filename:comptia-secplussy0601-1-16-1-threat-intelligence-threat_maps_and_feeds
Showname: Security+ \(SY0-601\)
Topic: Threats, Attacks and Vulnerabilities
Episode: Threat Maps and Feeds
Learner Objectives:

Explain different threat actors, vectors, and intelligence sources.

Description: In this episode, the viewer will identify various components and attributes of threat feeds as well as threat feeds. The viewer will identify examples of threat maps as well as threat feeds.

---

* Mitigating Threats
* Threat Maps
    + Real time or near real-time map of various attacks around the globe
* Sources
    + Kaspersky's Threat Map
    + FireEye
    + Fortinet
* \(Dan - How are the maps builts\)
    + Retrieving data from numerous sources
* \(Dan - could you show us an example?\)
    + Kaspersky's Threat Map
        - On-access scans - detection based on copy, run, access operations
        - On-Demand Scan - detection based on user-based or manual scans
        - Web Anti-virus Scans - html pages opening, downloading files
        - Mail Antivirus Scans - when objects appear in emails
        - Intrusion Detection Scans - network detection activity
        - Vulnerability Scans - vulnerability detection scans
        - Botnet Activity Scans
        - Kaspersky's Anti-spam - unwanted/suspicious emails detected by Kaspersky's email filtering engine
* Threat Feeds
    + Real-time data streams of data providing information on potential cyber threats and risks
* Information Examples
    + Domains with poor reputation
    + Known Malware

    + IP addresses known for malicious activity
    + Machine readable data that can be feed into security information and event management \(SIEM systems\).
+ IoC - pieces of data that identify malicious activity
    + STIX and TAXII standardize IoC documentation and reporting
    + FireEye - Redline \(free IoC monitoring tools\) https://www.fireeye.com/services/freeware/redline.
    + Automated Indicator Sharing (AIS) enables the exchange of cyber threat indicators between the Federal Government, SLTT(State, Local, Tribal and Territorial) governments, and the private sector at machine speed.
* \(Dan - can we see some example of these Threat Feeds)
* Threat feed examples
    + DHS - AIS participants connect to a DHS-managed system in the Department’s National Cybersecurity and Communications Integration Center (NCCIC) that allows bidirectional sharing of cyber threat indicators.
    + FBI's Infragard.org
    + SANs Internet Storm Center
    + Cisco's Talos Intelligence

Cisco's Talos Intelligence: https://talosintelligence.com/
DHS AIS - https://www.cisa.gov/automated-indicator-sharing-ais
FBI's Infragard.org - https://www.infragard.org/
SANS Internet Storm - https://isc.sans.edu/