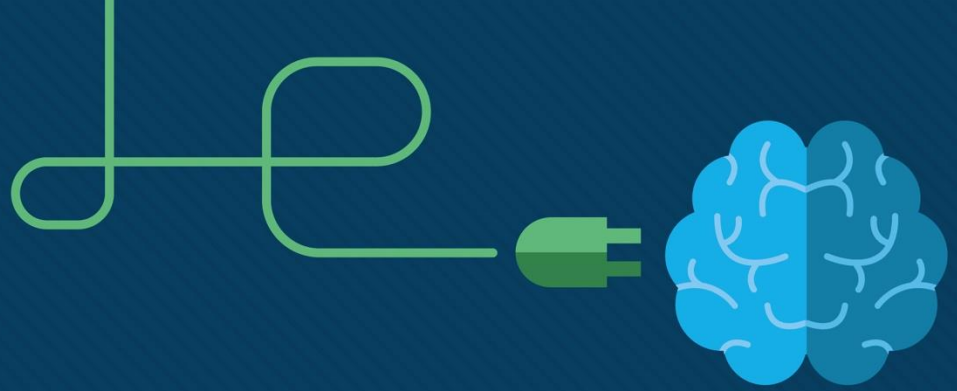


Module 20: Threat Intelligence

CyberOps Associate v1.0

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.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

20.1 Information Sources

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Network Intelligence Communities (Contd.)

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	The Mitre Corporation maintains a list of Common Vulnerabilities and Exposures (CVE) used by prominent security organizations.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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)	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.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

20.2 Threat Intelligence Services

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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 the Snort.org, ClamAV, and SpamCop network security tools.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

FireEye (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.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Common Vulnerabilities and Exposures (CVE) Database

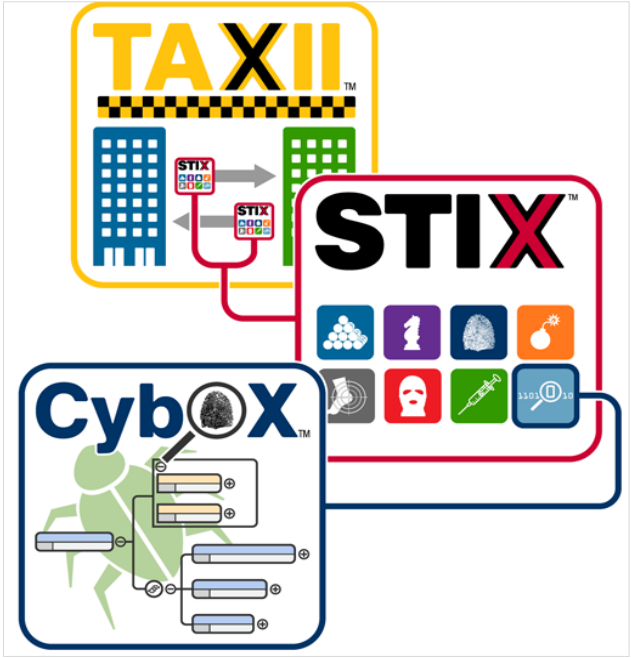
- The United States government sponsored the MITRE Corporation to create and maintain a catalog of known security threats called Common Vulnerabilities and Exposures (CVE).
- The CVE serves as a dictionary of CVE Identifiers for publicly known cybersecurity vulnerabilities.
- The MITRE Corporation defines unique CVE Identifiers for publicly known information-security vulnerabilities to make it easier to share data.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Threat Intelligence Communication Standards (Contd.)

- The Malware Information Sharing Platform (MISP) is an open source platform for sharing 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 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.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

20.3 Threat Intelligence Summary

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential


CISCO