Whitepaper

Using Threat Intelligence to Improve Your Security Posture

Publication date:

07. 30. 2024

Understanding threat intelligence and its importance

Threat intelligence is information about the potential and ongoing threats to an organization's information technology systems that is gathered, analyzed, curated and contextualized. It enables a proactive approach to cybersecurity by giving organizations the ability to prioritize, identify, assess and mitigate the risks posed by the cyber threats that are most likely to strike.

Curation and contextualization are especially important because it is where human expertise most comes into play. This is where the differences among various threat intelligence sources are the most impactful, and where defenders who rely on threat intelligence derive the most value.

For smaller- and medium-sized organizations especially, authoritative threat intelligence allows them to understand the threats that tend to target their specific industry, or the data they hold. This allows them to direct their resources for greatest defensive impact.

The ultimate goal of applying threat intelligence is to:

- Enable organizations to take proactive measures to prevent or mitigate cyber-attacks.
- Prioritize where to focus limited resources to mitigate the biggest risks.
- Assist with triaging events and reducing the damage from potential attacks.
- Minimize the overall negative impact once an organization is attacked.
- Respond effectively to security incidents.

Strategic threat intelligence identifies long-term broad trends and emerging threats, including how changes in geopolitical conditions, financial shifts, laws, technology and adversary motivations affect the cybersecurity landscape.

Tactical threat intelligence identifies the how and where of attacks. It provides timely, detailed, retrospective analysis of incidents including initial attack vectors as well as subsequent tactics such as privilege escalation, defensive evasion or lateral movement.

Operational threat intelligence primarily focuses on tracking adversary movements and understanding the techniques and procedures used during attacks. It identifies operational indicators of compromise (IOCs) that can include URLs, file hashes, malicious IPs, registry keys or network traffic patterns and protocols.

Technical threat intelligence helps to identify the what, so it focuses on the types of IOCs that occur during incidents. It can be applied to improving the ability to both detect and respond to incidents.

CONSIDER THE SOURCE

Threat intelligence is available from multiple sources, and most IT/security teams draw from several.

- **Industry feeds** are information-sharing platforms that bring together organizations in the same industry verticals and the security centers or analyst firms that serve them. They provide timely and relevant information on emerging threats, attack techniques and IOCs that are specific to an industry. Some industry feeds are paid, while others are free of charge.
- **Open-source intelligence** can come from public records, news articles, government websites, community forums, blogs and social media platforms that provide a wealth of information on cyber threats.
- **Peer-to-peer sharing** happens between organizations that face similar threats. They are similar businesses, within the same industry vertical or subset of an industry vertical, and are typically the same size with the same security capabilities.
- **Security-product vendors** provide intelligence as a part of their services, based on telemetry data gathered from their products in the field and curated by security analysts. They often provide summary reports for no charge, but deliver more timely reports and real-time actionable data feeds as an extension of their products and services.

THREAT INTELLIGENCE DELIVERY AND APPLICATION

Threat intelligence obtained from security-product vendors is most often applied in one of two forms: reports and feeds. The mix of reports and feeds varies by vendor; these are some typical examples.

Reports

Reports are in written form, typically in the form of monthly or other periodical updates, longer-form documents such as white papers, and occasional briefings or bulletins when late-breaking threats call for urgent updates.

- **Advanced persistent threat** (APT) reports deliver a mix of strategic, tactical, technical and operational intelligence that empowers organizations to improve their detection of threats and to become more proactive — or even predictive — about the specific threats they face or are likely to face. Knowing the threat actors, whom they're targeting and their IOCs give defenders the information needed to block them.
- **Malware** reports may be global or customer-specific and can include detection rules and details about the malware's operation.
- **Botnet** reports deliver data about identified variants of botnet malware and actionable data that includes the Command and Control (C&C) servers involved in botnet management.
- **Phishing reports** may be global or customer-specific and include details about current phishing campaigns that can include previews of the phishing email and location of servers involved.

Feeds

Feeds deliver intelligence in electronic form for automated ingest into security systems and consoles such as security information and event management (SIEM), security orchestration and response (SOAR) and extended detection and response (XDR) systems.

- Malicious files feeds provide information on newly discovered malware samples and the IOCs associated with them, as well as the information needed to detect, identify and block them.
- APT feeds typically focus on the IOCs associated with the various active APTs, similar to the APT report but delivered directly to the security consoles for taking the fastest-possible defensive action.
- Botnet feeds deliver intelligence about active botnets and the C&C servers associated with them, but may also include information about the organizations that are the likeliest targets.
- Domain, IP or URL feeds identify locations associated with botnets, phishing campaigns or currently active attacks; vendors may deliver one, two or all three so that the malicious site can be blocked at the most appropriate level.

ABOUT ESET THREAT INTELLIGENCE

ESET Threat Intelligence offers a view of the worldwide threat landscape based on unique telemetry. ESET feeds are drawn from a pool of more than 110 million sensors around the globe, processed through proprietary artificial intelligence-driven systems to extract the most relevant insights, then curated by a team of top security analysts who serve it in the most useful forms to drive immediate action. Unique to ESET are (1) a cloud-based system, LiveGrid, through which ESET endpoints submit and share suspicious samples and protective measures with our network of worldwide research labs and security centers, and (2) a proprietary, automated botnet tracking system that ensures the lowest number of false positives.

ESET research labs are widely recognized for tracking and reporting on the most notorious nation-state threat actors, botnet operators and ransomware gangs and sharing intimate knowledge of their tactics, techniques and procedures. This knowledge is translated directly into ESET Threat Intelligence delivered through immediately actionable reports and data feeds that customer organizations apply to proactively protect themselves.

welivesecurity

Some of the most significant findings of the ESET labs are reported publicly on ESET's award-winning blog, WeLiveSecurity.

LEARN MORE

About ESET

AI-NATIVE PREVENTION FOR TOMORROW'S THREATS

Stay one step ahead of known and emerging cyber threats with our **AI-native, prevention-first approach**. ESET combines the power of AI and human expertise to make protection easy and effective.

Developed over 30 years, ESET's best-in-class protection is powered by our **in-house global cyber threat intelligence**, including our **extensive R&D network** led by industry-acclaimed researchers.

ESET PROTECT, our scalable, cloud-first XDR cybersecurity platform combines next-gen prevention, detection and proactive threat-hunting capabilities with a wide range of security services, including **managed detection and response** (MDR). Our highly customizable, integration-ready solutions support all deployment methods, include local support and have minimal impact on performance. They identify and neutralize known and emerging threats before they can be executed, support business continuity, and reduce the cost of implementation and management.

Our mission isn't just to stop attacks in their tracks; it's to prevent them from ever happening. ESET protects your business so you can unlock the full potential of technology.

LEARN MORE

eset® Digital Security
Progress. Protected.