Threat and Vulnerability Management

Domain 1.0

The Importance of Threat Data and Intelligence

Chapter 1

Episode 1.01

Intelligence Sources and Confidence Levels

Objective 1.1 Explain the importance of threat data and intelligence.

- Intelligence sources
  - Open-source intelligence
  - Proprietary/closed-source intelligence
  - Timeliness
  - Relevancy
  - Accuracy
- Confidence levels

Intelligence Sources

- Open-source intelligence (OSINT)
- Closed-source/ proprietary intelligence

OSINT

- Intelligence anyone can find
- Source examples
  - Google
  - Job sites
  - Internet registries
  - Social media

Closed-Source Intelligence

- Privileged access
- Covertly collected

Gathering Important Information

- Timeliness
  - Recent or current data
- Relevancy
  - Does it pertain to your objective?
- Accuracy
  - Is intelligence correct?

Confidence Levels

- Evaluation metric determined by timeliness, relevancy, and accuracy
- Assessment of information from sources
- Trust of information's quality
  - High
  - Medium
  - Low
- Impact likelihood of resulting action

Episode 1.02

Threat Indicators and Actors

Objective 1.1 Explain the importance of threat data and intelligence.

- Indicator management
  - Structured Threat Information eXpression (STIX)
  - Trusted Automated eXchange of Indicator Information (TAXII)
  - OpenIoC
- Threat actors
  - Nation-state
  - Hacktivist
  - Organized crime
  - Insider threat
  - Intentional
  - Unintentional

Indicator

- Result of an observable event in a network
- Any event used to gain understanding
- Organizations needed to create standards for threat documentation and communication

Indicator Management

- Structured Threat Information eXpression (STIX)
  - MITRE Corporation
  - Effort to standardize threat data communication and documentation

Structured Threat Information eXpression (STIX)

- 12 STIX domain objects (SDOs)
  - Attack pattern
  - Campaign
  - Course of action
  - Grouping
  - Identity
  - Indicator
  - Intrusion set
  - Malware
  - Observed data
  - Report
  - Threat actor
  - Tool
- 2 STIX relationship objects (SROs)
  - Sighting – something has occurred
  - Relationship – connection between two SDOs

Structured Threat Information eXpression (STIX)

- Example relationship:

- Defines how threat data is formally documented in standard format
- Results in ability to exchange STIX documents with other organizations

Exchanging Threat Data

- Trusted Automated eXchange of Indicator Information (TAXII)
  - Defines how STIX data is transferred via API
  - Makes STIX data available to other entities
- OpenIOC
  - Open-source
  - Created by Mandiant (now part of FireEye)
  - Framework for collecting and exchanging indicators of compromise data

Threat Actors

- Nation-state
  - Sophisticated and well-funded
  - On behalf of government or government agency
- Hacktivist
  - Individual or groups that pursue social goal through hacking
- Organized crime
  - In it for the money
  - Often uses ransomware
- Insider threat
  - Intentional
    - Ex: disgruntled employee
  - Unintentional
    - Ex: victim of social engineering

Episode 1.03

Threat Trends

Objective 1.1 Explain the importance of threat data and intelligence.

- Threat classification
  - Known threat vs. unknown threat
  - Zero-day
  - Advanced persistent threat

Threat Classification

- Known vs. unknown threats
- Absence of evidence isn't evidence of absence
- Zero-day
  - Exploits an undiscovered vulnerability

Advanced Persistent Threat (APT)

- Advanced
  - Well-funded
  - Often from a nation state
  - Coordinated
- Persistent
  - 24/7
  - Security professional may work non-standard hours
- Threat
  - Threat actors are very focused
  - Geopolitical motivation
  - Technical methods

Hacktivism

- Politically or socially motivated
- Nuisance
- Decentralized
- Ad-hoc
- Easy to participate

Cyber Warfare Timeline

Attributions: https://www.flickr.com/photos/intelfreepress/10477292993

Episode 1.04

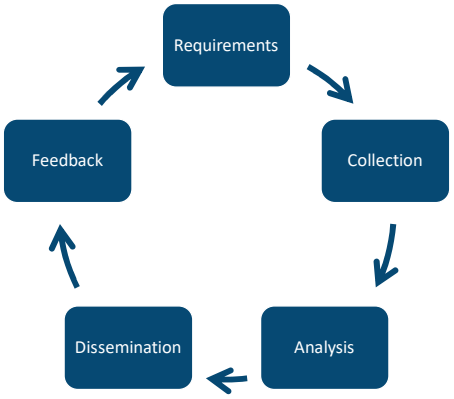
Intelligence Cycle and ISACs

Objective 1.1 Explain the importance of threat data and intelligence.

- Intelligence cycle
  - Requirements
  - Collection
  - Analysis
  - Dissemination
  - Feedback
- Commodity malware
- Information sharing and analysis communities
  - Healthcare
  - Financial
  - Aviation
  - Government
  - Critical infrastructure

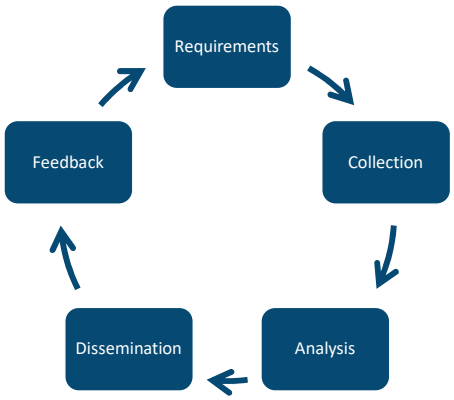
Intelligence Cycle

- Method to translate raw data into actionable information



Intelligence Cycle

- Requirements
  - What you need
  - Example: domain registrations, contact names, addresses, etc.
- Collection
  - Collect the data
  - OSINT or proprietary sources
- Analysis
  - Look at what you have
  - CompTIA CySA+ exam emphasizes this step
  - Find importance and meaning
- Dissemination
  - Explanation of analysis
  - Recommendation of action given to customer
- Feedback
  - Response of the customer
- If customer requires more information, start cycle again



Commodity Malware

- Malware for sale
  - Popular in underground communities
  - Allows attackers with limited skills to engage
- Malware-as-a-service

Information Sharing

- Communities exist to facilitate information sharing
- Information Sharing and Analysis Centers (ISACs)

Information Sharing and Analysis Centers (ISACs)

- Example industries:
  - Automotive
  - Aviation
  - Communications
  - Electricity
  - Elections
  - Financial
  - Healthcare
  - Information technology
  - MultiState

ISAC	Description
Automotive (Auto-ISAC)	Founded in 2015, Auto-ISAC is the primary mechanism for global car manufacturers to share information about threats, vulnerabilities, and best practices related to connected vehicles.
Aviation (A-ISAC)	Open to trusted global private aviation companies, A-ISAC works with public aviation entities to ensure resilience of the shared global air transportation network.
Communications (NCC)	Also known as the National Coordinating Center for Communications, NCC facilitates the sharing of threat and vulnerability information among communications carriers, ISPs, satellite providers, broadcasters, vendors, and other stakeholders.
Electricity (E-ISAC)	Working with the US Department of Energy and the Electricity Subsector Coordinating Council (ESCC), the E-ISAC establishes awareness of incidents and threats relevant to the electricity sector.
Elections Infrastructure (EI-ISAC)	Established in 2018, EI-ISAC enables election bodies, from local municipalities to the federal government, to ensure the security and integrity of elections. The EI-ISAC is spearheaded by the nonprofit Center for Internet Security (CIS) and routinely collaborates with the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency and the Election Infrastructure Subsector Government Coordinating Council (GCC).
Financial Services (FS-ISAC)	As one of the oldest ISACs, the FS-ISAC has existed in support of the resilience and continuity of the global financial services infrastructure with information sharing, education, and collaboration initiatives between private firms and government agencies.
Health (H-ISAC)	With membership comprising patient care providers, health IT companies, pharmaceutical companies, medical device manufacturers, and labs, H-ISAC exists to maintain the continuity of the health sector against cyber and physical threats.
Information Technology (IT-ISAC)	Operating since 2001, IT-ISAC has provided a forum for members of the IT sector to continuously share high-volume indicators related to their sector.
MultiState (MS-ISAC)	The MS-ISAC provides resources for information sharing for the nation's state, local, tribal, and territorial governments focused on response to and recovery from security events.

Table 1-7 A List and Description of Several ISACs

Source: Chapman, B., & Maymí, F. (2020). *CompTIA CySA+™ Cybersecurity Analyst Certification All-in-One Exam Guide, Second Edition (Exam CS0-002)*, 28.