CISA CSET Report VirusTotal, Alien Labs OTX and IBM X-Force Exchange

VirusTotal [1]

VirusTotal, an online virus scanning service that allows files, URLs, or IP addresses to be scanned across multiple antivirus engines. Users can quickly analyze potential threats and access threat data shared by the community. The primary benefit of VirusTotal is to help users protect their systems and data by quickly and accurately detecting malicious content.

- It is a community-based database where users can submit suspicious files contributing to collective security.
- It scans using more than 70 antivirus engines simultaneously.

Alien Labs Open Threat Exchange (OTX) [2]

A platform where security researchers can collaborate with the threat intelligence community. Users can share and access up-to-date information about malware, attack techniques, and other threats. This enables security experts to make faster and more informed decisions regarding threats.

- It's a collaborative platform facilitating the sharing of threat indicators among community members.
- Users can submit files and URLs for free malware analysis in Alien Labs' OTX sandbox.
- Utilizes community-sourced threat intelligence to identify potential threats on your devices by known threat indicators (IOCs).
- OTX threat data can be directly integrated into AlienVault and third-party security products via APIs and STIX/TAXII, keeping your threat detection defenses up to date.

IBM X-Force Exchange [3]

A platform where security experts can collaborate to protect against security threats. Users can analyze malware samples, obtain information about security vulnerabilities, and share threat intelligence. This accelerates organizations' detection and response times to threats and enhances overall security awareness.

- Represents a global community with open access provided to threat researchers and security professionals.
- Provides compatibility with other IBM Security solutions, unified security operations centers, and enhanced environmental awareness.
- Requires subscription fee

Choosing the Right Tool:

- **VirusTotal:** Ideal for quick threat checks and basic analysis.
- **OTX:** Best for security professionals and researchers seeking community collaboration and in-depth threat analysis.
- **X-Force Exchange:** Suitable for organizations requiring curated intelligence, expert insights, and collaboration tools (at a higher price point).

Each tool has its strengths and weaknesses, as well as similarities. They can be combined with other security research tools for a comprehensive defense strategy.

In summary, these tools provide security professionals with real-time threat intelligence, collaborative research, and the ability to be prepared for emerging threats. The most suitable one can be chosen based on the needs and resources of the organization.