



UNIVERSITY OF ŽILINA
Faculty of Management Science
and Informatics

Prednáška 6

Network monitoring and vulnerabilities



Riešenie bezpečnostných incidentov
(CyberOps Associate v1.02)

Mgr. Jana Uramová, PhD.
Katedra informačných sietí
Fakulta riadenia a informatiky, ŽU

Ktorý výsledok pokrýva táto prednáška

Výsledky vzdelávania

Študent po absolvovaní predmetu získa vedomosti a zručnosti potrebné na úspešné zvládnutie úloh, povinností a zodpovedností bezpečnostného analytika v operačnom centre bezpečnosti.

Študent po absolvovaní predmetu bude vedieť:

- Vysvetliť rolu analytika v rámci kybernetickej bezpečnosti
- Vysvetliť prostriedky operačného systému Windows a Linux a charakteristiky pre podporu analýzy v rámci kybernetickej bezpečnosti
- Analyzovať operácie v rámci sieťových protokolov a služieb
- Vysvetliť operácie sieťovej infraštruktúry
- Klasifikovať rôzne typy sieťových útokov
- Použiť sieťové monitorovacie nástroje na identifikáciu útokov proti sieťovým protokolom a službám
- Použiť rôzne metódy na prevenciu škodlivého prístupu do počítačových sietí, k používateľom a k dátam
- Vysvetliť vplyvy kryptografie v rámci monitorovania bezpečnostných sietí
- Vysvetliť, ako skúmať zraniteľnosti a útoky koncových zariadení
- Identifikovať hlásenia v rámci sieťovej bezpečnosti
- Analyzovať sieťovú prevádzku na overenie potencionálneho zneužitia siete
- Aplikovať reakčné modely na incident, a získať prostriedky na manažovanie sieťových bezpečnostných incidentov
- Prerekvizity:
 - Princípy IKS, Počítačové siete 1, Úvod do OS

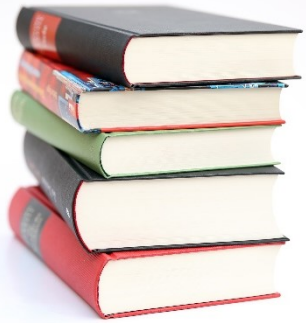


Preliminary version of topics for lectures

Planning

Week	CyberOps Modules in lectures	Exam from:
1	Chapter 1 The Danger Chapter 2 Fighters in the War Against Cybercrime Chapter 3: The Windows Operating System	none
2	Chapter 4: Linux Overview Chapter 5 Network Protocols Chapter 6 Ethernet and Internet Protocol (IP) Chapter 7 Connectivity Verification Chapter 8 Address Resolution Protocol Chapter 10 Network Services Chapter 11 Network Communication Devices	1-2
3	Chapter 9 The Transport Layer (+nmap) Chapter 12 Network Security Infrastructure	3-4
4	Chapter 13 Attackers and Their Tools Chapter 14 Common Threats and Attacks	5-10

Week	CyberOps Modules in Lectures	Exam from:
5	Chapter 15 Network Monitoring and Tools (<i>SIEM, SOAR</i>) Chapter 16 Attacking the Foundation (<i>L2, L3 protocols vulnerabilities and attacks</i>) Chapter 17 Attacking What We Do (<i>L7 vulnerabilities and attacks</i>)	11-12
6	Chapter 18 Understanding Defense (<i>security management</i>) Chapter 19 Access Control (<i>AAA</i>) Chapter 20 Threat Intelligence (<i>commercials, CVE database</i>)	13-17
7	Chapter 21 Cryptography Chapter 22 Endpoint Protection	18-20
8	Chapter 23 Endpoint Vulnerability Assessment Chapter 24 Technologies and Protocols	none
9	Chapter 25 Network Security Data Chapter 26 Evaluating Alerts (in Security Onion)	21-23
10	Chapter 27 Working with Network Security Data (Security Onion and ELK)	24-25
11	Chapter 28 Digital Forensics and Incident Analysis and Response	none
12	Expert talk (invited lecture)	26-28



Obsah dnešnej prednášky

Čo prejdeme spolu na prednáške:

- **Chapter 18 Understanding Defense**
(security management)
- **Chapter 19 Access Control (AAA)**
- **Chapter 20 Threat Intelligence**
(commercials, CVE database)



Module 18: Understanding Defense

Module Objective: Explain approaches to network security defense

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.

18.1 Defense-in-Depth

Assets, Vulnerabilities, Threats

- Cybersecurity analysts must prepare for any type of attack. It is their job to secure the assets of the organization's network.
- To do this, cybersecurity analysts must first identify:
 - **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 actor.
 - **Threats** - Any potential danger to an asset.



Understanding Defense

Identify Assets



- The collection of all the **devices** and **information** owned or managed by the organization are the assets.
- These assets must be **inventoried** and **assessed** for the level of protection needed to thwart (*prekazit'*) potential attacks.
- Asset management consists of inventorying all assets, and then developing and implementing **policies** and **procedures** to protect them.
- This task can be daunting (*skl'učujúca*) considering many organizations must protect internal users and resources, mobile workers, and cloud-based and virtual services.
- Further, organizations need to identify **where** critical information assets are stored, and **how access** is gained to that information.
- Information assets **vary**, as do the threats against them. Each of these assets can attract **different threat actors** who have **different skill levels and motivations**.

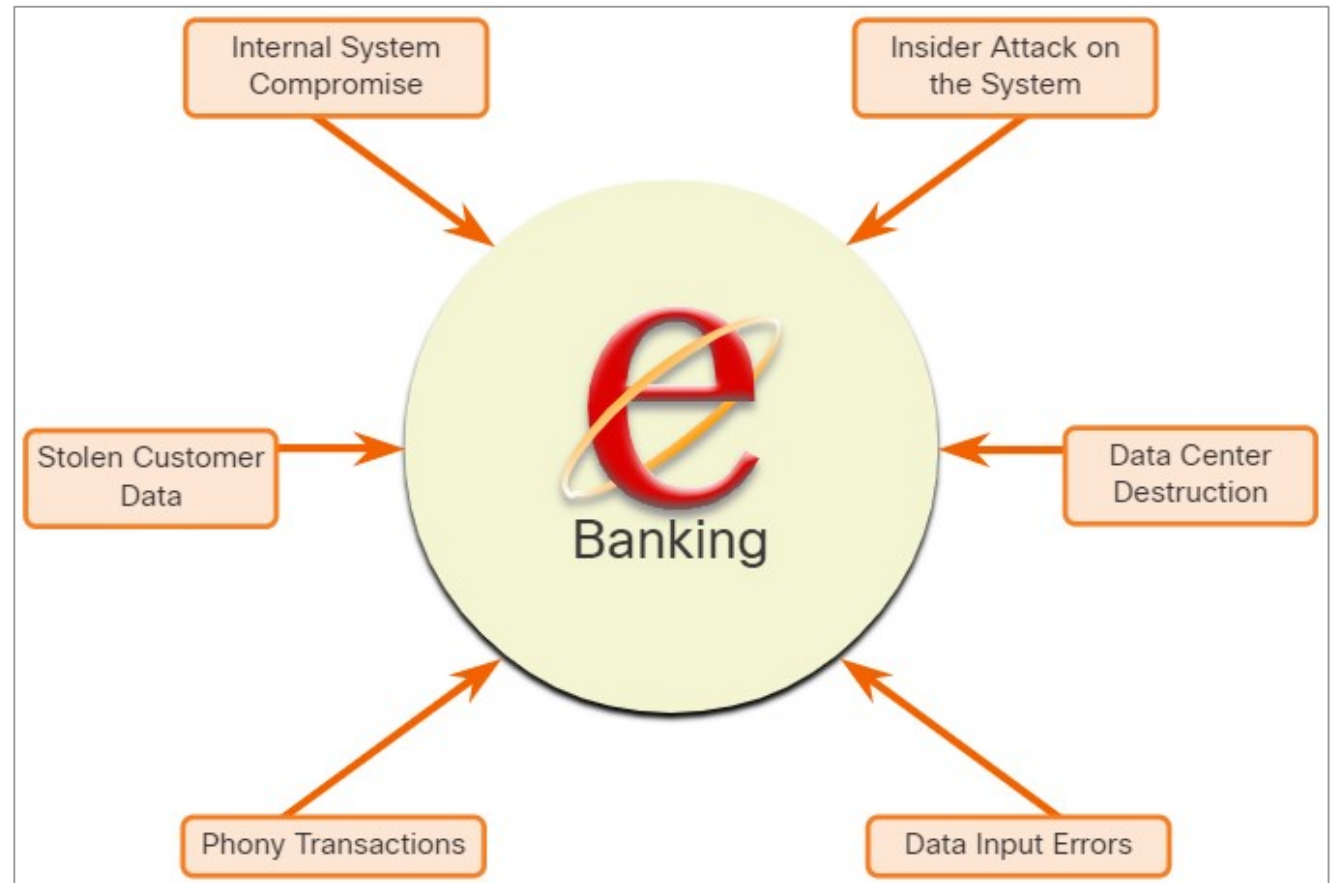
Identify Vulnerabilities

- Threat identification provides an organization with a **list of likely threats** for a particular environment.
- When identifying threats, it is important to ask several questions:
 - **What** are the **possible** vulnerabilities of a system?
 - **Who** may want to **exploit** those vulnerabilities to access specific information assets?
 - What are the **consequences** if system vulnerabilities are exploited and assets are lost?

Identify Vulnerabilities (Contd.)

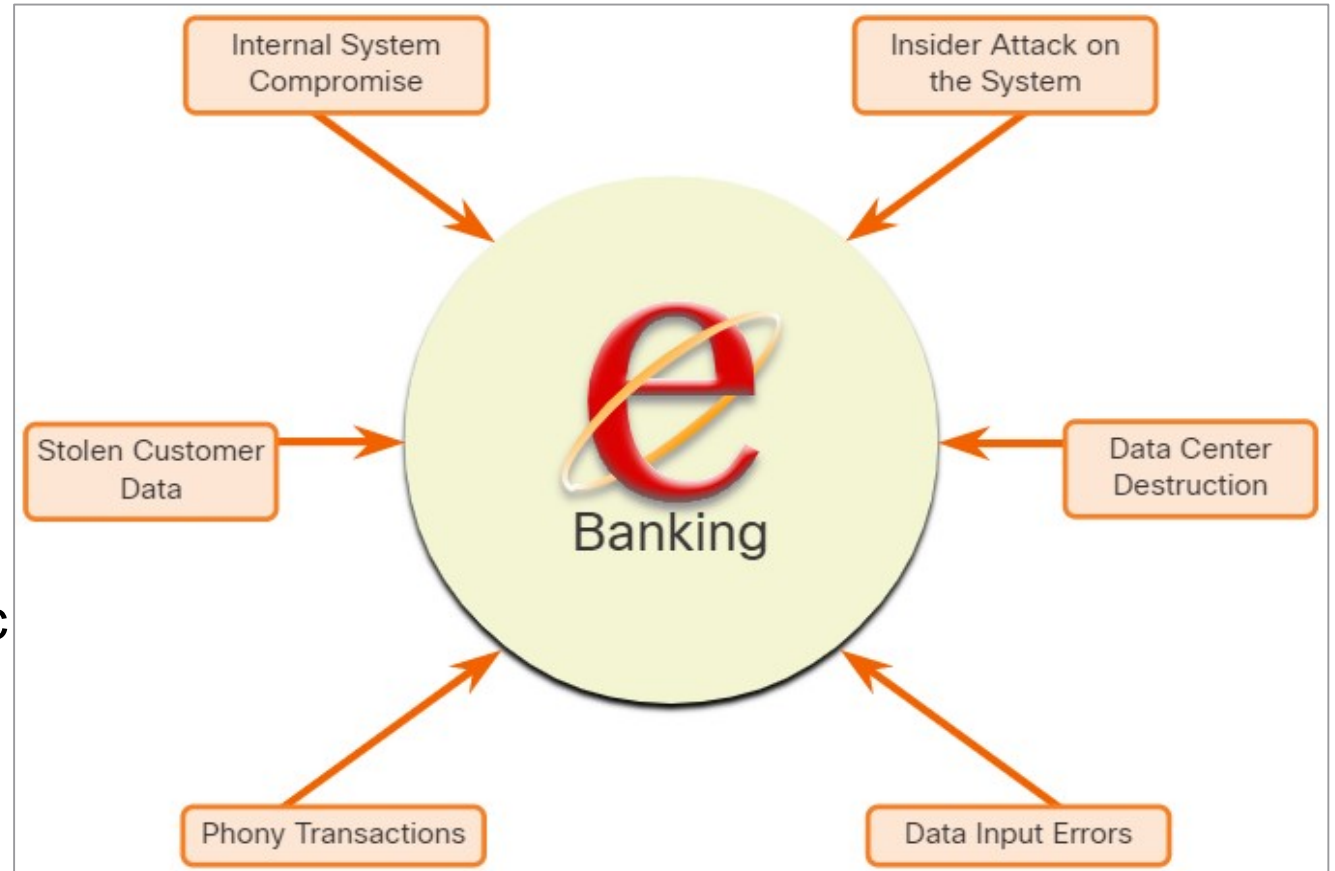
The threat identification for an e-banking system would include:

- **Internal system compromise** - The attacker uses the exposed e-banking servers to break into an internal bank system.
- **Stolen customer data** - An attacker steals the personal and financial data of bank customers from the customer database.
- **Phony (*falošná*) transactions from an external server** - An attacker alters the code of the e-banking application and makes transactions by impersonating a legitimate user.



Identify Vulnerabilities (Contd.)

- **Phony transactions using a stolen customer PIN or smart card** - An attacker steals the identity of a customer and completes malicious transactions from the compromised account.
- **Data input errors** (*chyby zadávania údajov*) - A user inputs incorrect data or makes incorrect transaction requests.
- **Data center destruction** - A cataclysmic event severely damages or destroys the data center.

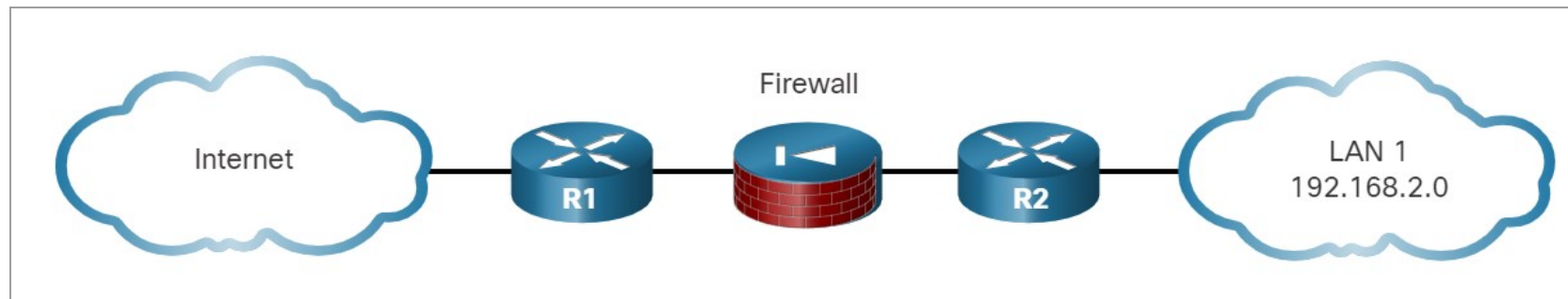


- Identifying vulnerabilities on a network requires an understanding of the important applications used as well as the different vulnerabilities of that application and hardware. This requires a significant amount of research on the part of the network administrator.

Understanding Defense

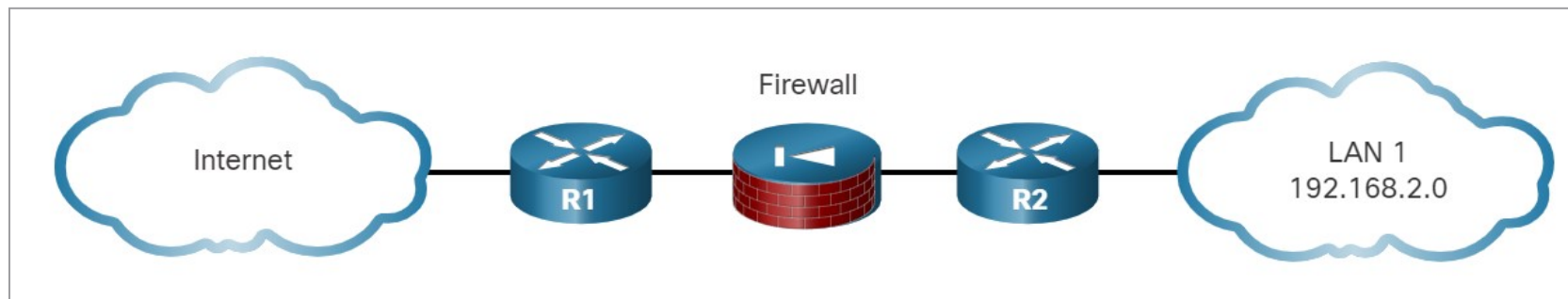
Identify Threats

- Organizations must use a defense-in-depth approach (hĺbkový prístup obrany) to identify threats and secure vulnerable assets.
- This approach uses multiple layers of security at the network edge, within the network, and on network endpoints.
- In this approach, a router first screens the traffic before forwarding it to a dedicated firewall appliance, for example, the Cisco ASA.
- Routers and firewalls are not the only devices that are used in a defense-in-depth approach.
- Other security devices include Intrusion Prevention Systems (IPS), advanced malware protection (AMP), web and email content security systems, identity services, network access controls and more.
- In the layered defense-in-depth security approach, the different layers work together to create a security architecture in which the failure of one safeguard does not affect the effectiveness of the other safeguards.

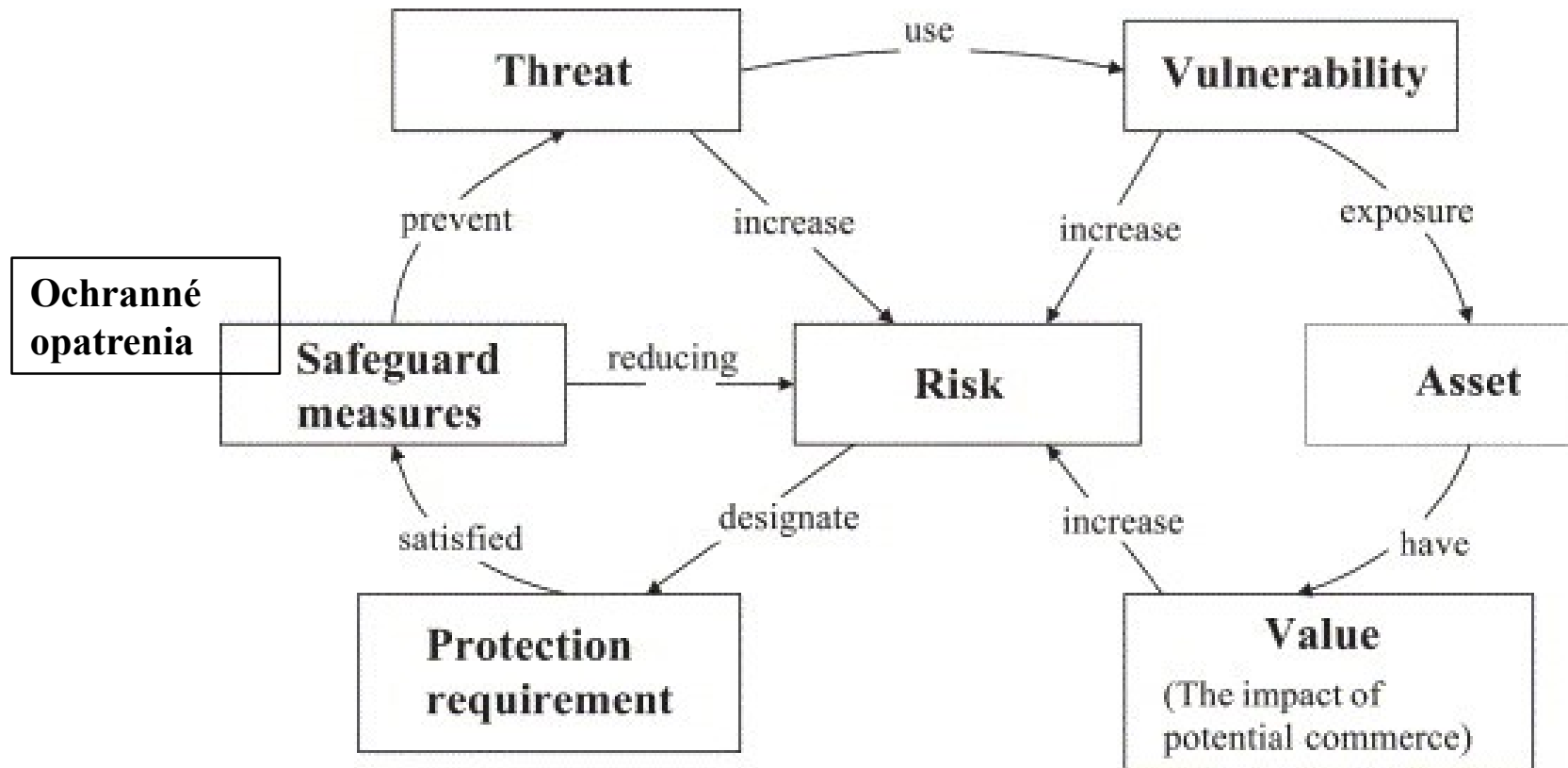


Identify Threats (Contd.)

- 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.



Information security management system evaluation

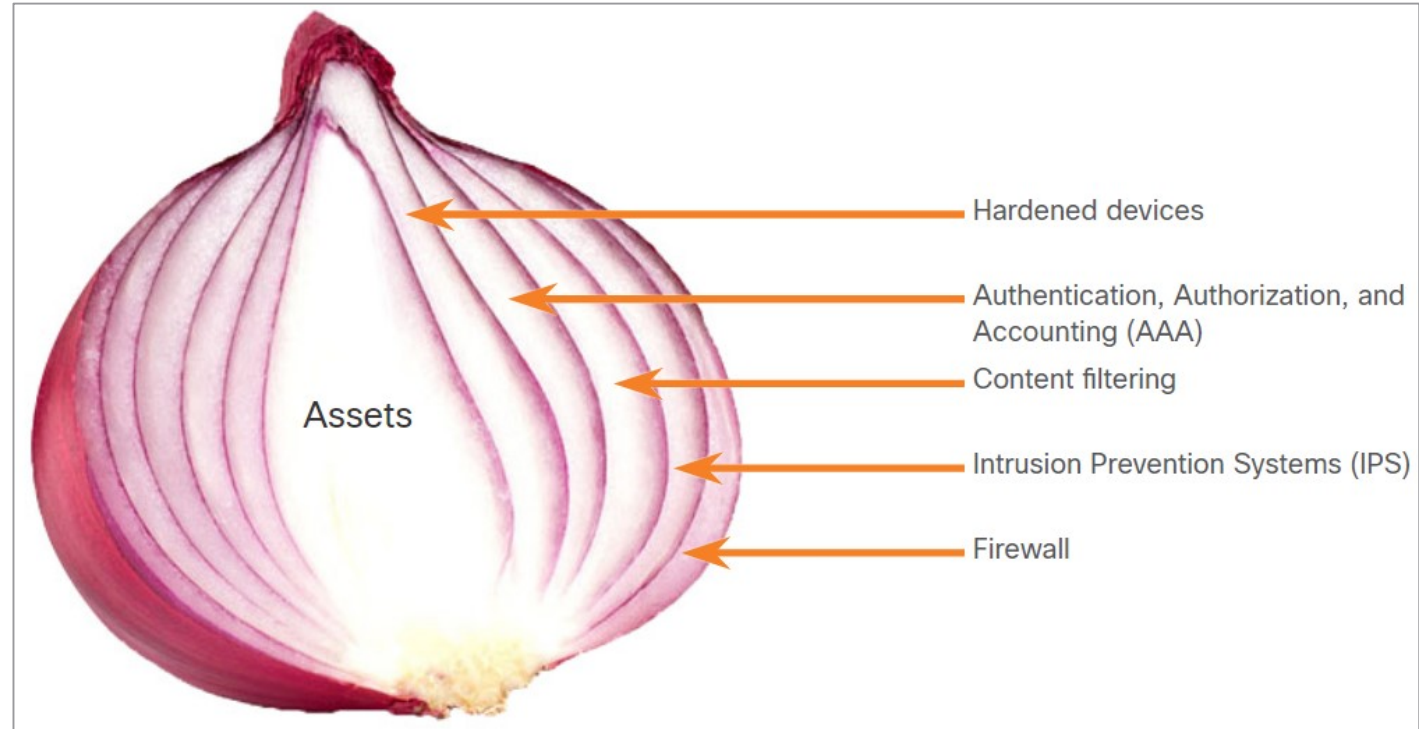


The Security Onion and The Security Artichoke

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 similar to peeling an onion.
- Only after penetrating each layer would the threat actor reach the target data or system.



Note: *The security onion described on this page is a way of visualizing defense-in-depth. This is not to be confused with the Security Onion suite of network security tools.*

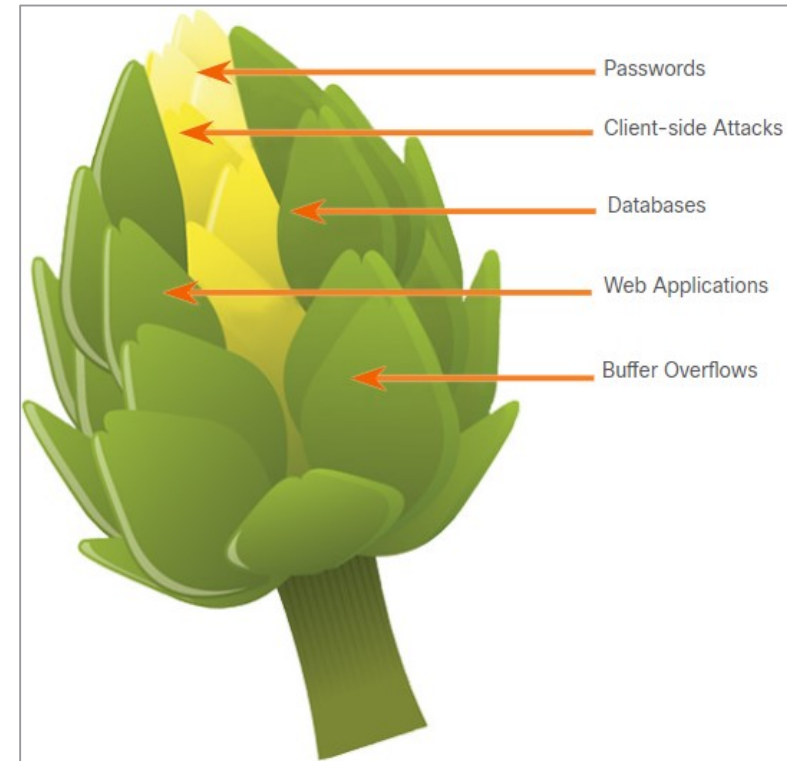
Understanding Defense

The Security Onion and The Security Artichoke

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 have to 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.

The **Borderless Networks Architecture** enables deployment of its systems and policies efficiently to provide **secure, reliable, and seamless** (*bezproblémový*) access to resources **from multiple locations, from multiple devices**, and to applications that can be **located anywhere**.



18.2 Security Policies, Regulations, and Standards

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.



Business Policies (Contd.)

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

Policy	Description
Company policies	<ul style="list-style-type: none">• It establishes the rules of conduct and the responsibilities of both <u>employees and employers</u>.• 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 (správanie), attendance, dress code, privacy and other areas related to the terms and conditions of employment.
Employee policies	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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 <u>evolving document</u> based on changes in the threat landscape, vulnerabilities, and business and employee requirements.

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 a number of benefits, including the following:
 - Závazok Demonstrates an organization's commitment to security
 - Pravidlá Sets the rules for expected behavior
 - Konzistencia Ensures consistency in system operations, software and hardware acquisition and use, and maintenance
 - Následky Defines the legal consequences of violations
 - Neignorovanie Gives security staff the backing of management
- A security policy also
 - specifies the **mechanisms** that are needed to meet **security requirements**
 - provides a **baseline** from which to acquire, configure, and audit computer systems and networks

Security Policies, Regulations, and Standards

Security Policy (Contd.)

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 <u>network resources</u> and <u>identity verification procedures</u> .
Password policies	These ensure passwords meet minimum requirements and are changed regularly.
Acceptable use policy (AUP)	It identifies <u>network applications and uses</u> that are acceptable to the organization. It may also identify ramifications (<i>dôsledky</i>) 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 <u>operating systems</u> and <u>end user application update procedures</u> .
Incident handling procedures	These describe how security incidents are handled.

BYOD Policies

- Bring Your Own Device (BYOD) enables employees to use their own mobile devices to access company systems, software, networks, or information.
- It provides key benefits to enterprises, including increased productivity, reduced costs, better mobility for employees, and so on. These benefits also bring an increased security risk as BYOD can lead to data breaches and greater liability for the organization.
- Therefore, a BYOD security policy should be developed to accomplish the following:
 - 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 (Contd.)

The following table lists the BYOD security best practices to help mitigate BYOD vulnerabilities:

Best Practice	Description
Password protect access	Use unique passwords for each device and account.
Manually control wireless connectivity	Turn off Wi-Fi and Bluetooth connectivity when not in use. Connect only to trusted networks.
Keep updated	Always keep the device OS and other software updated. Updated software often contains security patches to mitigate against the latest threats or exploits.
Back up data	Enable backup of the device in case it is lost or stolen.
Enable "Find my Device"	Subscribe to a device locator service with remote wipe feature.
Provide antivirus software	Provide antivirus software for approved BYOD devices.
Use Mobile Device Management (MDM) software	MDM software enables IT teams to implement security settings and software configurations on all devices that connect to company networks.

Regulatory and Standards Compliance

- There are also external regulations regarding network security.
- Network security professionals must be familiar with the laws and codes of ethics that are binding on Information Systems Security (INFOSEC) professionals.
- Many organizations are mandated to develop and implement security policies.
- **Compliance regulations** 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.

18.3 Understanding Defense Summary

What Did I Learn in this Module?

- The starting point for network defense is the identification of assets, vulnerabilities, and threats.
- Assets are anything of value to an organization that must be protected including servers, infrastructure devices, end devices, and the greatest asset, data.
- Vulnerabilities are weaknesses in a system or its design that could be exploited by a threat actor.
- Threats are any potential danger to an asset.
- Organizations must use a defense-in-depth approach to identify threats and secure vulnerable assets.
- Organizations must have a set of policies that define the activities that are allowed on the network.
- Business policies define standards of correct behavior for the business and its employees.

What Did I Learn in this Module? (Contd.)

- Security policies are used to inform users, staff, and managers of an organization's requirements for protecting technology and information assets.
- The purpose of a BYOD (Bring Your Own Device) policy is to enable employees to use their own mobile devices to access company systems, software, networks, or information.
- The compliance regulations that an organization is obligated to follow depend on the type of organization and the data that the organization handles.

New Terms and Commands

<ul style="list-style-type: none">• Assets• Vulnerabilities• Threats• Edge router• Internal router• Security Onion• Security Artichoke	<ul style="list-style-type: none">• Defense-in-Depth• Acceptable Use Policy (AUP)• Mobile Device Management (MDM)• Information Systems Security (INFOSEC)• BYOD
--	---



Module 19: 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.

19.1 Access Control Concepts

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.



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 (Contd.)

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

- **Zero Trust for the Workforce** (*pracovnú silu*) - 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** (*toky, prístupy*)- 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** (*pracovisko*) - 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

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) <i>(Podľa vlastného uváženia)</i>	<ul style="list-style-type: none">• 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)	<ul style="list-style-type: none">• 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 <i>(bezpečnostnej previerky)</i>.

Access Control

Access Control Models (Contd.)

Access Control Models	Description
Role-based access control (RBAC)	<ul style="list-style-type: none">• 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 <u>for the role</u>.• Also known as a type of non-discretionary access control.
Attribute-based access control (ABAC)	It allows access based on attributes of the object <u>to be accessed</u> , the subject <u>accessing the resource</u> , and environmental factors (<i>f. prostredia</i>) regarding <u>how</u> the object is to be accessed.
Rule-based access control (RBAC)	<ul style="list-style-type: none">• Network security staff specify sets of rules or conditions that <u>are associated with access to data or systems</u>.• These rules may specify <u>permitted or denied IP addresses, or certain protocols</u> 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 .

19.2 AAA Usage and Operation

AAA Operation

- A network must be designed to control **who** is allowed to connect to it and **what** they are allowed to do when they are connected. These design requirements are identified in the **network security policy**.
- The policy specifies **how network administrators, corporate users, remote users, business partners, and clients access** network resources.
- The network security policy can also **mandate** (*nariadit'*) the implementation of an **accounting system** that tracks who logged in and when and what they did while logged in.
- The Authentication, Authorization, and Accounting (**AAA**) protocol provides the necessary framework to enable **scalable access security**.

AAA Usage and Operation

AAA Operation (Contd.)

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

AAA Component	Description
Authentication KTO ?	<ul style="list-style-type: none">• Authentication can be established using <u>username and password</u> combinations, <u>challenge and response</u> questions, <u>token cards</u>, and other methods.• AAA authentication provides a centralized way to control access to the network.
Authorization ČO ?	<ul style="list-style-type: none">• 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 "<i>User can access host server XYZ using SSH only.</i>"
Accounting AKO ?	<ul style="list-style-type: none">• 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 <u>network resources are used</u>.• An example is "<i>User accessed host server XYZ using SSH for 15 minutes.</i>"

AAA Usage and Operation

AAA Operation (Contd.)

This concept is similar to 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.

The diagram illustrates the AAA (Authentication, Authorization, Accounting) process using a credit card analogy. It consists of three main parts: a credit card, a statement, and a transaction table.

Authentication: "Who are you?" - This is represented by the credit card, which identifies the user (JOE EMPLOYEE) and their account number (1234-567-890).

Authorization: "How much can you spend?" - This is represented by the credit limit on the statement, which is \$1,500.00.

Accounting: "What did you spend it on?" - This is represented by the transaction table, which lists all transactions and their amounts.

Statement of Personal Credit Card Account:

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

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

Credit Limit: \$1,500.00
Credit Available: \$1,221.50
New Balance: \$278.50
Minimum Payment Due: \$20.00

Account Summary:

Item	Amount	Item	Amount
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

Transaction Table:

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
2345678		01-30	Transaction Fees	\$3.00
34567890		01-01	Annual Fee	\$25.00

AAA Usage and Operation

AAA Authentication

- AAA Authentication can be used to authenticate users
 - for **administrative access**
 - for **remote network access**.
- Cisco provides two common methods for implementing AAA Services:
 - Local AAA
 - Server-based AAA
 - Centralized AAA

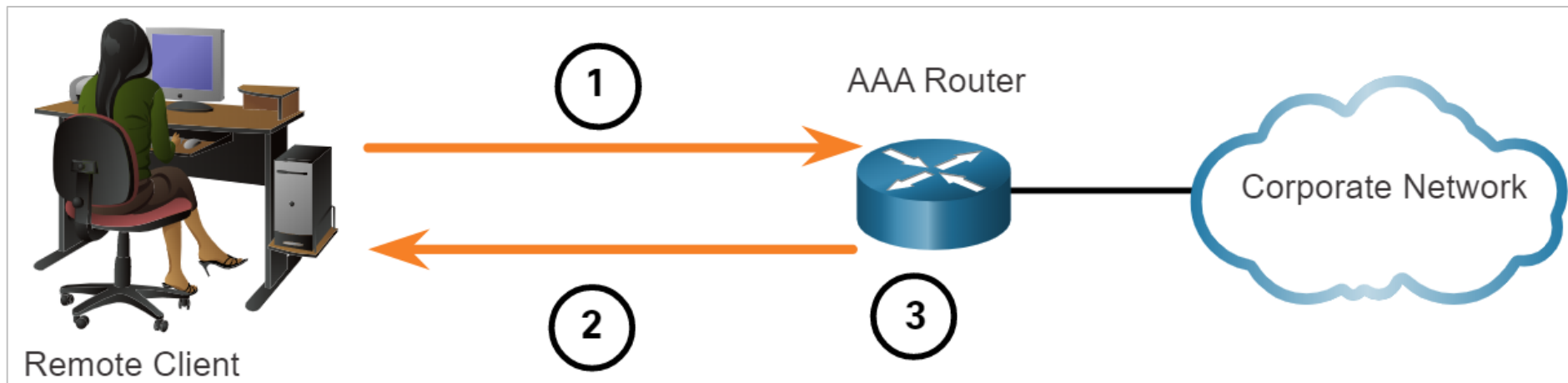
Local AAA Authentication

- 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**.

AAA Usage and Operation

Local AAA Authentication (Contd.)

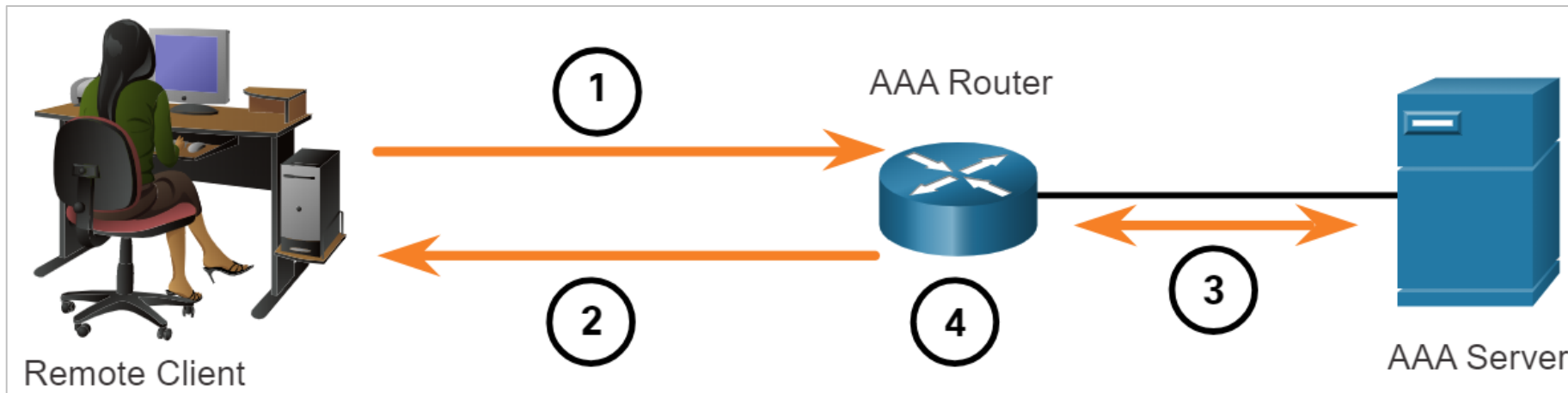
- The client establishes a connection with the router.
- The AAA router prompts the user for a username and password.
- The router authenticated the username and password using the local database and the user is provided access to the network based on information in the local database.



AAA Usage and Operation

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.
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 **AAA** server.
 4. The user is **provided access** to the network based on information in the remote AAA server.



Centralized AAA Authentication

- 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 use 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 (Contd.)

The following table lists the differences between the two protocols:

Functions	TACACS+	RADIUS
Functionality	It separates <u>authentication, authorization, and accounting</u> functions according to the AAA architecture. This allows modularity of the security server implementation.	It combines <u>authentication and authorization</u> but separates <u>accounting</u> , 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, it can support UNIX login, PPP, CHAP, or PAP

AAA Authentication (Contd.)

Functions	TACACS+	RADIUS
Confidentiality	Encrypts the <u>entire body</u> of the packet but leaves a standard TACACS+ header.	Encrypts <u>only the password</u> 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 <u>per-user</u> or <u>per-group</u> basis.	Has no option to authorize router commands on a per-user or per-group basis.
Accounting	Limited	Extensive

AAA Usage and Operation

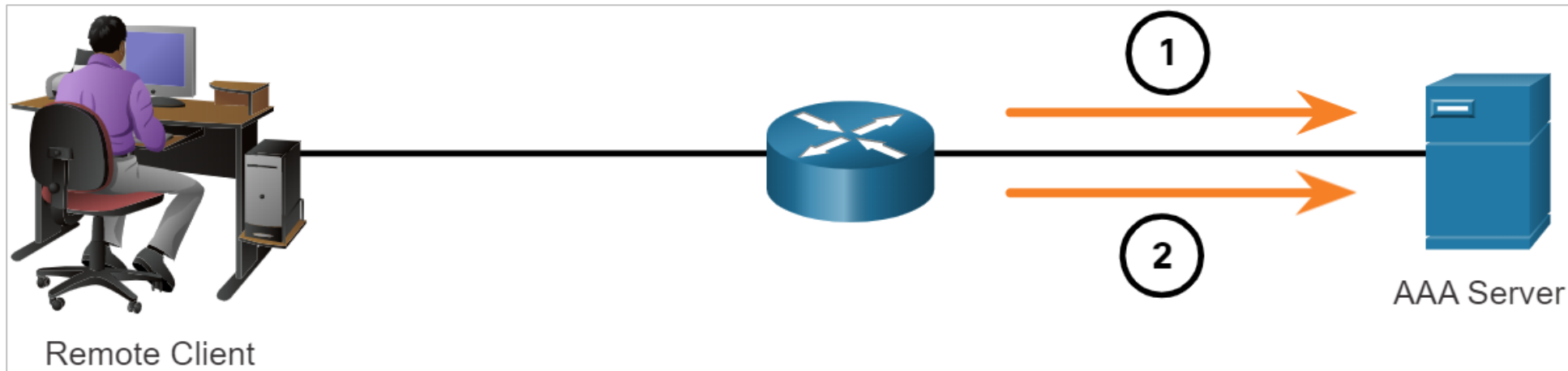
AAA Accounting Logs

- Centralized AAA also enables the use of the Accounting method.
- **Accounting records** from all devices are sent to centralized repositories, which simplifies **auditing** of user actions.
- AAA Accounting collects and reports usage data in **AAA logs**. These logs are useful for security **auditing**.
 - The collected data might include
 - start and stop connection times
 - executed commands
 - number of packets
 - number of bytes
- One widely deployed use of accounting is to combine it with AAA authentication. This helps with managing access to internetworking devices by network administrative staff.

AAA Usage and Operation

AAA Accounting Logs (Contd.)

- 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 <u>username, date, start and stop times, and the access server IP address</u> .
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.

19.3 Access Control Summary

What Did I Learn in this Module?

- The CIA triad consists of the primary three components of information security: confidentiality, integrity, and availability.
- Zero trust is a comprehensive approach to securing all access across networks, applications, and environments.
- The principle of zero trust is "never trust, always verify". The pillars of trust are zero trust for workforce, zero trust for workloads, and zero trust for workplace.
- In a zero trust approach, any place at which an access control decision is required should be considered a perimeter.
- Access control methods include discretionary access control (DAC), mandatory access control (MAC), role-based access control (RBAC), attribute-based control (ABAC), rule-based access (RBAC), and time-based access control (TAC).
- A network must be designed to control who is allowed to connect to it and what they are allowed to do when they are connected which is specified in the network security policy.

What Did I Learn in this Module? (Contd.)

- Authentication, Authorization, and Accounting (AAA) systems provide the necessary framework to enable scalable security.
- Cisco provides two common methods of implementing AAA services: Local AAA Authentication and Server-based AAA Authentication.
- Centralized AAA is more scalable and manageable than local AAA and is the preferred AAA implementation.
- Devices communicate with the centralized AAA server using with the Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access Control Systems (TACACS+) protocols.
- Centralized AAA also enables the use of the accounting method. AAA accounting collects and reports usage data in AAA logs.
- Various types of accounting information that can be collected are network accounting, connection accounting, EXEC accounting, system accounting, command accounting, and resource accounting.



Module 20: 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.

20.1 Information Sources

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 (Contd.)

The table lists the important network security organization.

Organization	Description
SysAdmin, Audit, Network, Security (SANS)	<p>SANS Institute resources are largely free upon request and include:</p> <ul style="list-style-type: none">• 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	<p>The Mitre Corporation maintains a list of Common Vulnerabilities and Exposures (CVE) used by prominent security organizations.</p>

Information Sources

Network Intelligence Communities (Contd.)

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) ..MS-ISAC	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.

Threat Intelligence

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.

Ukážka reportu z r. 2018:

Table of contents

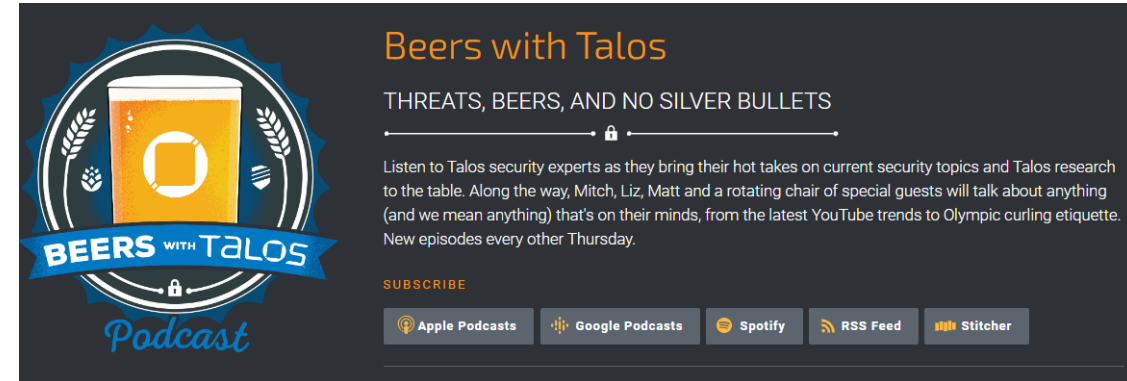
Executive summary	3
Part I: The attack landscape	6
The evolution of malware	6
Encrypted malicious web traffic	9
Email threats	14
Sandbox evasion tactics	22
Abuse of cloud services and other legitimate resources.....	24
IoT and DDoS attacks.....	31
Vulnerabilities and patching	38
Part II: The defender landscape	46
The cost of attacks	46
Challenges and obstacles	47
Complexity created by vendors in orchestration	48
Impact: Public scrutiny from breaches, higher risk of losses	50
Services: Addressing people and policies, as well as technology	53
Expectations: Investing in technology and training	54
Conclusion	57
About Cisco	60
Appendix	65

Threat Intelligence

Security Blogs and Podcasts

- Blogs and podcasts also provide
 - Advice
 - Research
 - 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.

<https://www.talosintelligence.com/podcasts>



Beers with Talos
THREATS, BEERS, AND NO SILVER BULLETS

Listen to Talos security experts as they bring their hot takes on current security topics and Talos research to the table. Along the way, Mitch, Liz, Matt and a rotating chair of special guests will talk about anything (and we mean anything) that's on their minds, from the latest YouTube trends to Olympic curling etiquette. New episodes every other Thursday.

SUBSCRIBE

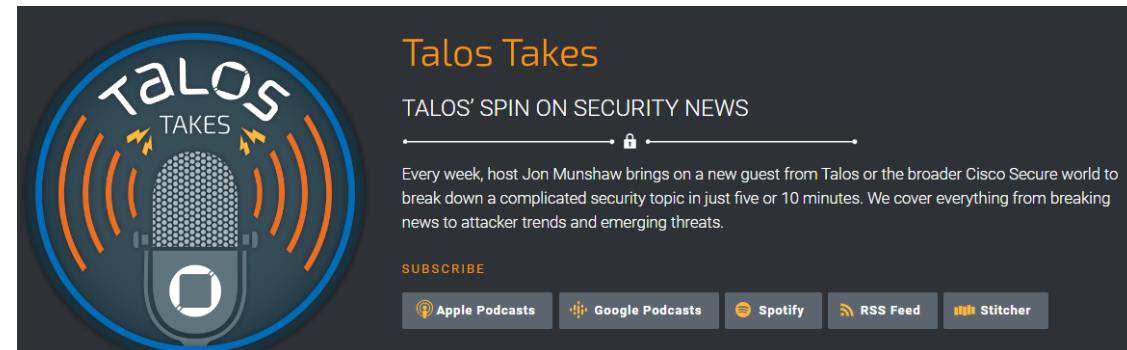
Apple Podcasts Google Podcasts Spotify RSS Feed Stitcher

[Im a skiddie, and you can too!](#)

[The intricacies of cyber conflict in Ukraine](#)

[A\(nother\) new host approaches!](#)

....



Talos Takes
TALOS' SPIN ON SECURITY NEWS

Every week, host Jon Munshaw brings on a new guest from Talos or the broader Cisco Secure world to break down a complicated security topic in just five or 10 minutes. We cover everything from breaking news to attacker trends and emerging threats.

SUBSCRIBE

Apple Podcasts Google Podcasts Spotify RSS Feed Stitcher

[The best \(and free\) ways to improve your cybersecurity skills](#)

[The basics of threat hunting](#)

[Tips for kickstarting your cybersecurity career](#)

[The latest on Lockbit 3.0 drama and the rest of the ransomware landscape](#)

....

20.2 Threat Intelligence Services

Threat Intelligence Services

Cisco Talos

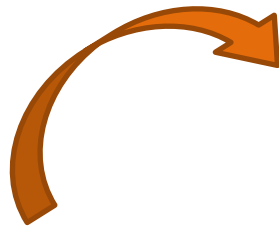
- Talos is one of the largest commercial **threat intelligence teams** in the world, and is comprised of world-class researchers, analysts and engineers.
- The goal is to **help protect** enterprise users, data, and infrastructure from active adversaries.
- The team collects information about active,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



Threat Intelligence Services

FireEye >> Trellix

- 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.



Featured FireEye Products



Helix Security Platform

Applies threat intelligence, automation, and case management.



Endpoint Security

Comprehensive endpoint defense to stop breaches in their tracks.



Email Security

Detects and blocks every kind of unwanted email, especially advanced attacks.



Cloud Security

Controls the cloud with our holistic cyber security approach.

January 19, 2022:

- McAfee Enterprise and FireEye Emerge as Trellix
 - a new business delivering **extended detection and response (XDR)** to organizations with a focus on accelerating technology innovation through **machine learning and automation**
 - Trellix's XDR ecosystem is designed to **accelerate the effectiveness** of **security operations** by providing customers with the capability to ingest over six hundred native and open security technologies

https://www.trellix.com/en-us/about/newsroom/news/news-detail.html?news_id=3e247ede-b638-4bb4-bd13-00b94a623e01



Trellix XDR Platform



Endpoint Security

Secure your organization with proactive endpoint detection, response, and prevention.

[Explore Endpoint Products →](#)



SecOps and Analytics

Conduct streamlined, efficient SecOps (Security Operations) and Analytics from a holistic foundation.

[Explore SecOps Products →](#)



Data Protection

Keep your information safe with a single integrated suite.

[Explore Data Protection Products →](#)



Network Detection and Response

Protect networks, servers, and data centers with a living, learning solution.

[Explore Network Products →](#)



Email Security

Keep your email infrastructure and users safe—whether on-premises or in the cloud.

[Explore Email Products →](#)



Cloud Security

Unlock unparalleled protection and productivity across your organization.

[Explore Cloud Products →](#)

FireEye >> Trellix (Contd.)

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.

NBU - Hlásenie kyber. bezpeč. incidentov

- Povinnosť pre prevádzkovateľov základných služieb, do 30 dní
- za základnú službu sa považuje služba, ktorá je zaradená v zozname základných služieb a
 1. závisí od sietí a informačných systémov a je vykonávaná aspoň v jednom sektore alebo podsektore,
 2. je prvkom kritickej infraštruktúry.
- Úrad zaradí základnú službu do zoznamu základných služieb a jej prevádzkovateľa do registra prevádzkovateľov základných služieb

Kritická infraštruktúra - pojmy

Sektor	Podsektor	Ústredný orgán
1. Doprava	Cestná doprava Letecká doprava Vodná doprava Železničná doprava	Ministerstvo dopravy a výstavby Slovenskej republiky
2. Elektronické komunikácie	Satelitná komunikácia Siete a služby pevných elektronických komunikácií a mobilných elektronických komunikácií	Ministerstvo dopravy a výstavby Slovenskej republiky
3. Energetika	Baníctvo Elektroenergetika Plynárenstvo Ropa a ropné produkty	Ministerstvo hospodárstva Slovenskej republiky
4. Pošta	Poskytovanie poštových služieb, poštový platobný styk a obstarávateľská činnosť	Ministerstvo dopravy a výstavby Slovenskej republiky
5. Priemysel	Farmaceutický priemysel Hutnícky priemysel Chemický priemysel	Ministerstvo hospodárstva Slovenskej republiky
6. Informačné a komunikačné technológie	Informačné systémy a siete	Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky
7. Voda a atmosféra	Meteorologická služba Vodné stavby Zabezpečovanie pitnej vody	Ministerstvo životného prostredia Slovenskej republiky
8. Zdravotníctvo		Ministerstvo zdravotníctva Slovenskej republiky
9. Financie	Bankovníctvo; tým nie sú dotknuté vylúčenia podľa osobitného predpisu o kybernetickej bezpečnosti. ¹⁰⁾ Finančné trhy; tým nie sú dotknuté vylúčenia podľa osobitného predpisu o kybernetickej bezpečnosti. ¹⁰⁾ Systémy riadenia verejných financií.	Ministerstvo financií Slovenskej republiky
10. Pôdohospodárstvo	poľnohospodárstvo potravinárstvo	Ministerstvo pôdohospodárstva a rozvoja vidieka Slovenskej republiky

§ 2

Vymedzenie základných pojmov

Na účely tohto zákona sa rozumie

a)

prvkom **kritickej infraštruktúry** (ďalej len „prvok“) najmä **inžinierska stavba,²⁾ služba** vo verejnom záujme a **informačný systém** v sektore kritickej infraštruktúry, ktorých narušenie alebo zničenie by malo podľa sektorových kritérií a prierezových kritérií závažné nepriaznivé dôsledky na uskutočňovanie hospodárskej a sociálnej funkcie štátu, a tým na kvalitu života obyvateľov z hľadiska ochrany ich života, zdravia, bezpečnosti, majetku, ako aj životného prostredia,

b)

sektorom **kritickej infraštruktúry** (ďalej len „sektor“) časť kritickej infraštruktúry, do ktorej sa zaraďujú prvky; sektor môže obsahovať **jeden alebo viac podsektorov** kritickej infraštruktúry (ďalej len „podsektor“),

c)

kritickou infraštruktúrou systém, ktorý sa člení na sektory a prvky,

<https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2011/45/#>

Focus areas

MITRE corporation

- * 1958, sponsored by the U.S, not-for-profit company, to serve as objective advisers in systems engineering to government agencies, both military and civilian
- is trusted to deliver data-driven results and recommendations without any conflicts of interest
- to convene government, industry, and academia to collaborate on big societal challenges, from pandemic response to highway safety to social justice
- operated [federally funded research and development centers](#), or FFRDCs
 - now operate six of the 42 FFRDCs in existence



Aerospace



AI & Machine Learning



Aviation & Transportation



Cybersecurity



Defense & Intelligence



Government Innovation



Health



Homeland Security



Telecom

Common Vulnerabilities and Exposures (CVE) Database

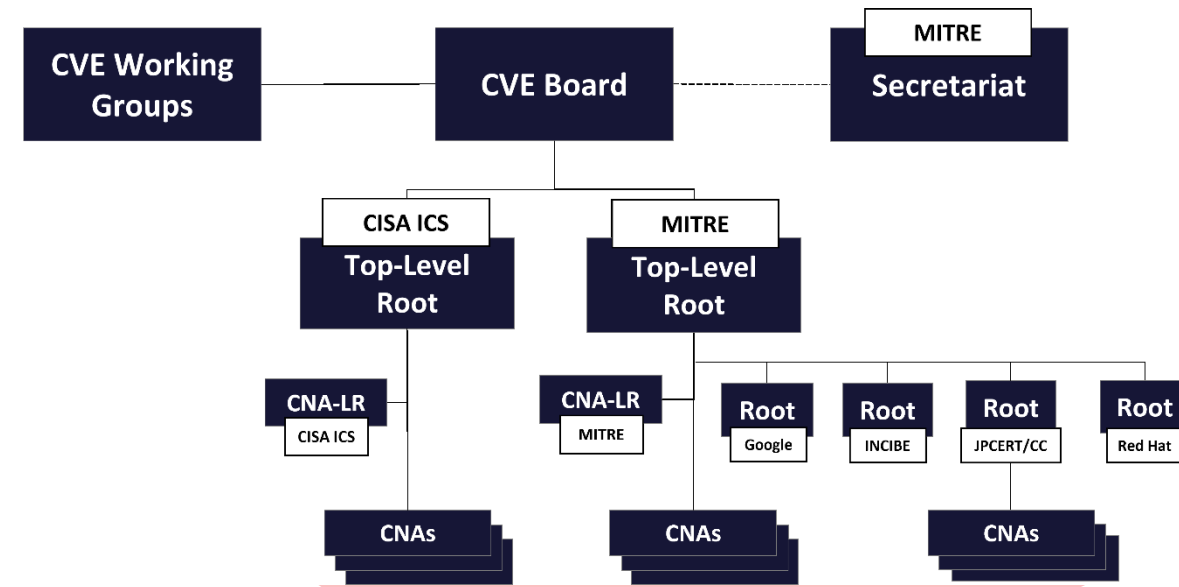
- US government sponsored the MITRE Corporation to create and maintain a catalog of known security threats called Common Vulnerabilities and Exposures (CVE).
- CVE Program Mission for publicly known cybersecurity vulnerabilities:

to identify and define	defines unique CVE Identifiers
to catalog	there are 188,049 CVE Records accessible (5.11.2022), which can be search and downloaded

Root – managerial functions
CNA (CVE Numbering Authority) – operational functions

Each CVE Record includes the following:

- CVE ID [number](#) with four or more digits in the sequence number portion of the ID (e.g., "CVE-1999-0067", "CVE-2014-12345", "CVE-2016-7654321").
- Brief [description](#) of the security vulnerability.
- Any pertinent [references](#) (i.e., vulnerability reports and advisories).
- State: Reserved/Published/Rejected



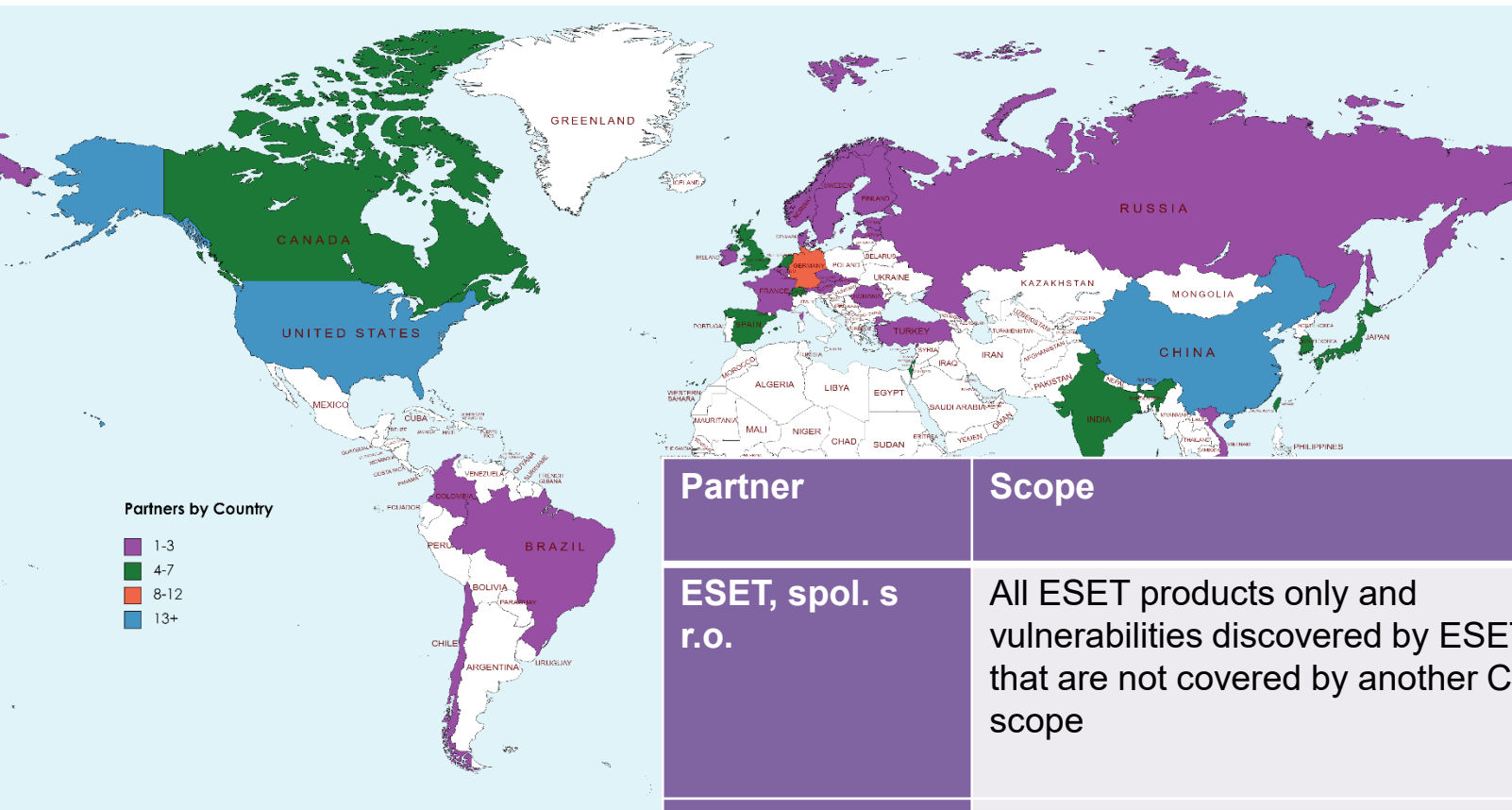
<https://cve.mitre.org/> → in progress

<https://www.cve.org/>

Confidential

There are currently **251** partners from **35** countries participating

Sú CNA partneri aj zo SR?



<https://www.cve.org/ProgramOrganization/CNAs>

<https://www.cve.org/PartnerInformation/ListofPartners>

Partner	Scope	Program Role	Organization Type	Country*
ESET, spol. s r.o.	All ESET products only and vulnerabilities discovered by ESET that are not covered by another CNA's scope	CNA	Vendors and Projects, Vulnerability Researchers	Slovak Republic
National Cyber Security Centre SK-CERT	Vulnerabilities in software discovered by National Cyber Security Centre SK-CERT, and vulnerabilities reported to National Cyber Security Centre SK-CERT for coordinated disclosure, which are not in another CNA's scope	CNA	National and Industry CERTs	Slovak Republic

U.S. – Department of Homeland Security (DHS)

<https://www.dhs.gov/operational-and-support-components>

- is designated as the Sector Risk Management Agency for the Emergency Services Sector, which provides a wide range of prevention, preparedness, response, and recovery services during both day-to-day operations and incident response
- Operational and Support Components that currently make up the DHS:

 <p>U.S. Immigration and Customs Enforcement</p> <p>United States Immigration and Customs Enforcement (ICE)</p>	 <p>United States Secret Service (USSS)</p> <p>USSS safeguards the</p>	 <p>Transportation Security Administration (TSA)</p>
 <p>Management Directorate</p> <p>Management Directorate</p>	 <p>Science and Technology</p> <p>Science and Technology Directorate (S&T)</p>	 <p>Countering Weapons of Mass Destruction</p> <p>Countering Weapons of Mass Destruction Office (CWMD)</p>
 <p>Intelligence and Analysis</p> <p>Office of Intelligence and Analysis</p>	 <p>Office of Operations Coordination</p> <p>Office of Operations Coordination (OPS)</p>	 <p>Citizenship and Immigration Services Ombudsman</p>  <p>Ombudsman Offices</p>



U.S. Citizenship and Immigration Services

U.S. Citizenship and Immigration Services (USCIS)




United States Coast Guard (USCG)




United States Customs and Border Protection

United States Customs and Border Protection (CBP)




CISA
CYBER+INFRASTRUCTURE

Cybersecurity and Infrastructure Security Agency (CISA)



FEMA

Federal Emergency Management Agency (FEMA)



Federal Law Enforcement Training Center

Federal Law Enforcement Training Center (FLETC)

Threat Intelligence Services

Automated Indicator Sharing



Homeland
Security



CYBERSECURITY
& INFRASTRUCTURE
SECURITY AGENCY



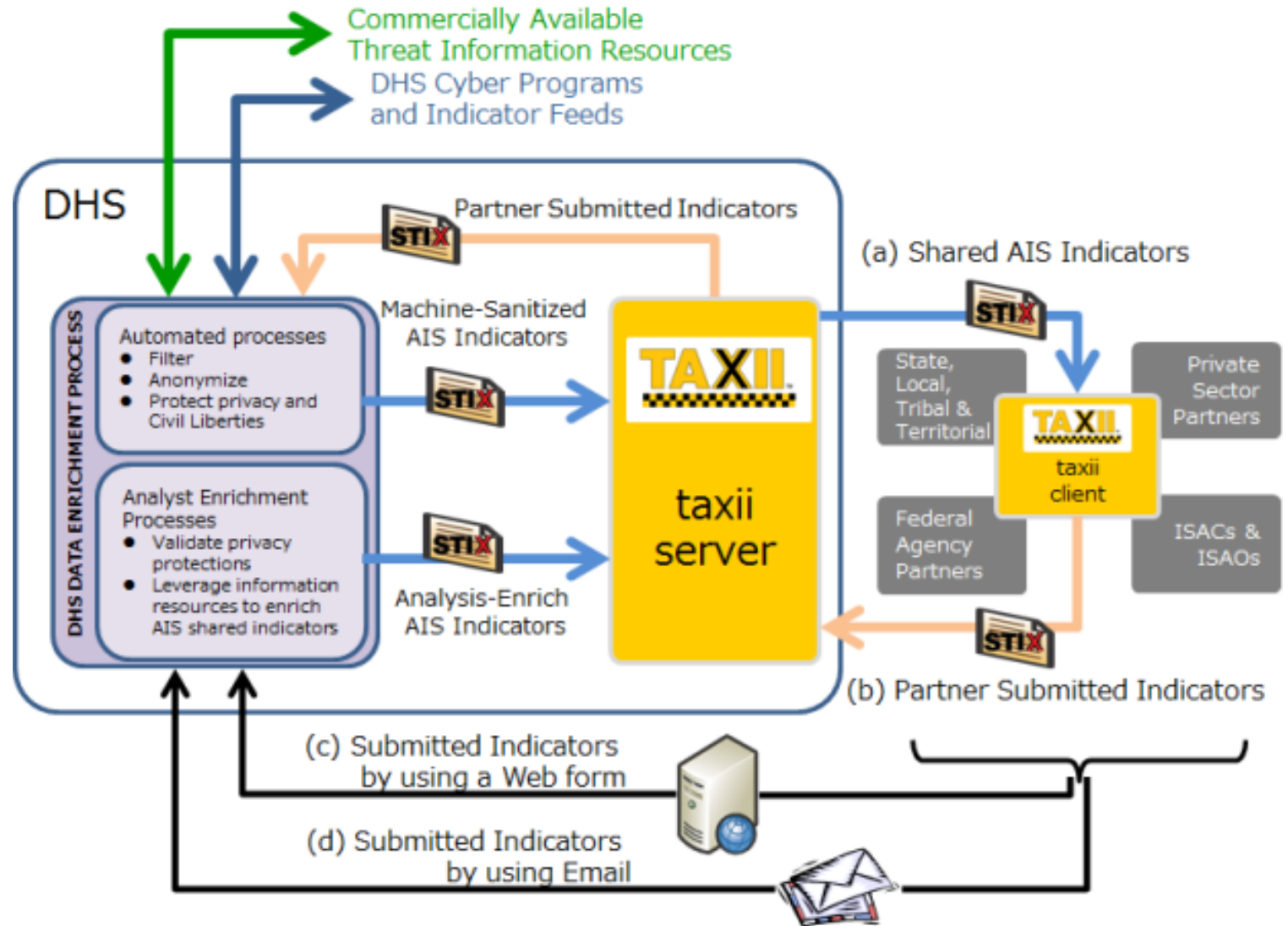
- The Automated Indicator Sharing (AIS) is a free service offered by the U.S DHS – by CISA
- AIS enables the real-time **exchange** of **cyber threat** indicators between
 - the U.S. Federal Government
 - and the private sector.
- AIS creates an **ecosystem** when a threat is recognized.
- Later, it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

<https://www.cisa.gov/ais>

Automated Indicator Sharing

Open Standards for AIS

- AIS uses open standards:
 - STIX™ = Structured Threat Information Expression for CTIs and DMs information
 - TAXII™ = Trusted Automated Exchange of TCIs for machine-to-machine communications
 - specification for an application layer protocol that allows the communication of CTIs over HTTPS. TAXII is designed to support STIX.
- CISA respects organizational privacy
 - AIS anonymizes submissions by default when transmitting them
 - identity of the submitter is not revealed without the prior express consent of the submitter

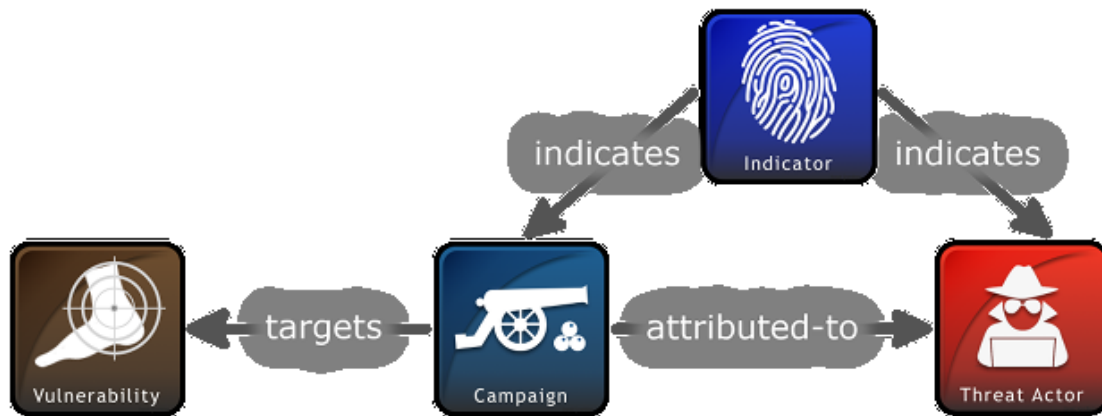


<https://www.hitachi.com/hirt/publications/hirt-pub17007/index.html>

Zneužitelné ciele a ich popis

STIX and CVE in an Exploit Target

- Threat intelligence often contains references to the vulnerabilities that threat actors are targeting
 - When those vulnerabilities have been formally **disclosed** (*zverejnené*) and **identified** (i.e., are not 0-day or unknown vulnerabilities), they are almost **always** identified via a **CVE**
- ExploitTargets** are **vulnerabilities** or **weaknesses** in software, systems, networks or configurations that are **targeted for exploitation** by the **TTP** (tactics, techniques, and procedures) of a ThreatActor



STIX Exploit Target consists of:

Field Name	Type	Description
@id optional	QName	Specifies a globally unique identifier for this ExploitTarget.
@idref optional	QName	Specifies a globally unique identifier of an ExploitTarget specified elsewhere. When idref is specified, the id attribute must not be specified, and any instance of this ExploitTarget should not hold content.
@timestamp optional	dateTime	Specifies a timestamp for the definition of a specific version of an ExploitTarget. When used in conjunction with the id, this field is specifying the definition time for the specific version of the ExploitTarget. When used in conjunction with the idref, this field is specifying a reference to a specific version of an ExploitTarget defined elsewhere. This field has no defined semantic meaning if used in the absence of either the id or idref fields.
@version optional	ExploitTargetVersionType	Specifies the relevant STIX-ExploitTarget schema version for this content.
Title 0..1	string	The Title field provides a simple title for this ExploitTarget.
Description 0..n	StructuredTextType	The Description field is optional and provides an unstructured, text description of this ExploitTarget.
Short_Description 0..n	StructuredTextType	The Short_Description field is optional and provides a short, unstructured, text description of this ExploitTarget.
Vulnerability 0..n	VulnerabilityType	The Vulnerability field identifies and characterizes a Vulnerability as a potential ExploitTarget. (CVE ID, OSVDB ID, ..)
Weakness 0..n	WeaknessType	The Weakness field identifies and characterizes a Weakness as a potential ExploitTarget.
Configuration 0..n	ConfigurationType	The Configuration field identifies and characterizes a Configuration as a potential ExploitTarget.

.....

Vulnerability in MS Internet Explorer

Example: [CVE-2013-3893](#) using the STIX exploit target element

Exploit Target	
ID	example:et-48a276f7-a8d7-bba2-3575-e8a63fcd488b
Title	Javascript vulnerability in MSIE 6-11
Vulnerability	
CVE ID	CVE-2013-3893

Implementation

XML

Python Producer

Python Consumer

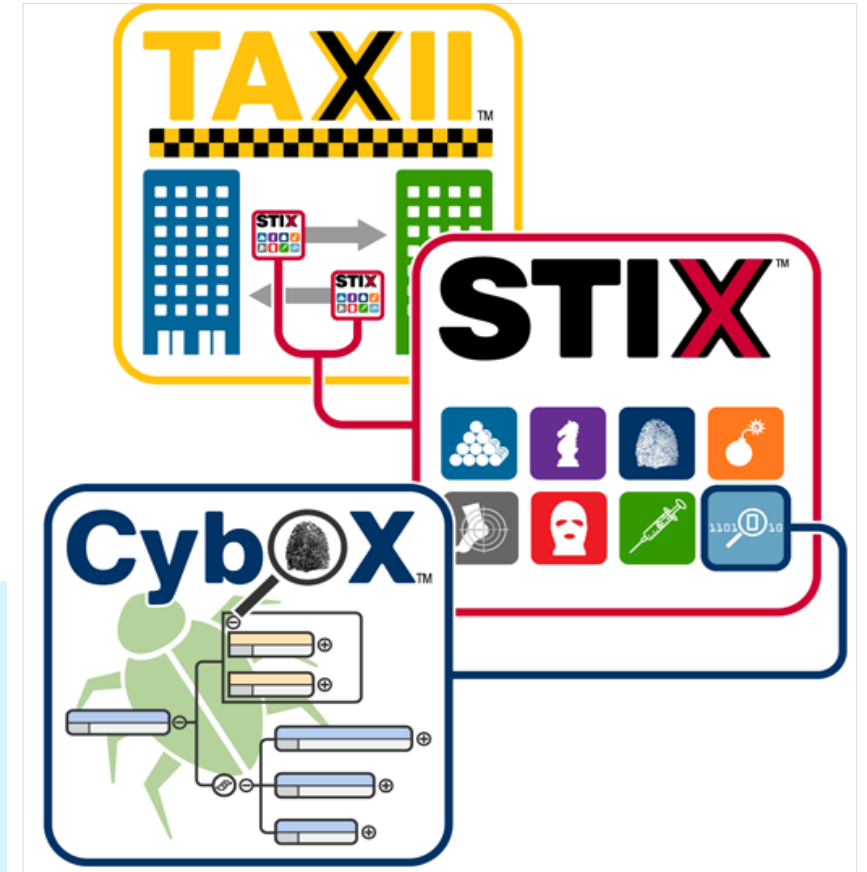
```
1 from stix.core import STIXPackage
2 from stix.exploit_target import ExploitTarget, Vulnerability
3
4 vuln = Vulnerability()
5 vuln.cve_id = "CVE-2013-3893"
6 vuln.add_reference("https://technet.microsoft.com/library/security/2887505")
7
8 et = ExploitTarget(title="Javascript vulnerability in MSIE 6-11")
9 et.add_vulnerability(vuln)
10
11 print et.to_xml(encoding=None)
```

<https://stixproject.github.io/documentation/idioms/cve/>

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 CTI 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.



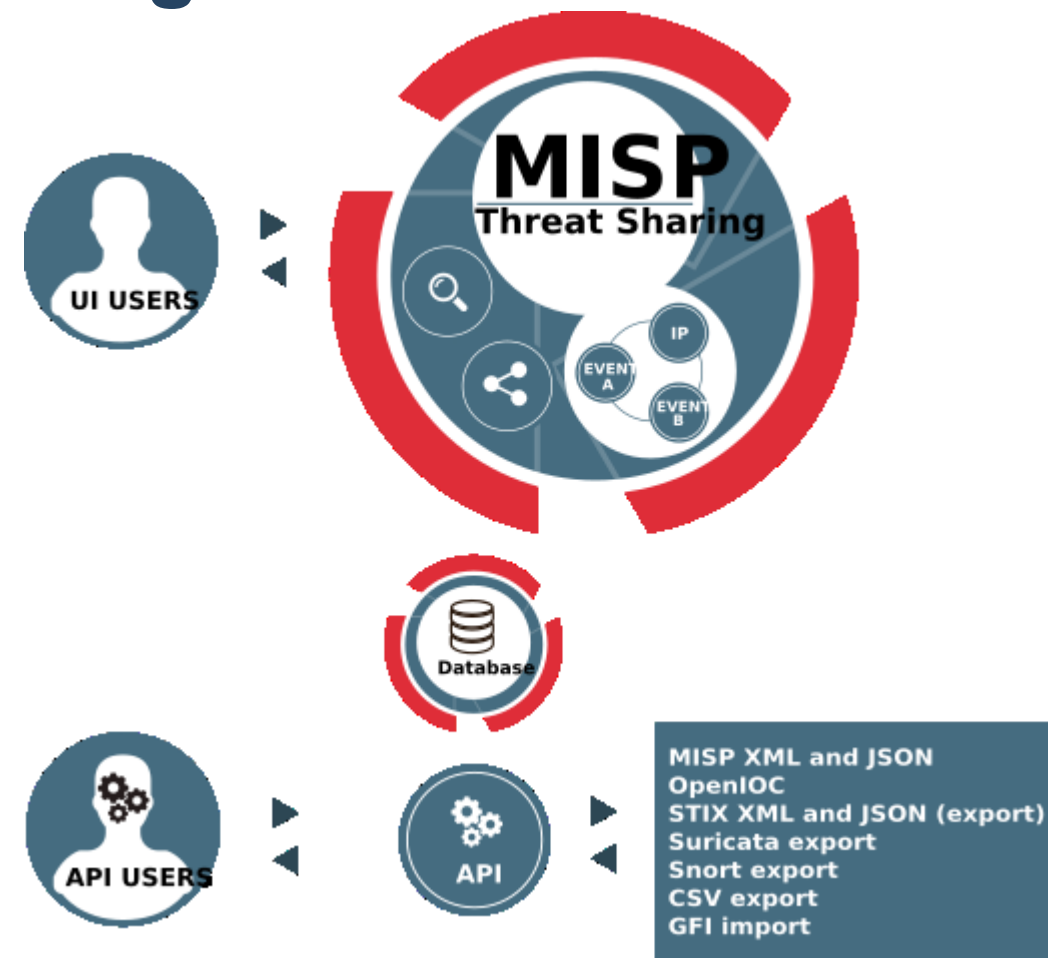
CybOX™ - Cyber Observable eXpression



- structured Language for Cyber Observables
- Examples of cyber observables include:
 - Registry Key is created
 - File is deleted
 - Mutex (lock) exists
 - Specific HTTP Get Request received
 - file has a specific MD5 hash
 - Data is sent to an address on a socket
 - Network traffic occurs to specific IP addresses
 - Email from a specific address is observed
 - Application logs show communication on certain ports
 - A service's configuration is changed
 - A remote thread is created
- support a wide range of cyberSec domains:
 - Threat assessment and characterization (detailed attack patterns)
 - Malware characterization
 - Operational event management
 - Logging
 - Cyber situational awareness
 - Incident response
 - Indicator sharing
 - Digital forensics
 - Etc.

MISP - Malware Information Sharing Platform

- The Malware Information Sharing Platform (MISP) is an open source platform for sharing IOCs for newly discovered threats.
- MISP is supported by the EU 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
 - Sharing and import data:
 - by generating **Snort/Suricata/Bro/Zeek IDS rules**
 - by **STIX, OpenIOC, text or csv** exports



<https://www.misp-project.org/features/>

MISP - Malware Information Sharing Platform

OSINT - CVE-2015-2545: overview of current threats

Event ID	3865
Uuid	57460863-76dc-4272-8116-4ea302de0b81
Org	CIRCL
Owner org	CIRCL
Contributors	
Email	alexandre.dulsunoy@circl.lu
Tags	ftp:white x circl:osint-feed x Type:OSINT x estimative-language:likelihood-probability-"very-likely" x +
Date	2016-05-25
Threat Level	Medium
Analysis	Completed
Distribution	All communities
Info	OSINT - CVE-2015-2545: overview of current threats
Published	Yes
Sightings	0 (0)

Related Events

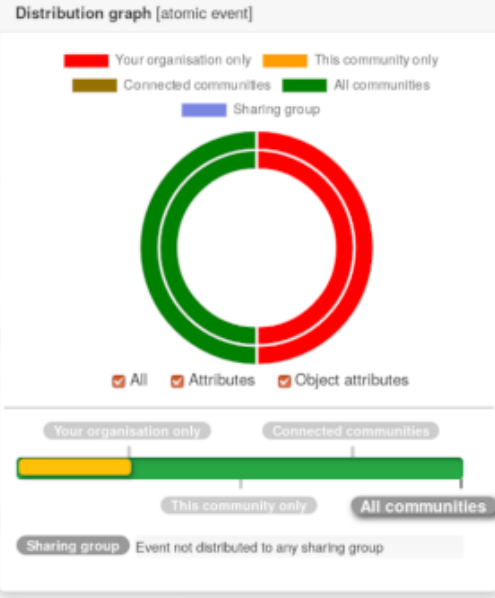
2016-05-27 (3883)	Org: CIRCL
2016-05-23 (3844)	Date: 2016-05-23
2016-05-06 (3826)	Info: OSINT - Operation Ke3chang
	Resurfaces With New TidePool Malware



Expanded	Events	Tag	Action
Likelihood or probability: Almost no chance - remote - 01-05%	0	estimative-language:likelihood-probability-"almost-no-chance"	
Likelihood or probability: Very unlikely - highly improbable - 05-20%	0	estimative-language:likelihood-probability-"very-unlikely"	

Malicious activities

Event ID: 10878
 Uuid: 5a6c700c-0eb8-468
 Org: CIRCL
 Owner org: CIRCL
 Contributors: alexandre.dulaunoy
 Email: alexandre.dulaunoy
 Tags: [icon]
 Date: 2018-05-04
 Threat Level: Low
 Analysis: Initial
 Distribution: All communities
 Info: Malicious activities
 Published: No
 #Attributes: 2
 Last change: 2018/05/04 02:38:12
 Extends: [empty]
 Extended by: [empty]
 Sightings: 0 (0)
 Activity: [empty]



Threat Level: Low
 Analysis: Initial

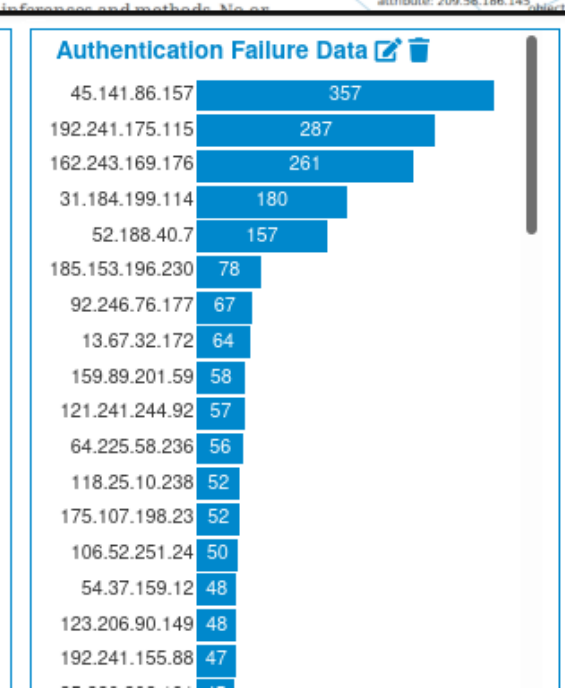
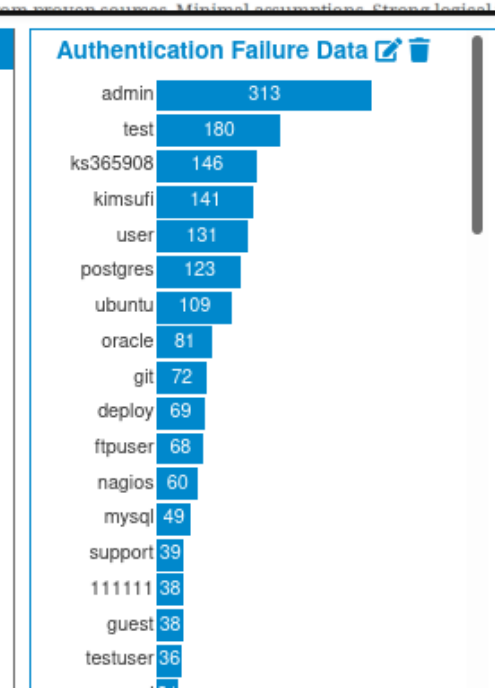
Event Info: Ransomware found on a production server

Extends event: 5ad8687b-De10-4a8b-a157-46a5950d210f

Matched event
 Id: 10728
 Analysis: Completed
 Threat level: Low
 Tags:
 - `circl:osint-feed` `tip:white`
 - `malware_classification:malware-category="Ransomware"`
 - `osint:source-type="blog-post"`
 - `misp-galaxy:ransomware="CSGO Ransomware"`
 - `misp-galaxy:ransomware="MC Ransomware"`
 Info: OSINT - Minecraft & CS:GO Ransomware Srv For Media Attention

estimative-language:confidence-in-analytic-judgment="high"
 High

View Dashboard
 Add Widget
 Import Config JSON
 Export Config JSON
 Save Dashboard Config
 List Dashboard Templates



Achievements of my organization

Achievements Unlocked!

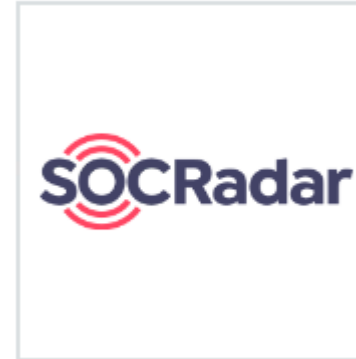
- Event**: Congratulations, you have shared your first event!
- Tagging**: You have been using tags, good job!
- Taxonomy**: Taxonomies have been used in your events.
- Galaxy**: Galaxies have no secrets for you in this Threat Sharing universe.

Next on your list:

Threat Intelligence Services

Threat Intelligence Platforms

- A Threat Intelligence Platform (TIP) centralizes the collection of threat data from numerous data sources and formats.
- **Types of threat Intelligence data:**
 - Indicators of Compromise (IOC)
 - Tools Techniques and Procedures (TTP)
 - Reputation information about internet destinations or domains
- Organizations can contribute to threat intelligence by sharing their intrusion data over the internet, typically through automation.
- Honeypots are simulated networks or servers that are designed to attract attackers. The attack-related information gathered from honeypots can be shared with threat intelligence platform subscribers.



Brandefense Digital Risk
Protection Platform
by Brandefense



20.3 Threat Intelligence Summary

What Did I Learn in this Module?

- Many organizations such as SANS, Mitre, FIRST, SecurityNewsWire, (ISC)2, and CIS provide network intelligence.
- The network security professionals must keep abreast of the latest threats and continue to upgrade skills.
- Threat intelligence services allow the exchange of threat information such as vulnerabilities, Indicators of Compromise (IOC), and mitigation techniques.
- Cisco Talos is one of the largest commercial threat intelligence teams in the world.
- 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.

What Did I Learn in this Module? (Contd.)

- The U.S Department of Homeland Security (DHS) offers a free service called Automated Indicator Sharing (AIS).
- AIS enables real-time exchange of cyber threat indicators between the U.S. Federal Government and the private sector.
- The United States government sponsored the MITRE Corporation to create and maintain a catalog of known security threats called Common Vulnerabilities and Exposure (CVE).
- Three common threat intelligence sharing standards include Structured Threat Information Expression (STIX), Trusted Automated Exchange of Indicator Information (TAXII), and CybOX.



UNIVERSITY OF ŽILINA
Faculty of Management Science
and Informatics

Ďakujem za pozornosť

Obsahom boli moduly:

Chapter 18 Understanding Defense (security management)

Chapter 19 Access Control (AAA)

Chapter 20 Threat Intelligence (commercials, CVE database)

Vyjadrite spätnú väzbu na prednášku a/alebo cvičenie v anonymnej ankete cez google form: [link](#)