IBM Security X-Force Advanced Threat Protection Feed

Machine-readable, actionable threat intelligence

Phishing operations emerged as the top pathway to compromise in 2021, with 41% of incidents X-Force remediated using this technique to gain initial access.[1] Although an organization may use external threat intelligence to enhance their security decision making, security teams often lack the critical support to make the most of these threat intelligence resources. Analysts can struggle to separate the signal from the noise, and threat data gathered from various sources can take too long to make actionable. A common challenge is the lack of reliable, actionable indicators to integrate with threat monitoring tools.

Highlights

- Helps monitor and protect against cyber threats
- Provides machine-readable, actionable indicators, including the DNS early warning feed
- Complements and integrates with existing security solutions and tools

Protecting your environment against cyber threats

IBM Security Advanced Threat Protection Feed by X-Force provides you with a list of machine-readable, actionable indicators curated by the IBM X-Force team that directly integrates with your existing security solutions and tools, such as firewalls, intrusion prevention systems (IPS) and security information and event management (SIEM) platforms. The feed provides access to:

- Domain Name Service (DNS) early warning indicators
- Analyst-derived indicators of compromise (IOCs)
- Actionable IOCs, such as IP addresses and HTTP URLs (command and control / botnet, malware, top traffic domains, threat policy categories)

[1] IBM Security X-Force Threat Intelligence Index 2022

Feeds are available in the following industry standard formats: STIX/TAXII, JSON, comma-separated values (CSV) and plain text.

DNS Early Warning: Malicious domains, blocked

The DNS early warning feed empowers an organization to act against undergoing and upcoming attacks faster by providing advanced information on hundreds of new, malicious domains surfaced daily through IBM's collaboration with Quad9. The feed is produced by IBM X-Force Research's *continuously delivering* threat analytics engine and is the result of IBM's real time DNS analytics applied to global DNS traffic. Early warning is effective at identifying malicious domains, both newly created and/or currently operational.

Quad9 is a recursive, anycast DNS platform that provides end users robust security protections, high-performance, and privacy. On average, it is blocking more than 220+ million malicious DNS requests every day[2]. IBM's X-Force threat intelligence contribution to this partnership helps to quickly identify and block malicious domains.

Analyst-derived high-fidelity indicators

IBM Security X-Force Threat Intelligence reports provide the latest threat intelligence indicators of compromise to block threat campaigns, malware, threat groups, and industry specific threats based on in-depth analysis by IBM's team of threat researchers working on incident response investigations. The Advanced Threat Protection Feed incorporates this indicator insight into its threat category feeds.

Summary

The Advanced Threat Protection Feed by X-Force offers powerful monitoring and protection capabilities by providing a list of machine-readable actionable indicators that can directly integrate with your existing threat management solutions. With the IBM Security QRadar Threat Intelligence app, available from the IBM Security App Exchange, we can provide seamless integration between IBM Security QRadar and the Advanced Threat Protection Feed.

---

[2] Quad9 https://quad9.net/

Why IBM?

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, provides security solutions to help organizations drive security into the fabric of their business so they can thrive in the face of uncertainty.

IBM operates one of the broadest and deepest security research, development and delivery organizations. Monitoring more than one trillion events per month in more than 130 countries, IBM holds over 3,000 security patents. To learn more, visit ibm.com/security.

For more information

To learn more about IBM Security X-Force Advanced Threat Protection Feed, please contact your IBM representative or IBM Business Partner, or visit the following website: ibm.com/products/xforce-exchange