filename:comptia-secplussy0601-1-17-vulnerability_databases_and_feeds
Showname: Security+ \(SY0-601\)
Topic: Threats, Attacks and Vulnerabilities
Episode: Vulnerability Databases and Feeds
Learner Objectives:

Explain different threat actors, vectors, and intelligence sources.
Description:In this episode, the viewer will identify and be able to explain the purpose of vulnerability databases and vulnerability feeds.

---

* What are vulnerability databases?
    + A collection of information related to security flaws in information systems
    + Thousands of data sources
        - Software vendors
        - Software users
        - Researchers
* MITRE
    + MITRE ATT&CK \(Adversarial tactics, techniques and common knowledge) \(also adversary tactics, techniques, and procedures \(TTP\)\)
    + CVE \(Common Vulnerabilities and Exposures)
        - List of publicly known vulnerabilities
        - ID Number, description, one public reference
        - https://cve.mitre.org/
* National Vulnerability Database
    + US government repository of standards based vulnerability using SCAP
    + Security Content Automation Protocol
        - Enumerates software flaws and security configuration issues
        - Automated configuration
        - Patch and Vulnerability checking
        - Security compliance measurement scanning
* Additional SCAP Components
    + Common Configuration Enumeration \(CCE\)
        - CCE provides unique identifiers to system configuration issues in order to facilitate fast and accurate correlation of configuration data across multiple information sources and tools.
        - https://nvd.nist.gov/config/cce/index
        - https://nvd.nist.gov/config/cce
    + Common Platform Enumerations \(CPE\)

- Common Platform Enumeration (CPE) is a standardized method of describing and identifying classes of applications, operating systems, and hardware devices present among an enterprise's computing assets.
- identifying the presence of XYZ Visualizer Enterprise Suite could trigger a vulnerability management tool to check the system for known vulnerabilities in the software, and also trigger a configuration management tool to verify that the software is configured securely in accordance with the organization's policies.

+ NVD Threat Data Feed
- https://nvd.nist.gov/vuln/data-feeds

* US Computer Emergency Response Team \(US-CERT\)
- https://www.kb.cert.org/vuls/

* Threat Feeds
+ Mitre Threat Feed
- https://cve.mitre.org/cve/data_feeds.html
+ NVD Threat Feed
- https://nvd.nist.gov/vuln/data-feeds