

Information Security Operations Center (Info SOC)

Lecture 6

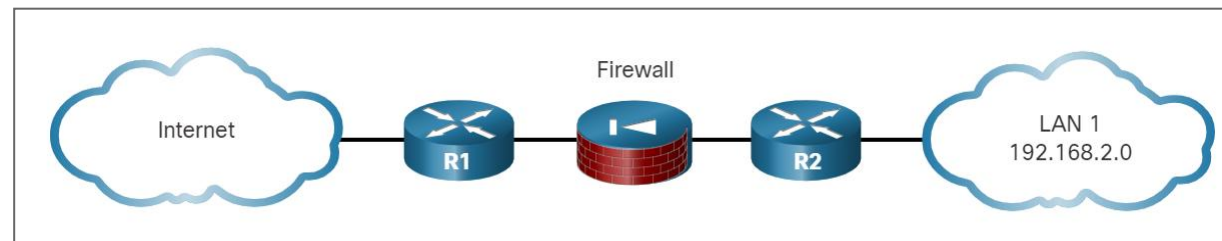
*Preventing malicious access to
computer networks, hosts, and data*

Contents

Topic Title	Topic Objective
Defense-in-Depth	Explain how the defense-in-depth strategy is used to protect networks.
Security Policies, Regulations, and Standards	Explain security policies, regulations, and standards.
Access Control Concepts	Explain how access control protocols network data.
AAA Usage and Operation	Explain how AAA is used to control network access.
Information Sources	Describe information sources used to communicate emerging network security threats.
Threat Intelligence Services	Describe various threat intelligence services.

Defense-in-Depth

- The figure displays a simple topology of a defense-in-depth approach:
 - Edge router** - The first line of defense is known as an edge router (R1 in the figure). The edge router has a set of rules specifying which traffic it allows or denies. It passes all connections that are intended for the internal LAN to the firewall.
 - Firewall** - A second line of defense is the firewall. The firewall is a checkpoint device that performs additional filtering and tracks the state of the connections. It denies the initiation of connections from the untrusted networks to the trusted network while enabling internal users to establish two-way connections to the untrusted networks.
 - Internal router** - Another line of defense is the internal router (R2 in the figure). It can apply final filtering rules on the traffic before it is forwarded to its destination.

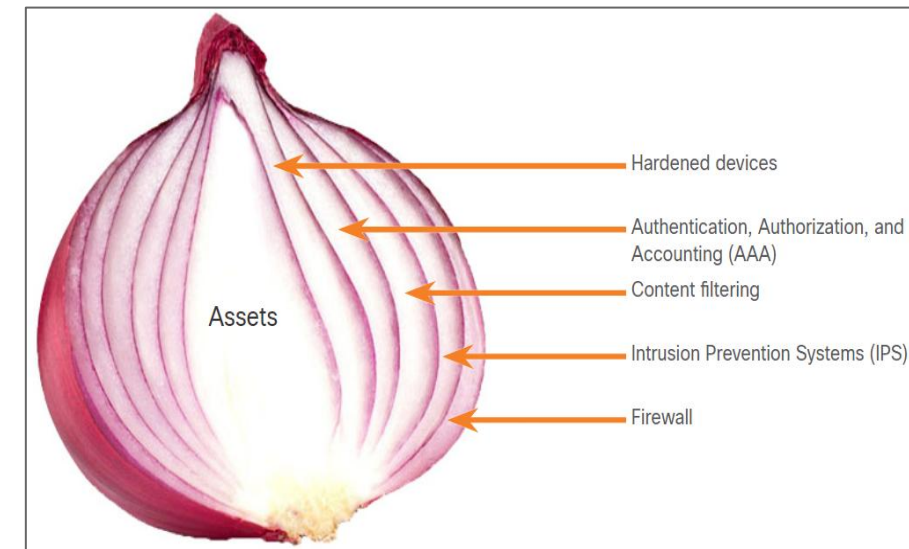


The Security Onion and The Security Artichoke

There are two common analogies that are used to describe a defense-in-depth approach.

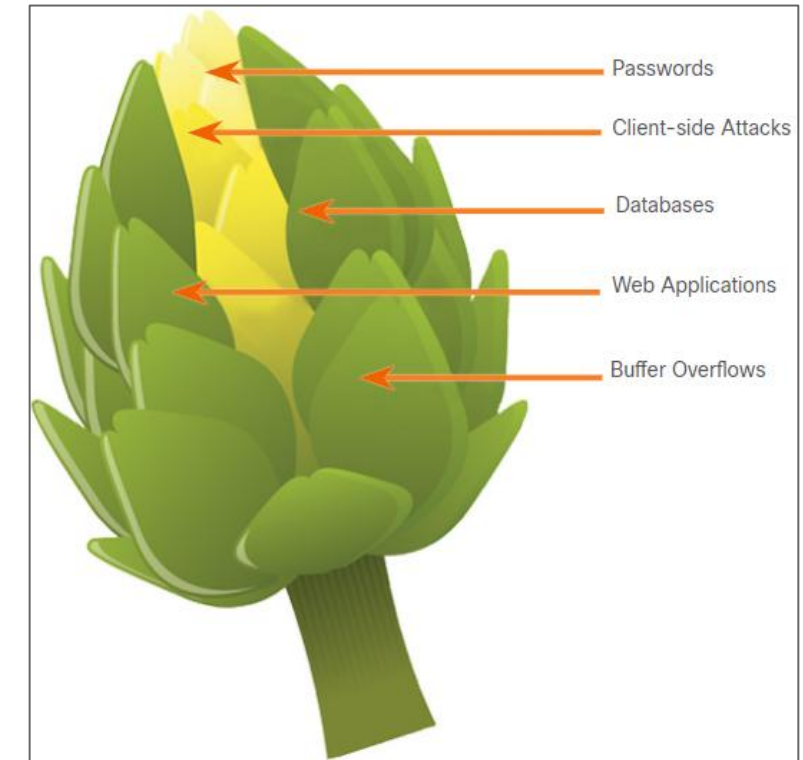
Security Onion

- A common analogy used to describe a defense-in-depth approach is called "the security onion."
- As illustrated in figure, a threat actor would have to peel away at a network's defenses layer by layer in a manner like peeling an onion.
- Only after penetrating each layer would the threat actor reach the target data or system.



The Security Onion and The Security Artichoke

- The evolution of borderless networks has changed the analogy to the "security artichoke", which benefits the threat actor.
- As illustrated in the figure, threat actors no longer must peel away each layer. They only need to remove certain "artichoke leaves."
- The bonus is that each "leaf" of the network may reveal sensitive data that is not well secured.
- In order to get at the heart of the artichoke, the hacker chips away at the security armor along the perimeter.
- While internet-facing systems are very well protected, persistent hackers do find a gap in that hard-core exterior through which they can enter.



Security Policies, Regulations, and Standards

Business Policies

- **Business policies** are the guidelines that are developed by an organization to govern its actions.
- **The policies** define standards of correct behavior for the business and its employees.
- **In networking**, policies define the activities that are allowed on the network.
- This sets a baseline of acceptable use. If behavior that violates business policy is detected on the network, it is possible that a security breach has occurred.

Security Policies, Regulations, and Standards

Business Policies

An organization may have several guiding policies, as listed in the table.

Policy	Description
Company policies	• It establishes the rules of conduct and the responsibilities of both employees and employers. • It protect the rights of workers as well as the business interests of employers. • Depending on the needs of the organization, various policies and procedures establish rules regarding employee conduct, attendance, dress code, privacy and other areas related to the terms and conditions of employment.
Employee policies	• These policies are created and maintained by human resources staff to identify employee salary, pay schedule, employee benefits, work schedule, vacations, and more. • They are often provided to new employees to review and sign.
Security policies	• These policies identify a set of security objectives for a company, define the rules of behavior for users and administrators, and specify system requirements. • These objectives, rules, and requirements collectively ensure the security of a network and the computer systems in an organization. • It is a constantly evolving document based on changes in the threat landscape, vulnerabilities, and business and employee requirements.

Security Policies, Regulations, and Standards

Security Policy

- **Security policies** are used to inform users, staff, and managers of an organization's requirements for protecting technology and information assets.
- A comprehensive security policy has several benefits, including the following:
 - 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 also specifies the mechanisms that are needed to meet security requirements and provides a baseline from which to acquire, configure, and audit computer systems and networks for compliance.

Security Policies, Regulations, and Standards

Security Policy

The following table lists the policies that may be included in a security policy:

Policy	Description
Identification and authentication policy	It specifies authorized persons that can have access to network resources and identity verification procedures.
Password policies	These ensure passwords meet minimum requirements and are changed regularly.
Acceptable use policy (AUP)	It identifies network applications and uses that are acceptable to the organization. It may also identify ramifications if this policy is violated.
Remote access policy	It identifies how remote users can access a network and what is accessible via remote connectivity.
Network maintenance policy	It specifies network device operating systems and end user application update procedures.
Incident handling procedures	These describe how security incidents are handled.

Zero Trust Security

- **Zero trust** is a comprehensive approach to securing all access across networks, applications, and environments.
- This approach helps secure access from users, end-user devices, APIs, IoT, microservices, containers, and more.
- The principle of a zero-trust approach is "never trust always verify".
- **A zero-trust security framework** helps to prevent unauthorized access, contain breaches, and reduce the risk of an attacker's lateral movement through a network.
- **In a Zero-trust approach**, any place at which an access control decision is required should be considered a perimeter.

Zero Trust Security

The **three pillars of zero trust** are **workforce, workloads, and workplace**.

- **Zero Trust for the Workforce** - This pillar consists of people who access work applications by using their personal or corporate-managed devices. It ensures only the right users and secure devices can access applications, regardless of location.
- **Zero Trust for Workloads** - This pillar is concerned with applications that are running in the cloud, in data centers, and other virtualized environments that interact with one another. It focuses on secure access when an API, a microservice, or a container is accessing a database within an application.
- **Zero Trust for the Workplace** - This pillar focuses on secure access for all devices, including on the internet of things (IoT), that connect to enterprise networks, such as user endpoints, physical and virtual servers, printers, cameras and more.

Access Control Models

- An organization must implement proper access controls to protect its network resources, information system resources, and information.
- A security analyst should understand the different basic access control models to have a better understanding of how attackers can break the access controls.
- The following table lists various types of access control models:

Access Control Models	Description
Discretionary access control (DAC)	• This is the least restrictive model and allows users to control access to their data as owners of that data. • It may use ACLs or other methods to specify which users or groups of users have access to the information.
Mandatory access control (MAC)	• This applies the strictest access control and is used in military or mission critical applications. • It assigns security level labels to information and enables users with access based on their security level clearance.

Access Control Models

Access Control Models	Description
Role-based access control (RBAC)	• Access decisions are based on an individual's roles and responsibilities within the organization. • Different roles are assigned security privileges, and individuals are assigned to the RBAC profile for the role. • Also known as a type of non-discretionary access control.
Attribute-based access control (ABAC)	It allows access based on attributes of the object to be accessed, the subject accessing the resource, and environmental factors regarding how the object is to be accessed.
Rule-based access control (RBAC)	• Network security staff specify sets of rules or conditions that are associated with access to data or systems. • These rules may specify permitted or denied IP addresses, or certain protocols and other conditions. • Also known as Rule Based RBAC.
Time-based access control (TAC)	It allows access to network resources based on time and day.

AAA Operation

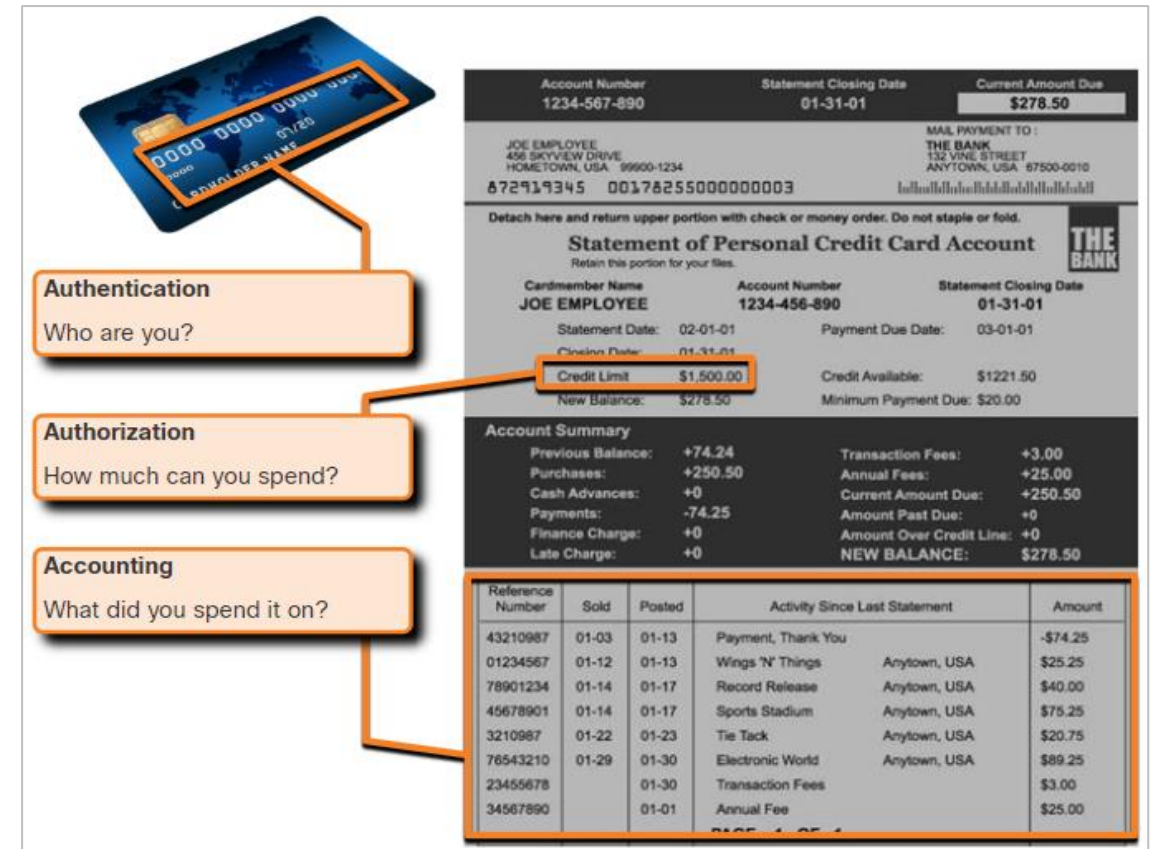
The following table lists the three independent security functions provided by the AAA architectural framework:

AAA Component	Description
Authentication	• Authentication can be established using username and password combinations, challenge and response questions, token cards, and other methods. • AAA authentication provides a centralized way to control access to the network.
Authorization	• After the user is authenticated, authorization services determine which resources the user can access and which operations the user is allowed to perform. • An example is "User can access host server XYZ using SSH only."
Accounting	• Accounting records what the user does, including what is accessed, the amount of time the resource is accessed, and any changes that were made. • Accounting keeps track of how network resources are used. • An example is "User accessed host server XYZ using SSH for 15 minutes."

Access Control Concepts

AAA Operation

This concept is like the use of a credit card, as indicated by the figure. The credit card identifies who can use it, how much that user can spend, and keeps account of what items the user spent money on.



AAA Authentication

- AAA Authentication can be used to authenticate users for administrative access, or it can be used to authenticate users for remote network access.
- Cisco provides two common methods for implementing AAA Services:

Local AAA Authentication

- This method is known as self-contained authentication because it authenticates users against locally stored usernames and passwords.
- Local AAA is ideal for small networks.

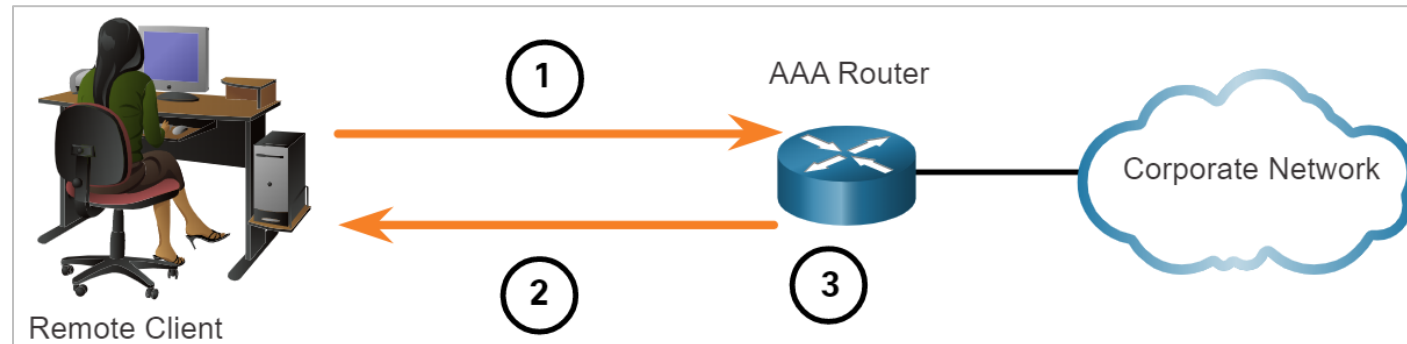
Server-based AAA Authentication

- This method authenticates against a central AAA server that contains the usernames and passwords for all users.
- This is ideal for medium-to-large networks.

AAA Authentication

Local AAA Authentication

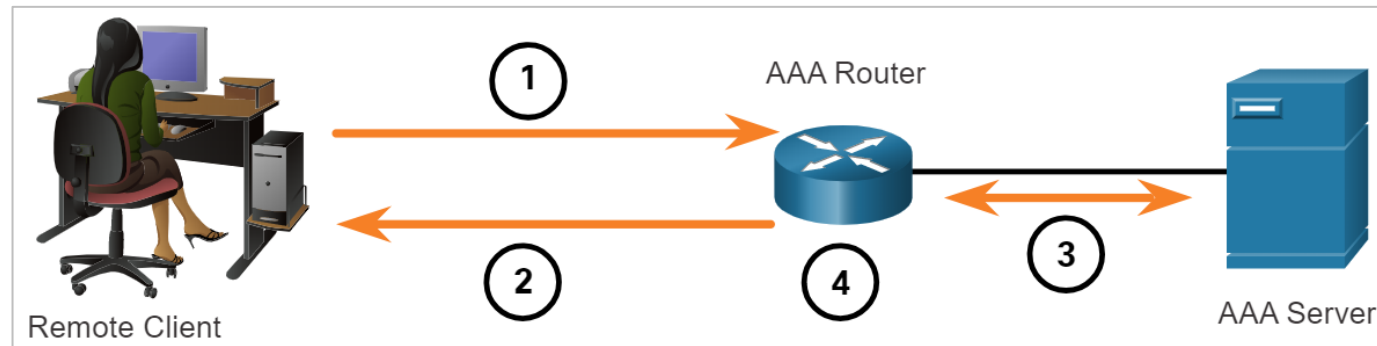
- The client establishes a connection with the router.
- The AAA router prompts the user for a username and password.
- The router authenticated the username and password using the local database and the user is provided access to the network based on information in the local database.



AAA Authentication

Server-based AAA Authentication

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



AAA Authentication

Centralized AAA

- Centralized AAA is more scalable and manageable than local AAA authentication, and therefore, it is the preferred AAA implementation.
- A centralized AAA system may independently maintain databases for authentication, authorization, and accounting.
- It can leverage Active Directory or Lightweight Directory Access Protocol (LDAP) for user authentication and group membership, while maintaining its own authorization and accounting databases.
- Devices communicate with the centralized AAA server using either the Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access Control System (TACACS+) protocols.

AAA Authentication

The following table lists the differences between the two protocols:

Functions	TACACS+	RADIUS
Functionality	It separates authentication, authorization, and accounting functions according to the AAA architecture. This allows modularity of the security server implementation.	It combines authentication and authorization but separates accounting, which allows less flexibility in implementation than TACACS+.
Standard	Mostly Cisco supported	Open/RFC standard
Transport	TCP port 49	UDP ports 1812 and 1813, or 1645 and 1646
Protocol CHAP	Bidirectional challenge and response as used in Challenge Handshake Authentication Protocol (CHAP)	Unidirectional challenge and response from the RADIUS security server to the RADIUS client

AAA Authentication

Functions	TACACS+	RADIUS
Confidentiality	Encrypts the entire body of the packet but leaves a standard TACACS+ header.	Encrypts only the password in the access-request packet from the client to the server. The remainder of the packet is unencrypted, leaving the username, authorized services, and accounting unprotected.
Customization	Provides authorization of router commands on a per-user or per-group basis.	Has no option to authorize router commands on a per-user or per-group basis.
Accounting	Limited	Extensive

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.

Network Intelligence Communities

The table lists the important network security organization.

Organization	Description
SysAdmin, Audit, Network, Security (SANS)	SANS Institute resources are largely free upon request and include: • The Internet Storm Center - the popular internet early warning system • NewsBites - The weekly digest of news articles about computer security. • @RISK - The weekly digest of newly discovered attack vectors, vulnerabilities with active exploits, and explanations of how recent attacks worked. • Flash security alerts • Reading Room - More than 1,200 award-winning, original research papers. • SANS also develops security courses.
MITRE (Massachusetts Institute of Technology Research and Engineering)	The Mitre Corporation maintains a list of Common Vulnerabilities and Exposures (CVE) used by prominent security organizations.

Information Security Operations Center

Network Intelligence Communities

Organization	Description
Forum of Incident Response and Security Teams (FIRST)	It is a security organization that brings together a variety of computer security incident response teams from government, commercial, and educational organizations to foster cooperation and coordination in information sharing, incident prevention and rapid reaction.
SecurityNewsWire	A security news portal that aggregates the latest breaking news pertaining to alerts, exploits, and vulnerabilities.
International Information Systems Security Certification Consortium (ISC) ²	Provides vendor neutral education products and career services to more than 75,000+ industry professionals in more than 135 countries.
Center for Internet Security (CIS)	It is a focal point for cyber threat prevention, protection, response, and recovery for state, local, tribal, and territorial (SLTT) governments through the Multi-State Information Sharing and Analysis Center (MS-ISAC). The MS-ISAC offers 24x7 cyber threat warnings and advisories, vulnerability identification, and mitigation and incident response.

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.



FireEye

- **FireEye** is another security company that offers services to help enterprises secure their networks.
- It uses a three-pronged approach combining security intelligence, security expertise, and technology.
- It offers **SIEM and SOAR** with the **Helix Security Platform**, which uses behavioral analysis and advanced threat detection and is supported by the FireEye Mandiant worldwide threat intelligence network.

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 threat.

The Malware Information Sharing Platform (MISP)

- The Malware Information Sharing Platform (MISP) is an open-source platform for sharing Indicators of Compromise (IOCs) for newly discovered threats.
- MISP is supported by the European Union and is used by over 6,000 organizations globally.
- MISP enables automated sharing of IOCs between people and machines by using STIX and other export formats.

Threat Intelligence Communication Standards

Three common threat intelligence sharing standards include the following:

- These standards enable the exchange of **cyber threat intelligence** (CTI) in an automated, consistent, and machine-readable format.
- **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.



Thanks