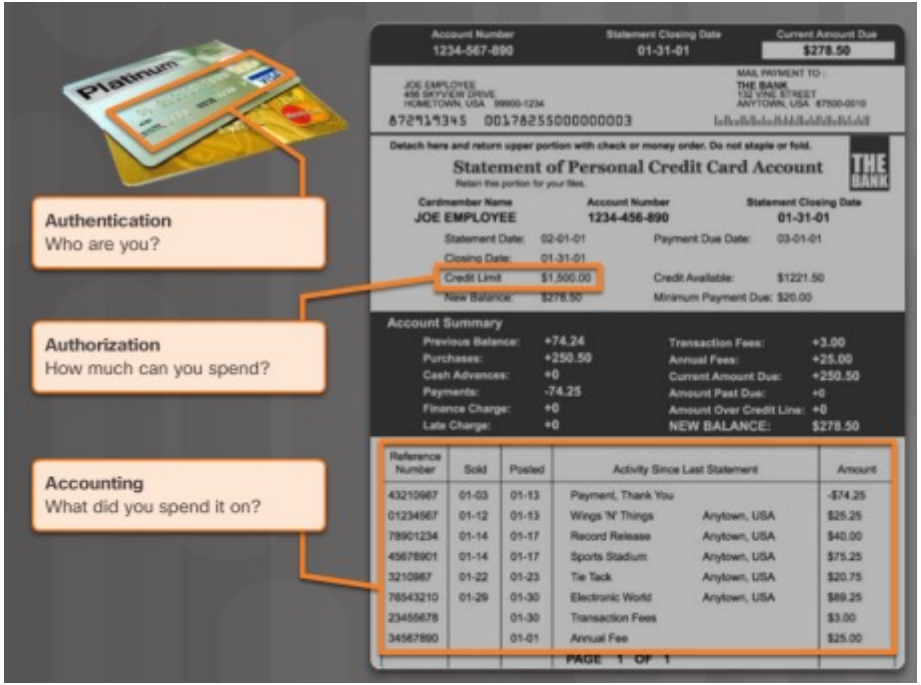
Discretionary Access Control

Non-Discretionary Access Control

Attribute-Based Access Control

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	Statement Closing Date	Current Amount Due
1234-567-890	01-31-01	$278.50

JOE EMPLOYEE
456 SKYVIEW DRIVE
HOMETOWN, USA 99900-1234

MAIL PAYMENT TO :
THE BANK
132 VINE STREET
ANYTOWN, USA 87500-0010

872919345 0017825500000003

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

Statement of Personal Credit Card Account

Retain this portion for your files.

THE BANK

Cardmember Name	Account Number	Statement Closing Date
JOE EMPLOYEE	1234-456-890	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:	$1221.50
New Balance:	$278.50	Minimum Payment Due:	$20.00

Account Summary

Previous Balance:	+74.24	Transaction Fees:	+3.00
Purchases:	+250.50	Annual Fees:	+25.00
Cash Advances:	+0	Current Amount Due:	+250.50
Payments:	-74.25	Amount Past Due:	+0
Finance Charge:	+0	Amount Over Credit Line:	+0
Late Charge:	+0	NEW BALANCE:	$278.50

Reference Number	Sold	Posted	Activity Since Last Statement		Amount
43210987	01-03	01-13	Payment, Thank You		-$74.25
01234567	01-12	01-13	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 Tack	Anytown, USA	$20.75
76543210	01-29	01-30	Electronic World	Anytown, USA	$89.25
23456678		01-30	Transaction Fees		$3.00
34567890		01-01	Annual Fee		$25.00

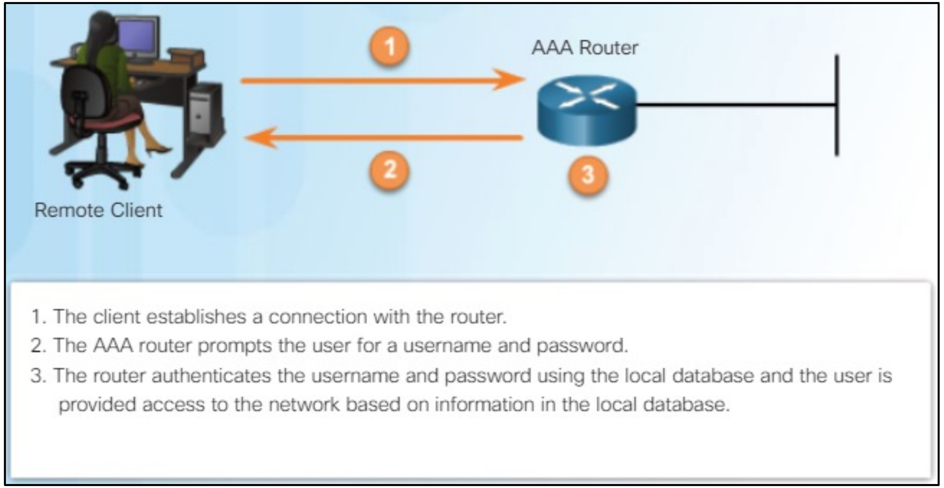
PAGE 1 OF 1

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.

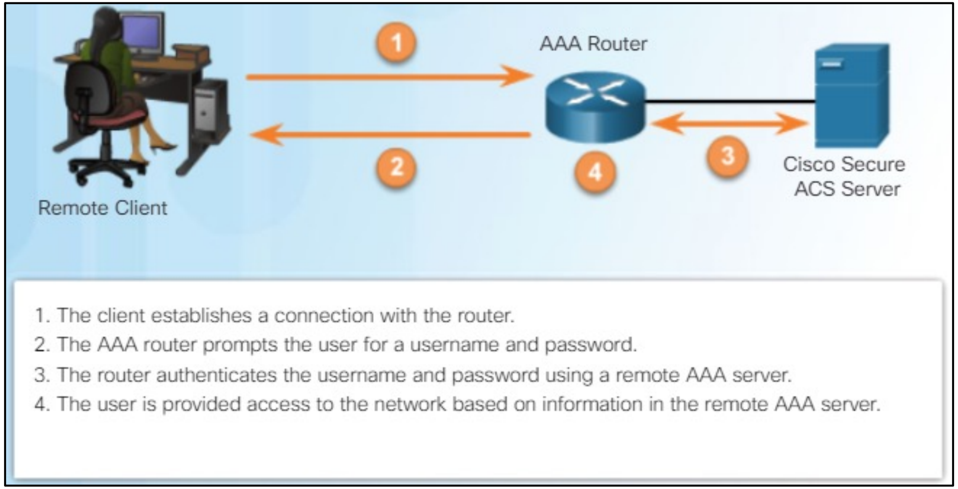
AAA Authentication (Cont.)

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.

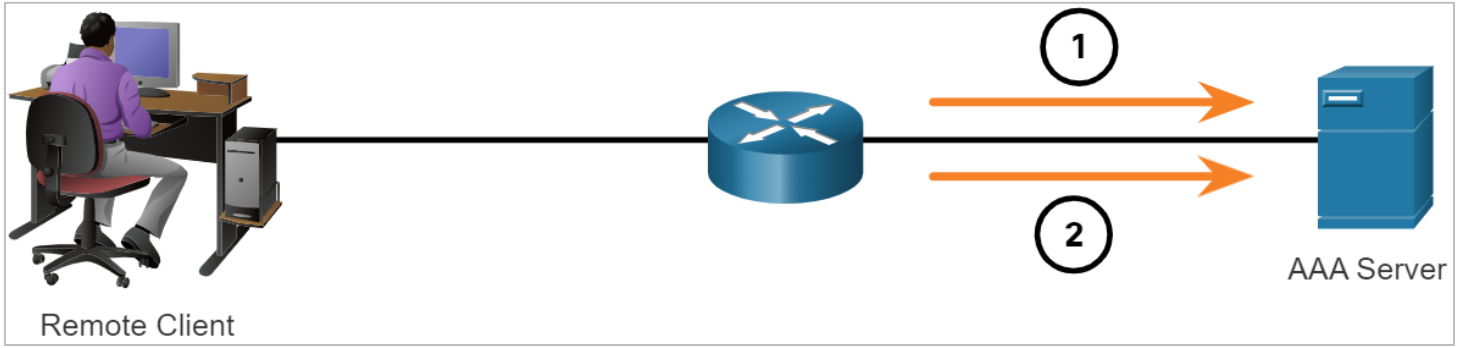
Server-Based AAA Authentication



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. The AAA servers keep a detailed log of exactly what the authenticated user does on the device.
- This includes all EXEC and configuration commands issued by the user.
- When a user has been authenticated, the AAA accounting process generates a start message to begin the accounting process.
- When the user finishes, a stop message is recorded and the accounting process ends.



AAA Usage and Operation

AAA Accounting Logs (Contd.)

The following table describes the types of accounting information that can be collected:

Types of Accounting Information	Description
Network Accounting	It captures information for all Point-to-Point Protocol (PPP) sessions, including packet and byte counts.
Connection Accounting	It captures information about all outbound connections that are made from the AAA client, such as by SSH.
EXEC Accounting	It captures information about user EXEC terminal sessions on the network access server, including username, date, start and stop times, and the access server IP address.
System Accounting	It captures information about all system-level events.
Command Accounting	It captures information about the EXEC shell commands for a specified privilege level ,as well as the date and time each command was executed, and the user who executed it.
Resource Accounting	It captures 'start' and 'stop' record support for connections that have passed user authentication.

8.3 Threat Intelligence

Module Objectives

Module Title: Threat Intelligence

Module Objective: Use various intelligence sources to locate current security threats.

Topic Title	Topic Objective
Information Sources	Describe information sources used to communicate emerging network security threats.
Threat Intelligence Services	Describe various threat intelligence services.

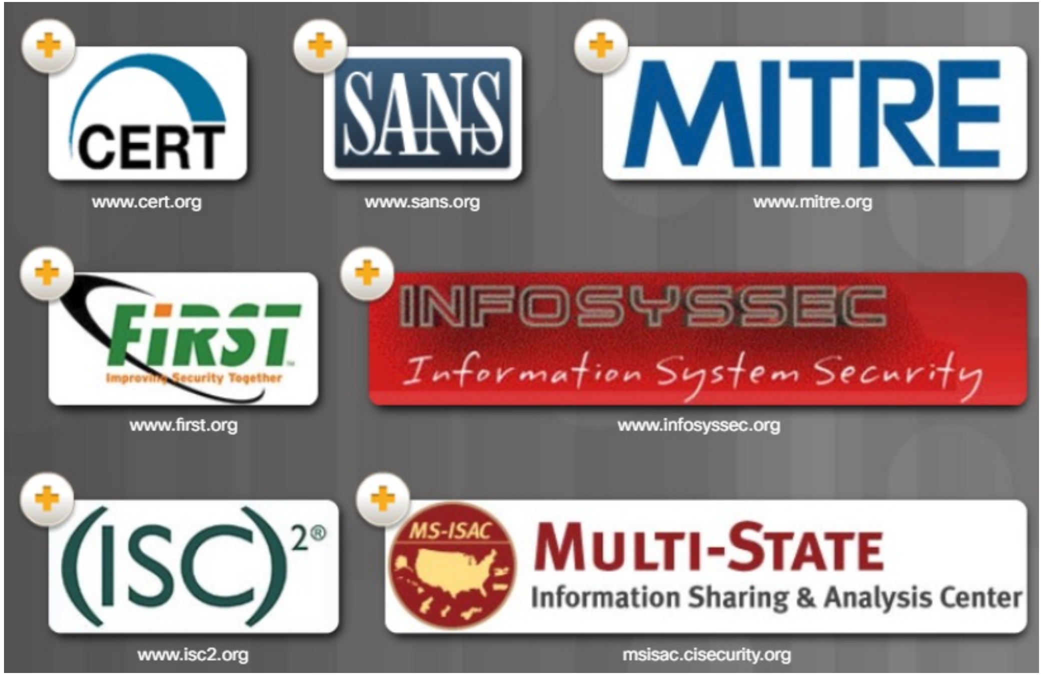
Network Intelligence Communities

- To effectively protect a network, the security professionals must stay informed about the threats and vulnerabilities.
- There are many security organizations which provide network intelligence, resources, workshops, and conferences to help security professionals.
- To remain effective, a network security professional must:
  - **Keep abreast of the latest threats** – Includes subscribing to real-time feeds regarding threats, routinely perusing security-related websites, following security blogs and podcasts, and more.
  - **Continue to upgrade skills** – Includes attending security-related training, workshops, and conferences.
- **Note**: Network security has a very steep learning curve and requires a commitment to continuous professional development.

Information Sources

Network Intelligence Communities

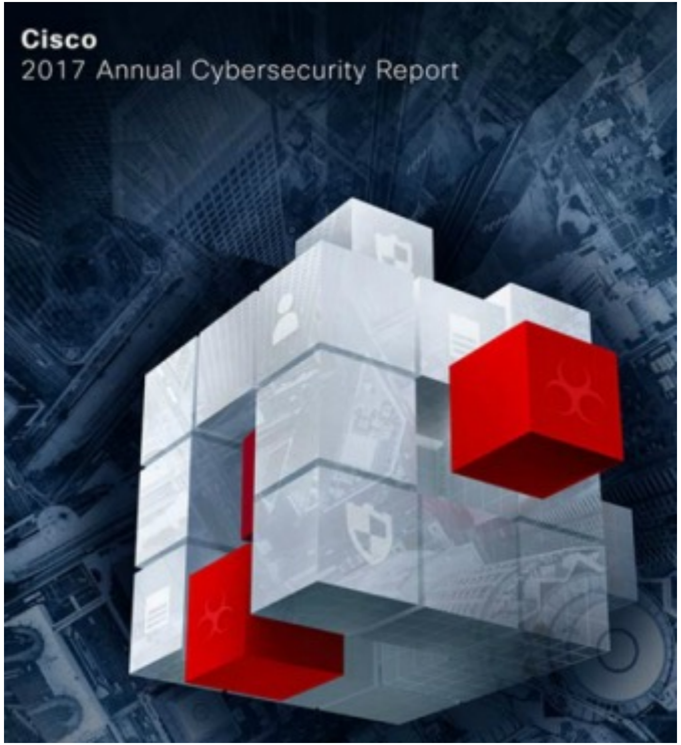
- Threat intelligence organizations such as CERT, SANS, and MITRE offer detailed threat information that is vital to cybersecurity practices.



Information Sources

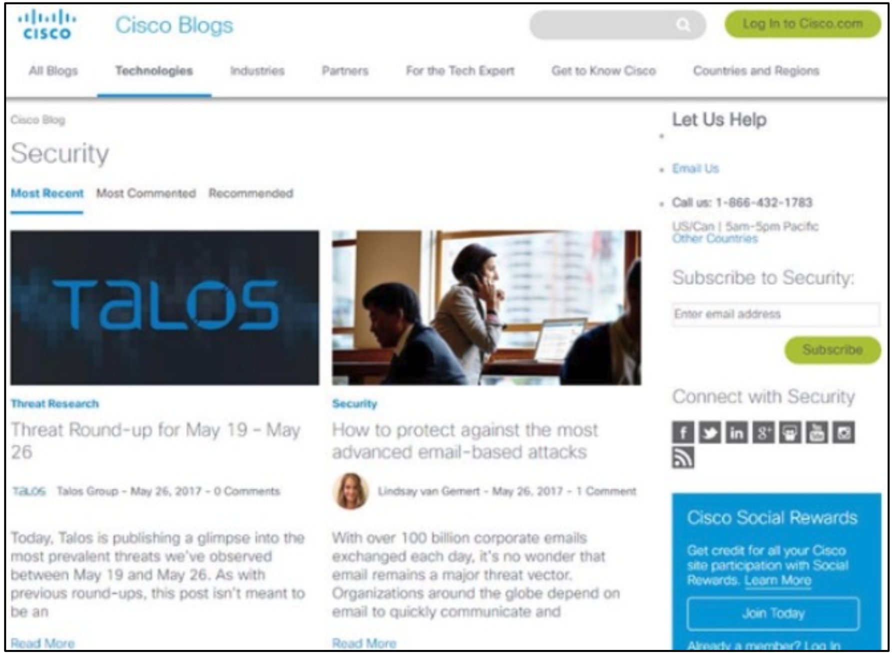
Cisco Cybersecurity Reports

- Resources to help security professionals stay abreast of the latest threats are the Cisco Annual Cybersecurity Report and the Mid-Year Cybersecurity Report.
- These reports provide an update on the state of security preparedness, expert analysis of top vulnerabilities, factors behind the explosion of attacks using adware, spam, and so on.
- Cybersecurity analysts should subscribe and read these reports to learn how threat actors are targeting their networks, and what action can be taken to mitigate these attacks.



Security Blogs and Podcasts

- Blogs and podcasts also provide advice, research, and recommended mitigation techniques.
- Cisco provides blogs on security-related topics from a number of industry experts and from the Cisco Talos Group.
- Cisco Talos offers a series of over 80 podcasts that can be played from the internet or downloaded to your device of choice.



Security

Let Us Help

- Email Us
- Call us: 1-866-432-1783

US/Can | 5am-5pm Pacific
Other Countries

Subscribe to Security:

Connect with Security

Threat Research

Threat Round-up for May 19 – May 26

Talos Group - May 26, 2017 - 0 Comments

Today, Talos is publishing a glimpse into the most prevalent threats we've observed between May 19 and May 26. As with previous round-ups, this post isn't meant to be an

Read More

Security

How to protect against the most advanced email-based attacks

Lindsay van Gemert - May 26, 2017 - 1 Comment

With over 100 billion corporate emails exchanged each day, it's no wonder that email remains a major threat vector. Organizations around the globe depend on email to quickly communicate and

Read More

Cisco Social Rewards

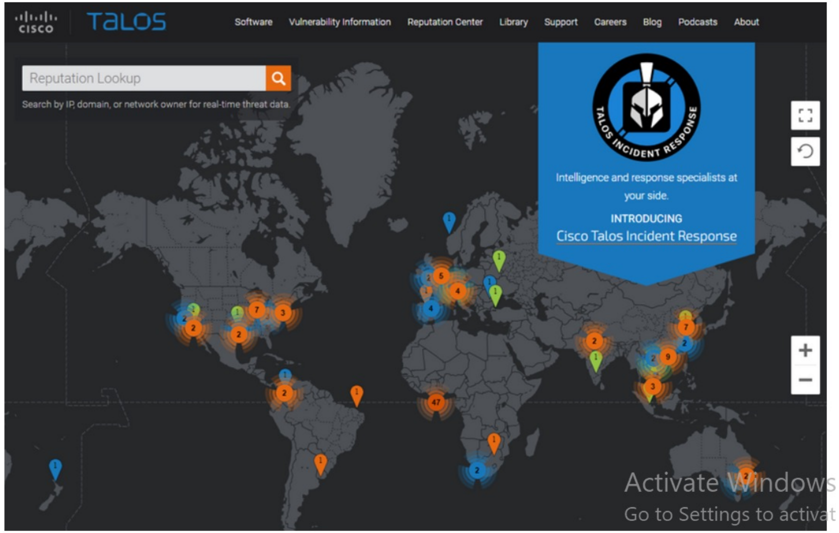
Get credit for all your Cisco site participation with Social Rewards. Learn More

Already a member? Log In

Threat Intelligence Services

Cisco Talos

- Talos is one of the largest commercial threat intelligence teams in the world, and is comprised of world-class researchers, analysts and engineers.
- The goal is to help protect enterprise users, data, and infrastructure from active adversaries.
- The team collects information about active, existing, and emerging threats, and then provides comprehensive protection against these attacks and malware to its subscribers.



Search by IP, domain, or network owner for real-time threat data.

Intelligence and response specialists at your side.

INTRODUCING

Cisco Talos Incident Response

- Cisco Security products can use Talos threat intelligence in real time to provide fast and effective security solutions.
- Cisco Talos also provides free software, services, resources, data and maintains the security incident detection rule sets for the Snort.org, ClamAV, and SpamCop network security tools.

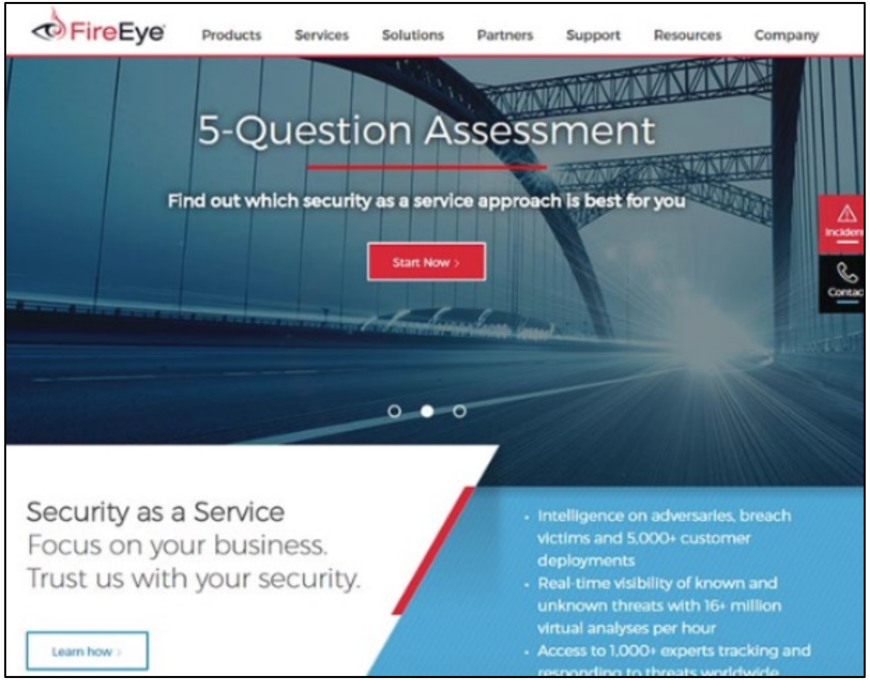
Threat Intelligence Services

FireEye

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

FireEye Security System:

- The FireEye Security System blocks attacks across web and email threat vectors, and latent malware that resides on file shares.
- It can block advanced malware that easily bypasses traditional signature-based defenses and compromises the majority of enterprise networks.
- It addresses all stages of an attack lifecycle with a signature-less engine utilizing stateful attack analysis to detect zero-day threats.



5-Question Assessment

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

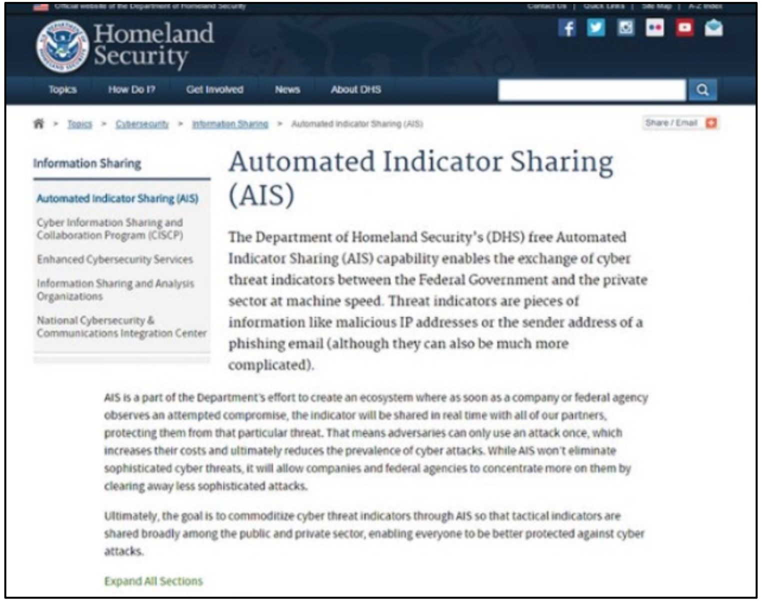
Security as a Service
Focus on your business.
Trust us with your security.

- 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

Threat Intelligence Services

Automated Indicator Sharing

- The Automated Indicator Sharing (AIS) is a free service offered by the U.S Department of Homeland Security(DHS).
- AIS enables the real-time exchange of cyber threat indicators between the U.S. Federal Government and the private sector.
- AIS creates an ecosystem when a threat is recognized. Later, it is immediately shared with the community to help them protect their networks from that particular threat.


Official website of the Department of Homeland Security
Contact Us | Quick Links | Site Map | A-Z Index
Homeland Security
Topics
How Do I?
Get Involved
News
About DHS
Topics > Cybersecurity > Information Sharing > Automated Indicator Sharing (AIS)
Share / Email
Information Sharing
Automated Indicator Sharing (AIS)
Cyber Information Sharing and Collaboration Program (CISCP)
Enhanced Cybersecurity Services
Information Sharing and Analysis Organizations
National Cybersecurity & Communications Integration Center

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.

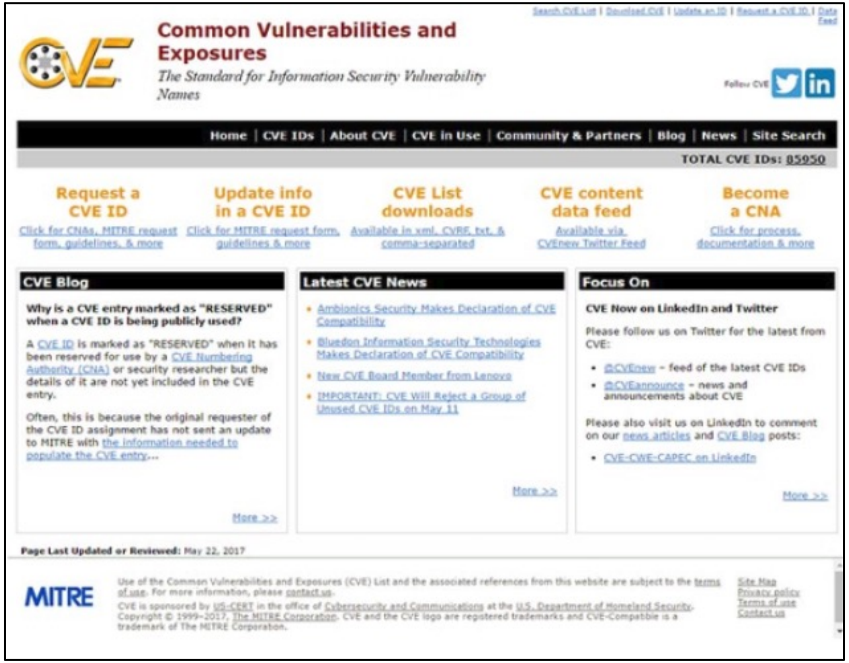
Ultimately, the goal is to commoditize cyber threat indicators through AIS so that tactical indicators are shared broadly among the public and private sector, enabling everyone to be better protected against cyber attacks.

Expand All Sections

Threat Intelligence Services

Common Vulnerabilities and Exposures (CVE) Database

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



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

Common Vulnerabilities and Exposures

The Standard for Information Security Vulnerability Names

Follow CVE

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

TOTAL CVE IDs: 85950

Request a CVE ID
Click for CNAs, MITRE request form, guidelines, & more

Update info in a CVE ID
Click for MITRE request form, guidelines & more

CVE List downloads
Available in xml, CVRF, txt, & comma-separated

CVE content data feed
Available via CVEnew 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
- Bluedon 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:

- @CVEnew – 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.

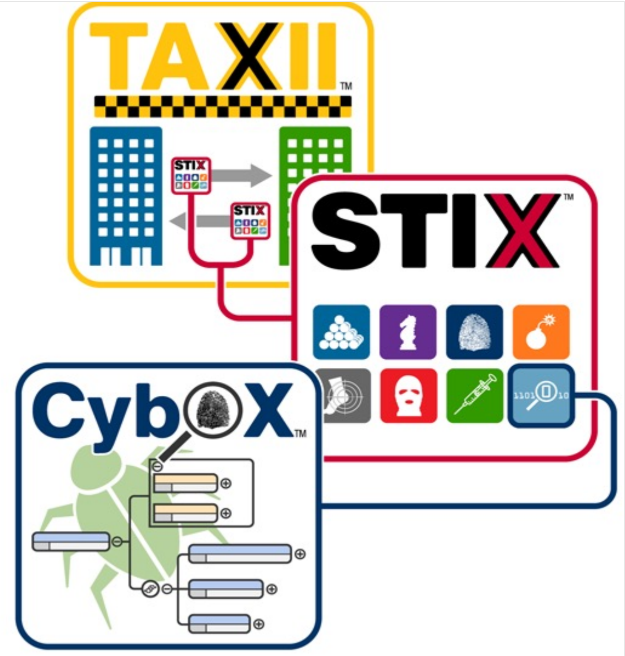
CVE is sponsored by US-CERT in the office of Cybersecurity and Communications at the U.S. Department of Homeland Security. Copyright © 1999–2017, The MITRE Corporation. CVE and the CVE logo are registered trademarks and CVE-Compatible is a trademark of The MITRE Corporation.

Site Map
Privacy policy
Terms of use
Contact us

Threat Intelligence Communication Standards

Three common threat intelligence sharing standards include the following:

- **Structured Threat Information Expression (STIX)** - This is a set of specifications for exchanging cyber threat information between organizations.
- **Trusted Automated Exchange of Indicator Information (TAXII)** – This is the specification for an application layer protocol that allows the communication of CTI over HTTPS. TAXII is designed to support STIX.
- **CybOX** - This is a set of standardized schema for specifying, capturing, characterizing, and communicating events and properties of network operations that supports many cybersecurity functions.



Protecting the Network

New Terms and Commands

- Discretionary access control (DAC)
- Mandatory access control (MAC)
- Attribute-based access control (ABAC)
- Role-based access control (RBAC)
- Availability
- Confidentiality
- Network Accounting
- Connection Accounting
- System Accounting
- EXEC Accounting
- Command Accounting
- Resource Accounting
- Authentication, Authorization, and Accounting (AAA)
- SysAdmin, Audit, Network, Security (SANS)
- Mitre
- Forum of Incident Response and Security Teams (FIRST)
- International Information Systems Security Certification Consortium (ISC)^2
- Cisco Talos
- FireEye
- Automated Indicator Sharing (AIS)
- Common Vulnerabilities and Exposures (CVE)
- Structured Threat Information Expression (STIX)
- Trusted Automated Exchange of Indicator Information (TAXII)
- CybOX

Lab 31 - The Cybersecurity Cube Scatter Quizlet

In this lab, you will identify the three dimensions of the Cybersecurity Cube and the elements of each dimension.