The Practical Applications of Threat Intelligence

accume partners

What is threat intelligence?

"Threat intelligence" is a commonly misunderstood security term. In general terms, it is information gathered from internal and external sources that is used to inform the organization about risks to their information systems and business operations. Information is gathered from external sources such as news articles, vendor and security organization alerts and technical publications. Internal sources can come from log files, security alerts and reports from your SEIM. Information gathered from these sources are analyzed for content and for possible risks, determining what actions, if any, need to be taken by the institution and its users. It is important to distinguish threat intelligence from alert response: threat intelligence is proactive analytical process around threats to the institution based on risk, whereas alert response is taking an action based on an alarm from one or more sources, and is purely reactive.

Bob Gaines, Director

646.375.9500 x114

rgaines@accumepartners.com

Situational awareness and the threat landscape

One of the primary functions of threat intelligence is to provide organizations situational awareness of the threats that are being detected around the world, and in their marketplace. It is important to know what types of attacks are trending, and what methods attackers are using to gain access to information systems. This type of situation awareness can provide enough lead time for institutions to prepare so that they know what security controls need to be modified, and how their processes need to change in order to properly respond to changes in the threat landscape.

User Information/Awareness

Another function of threat intelligence is to inform users of threats that they may encounter in their normal business functions. Users need to be aware of phishing campaigns, social engineering methods, and other attacks that present a risk to the institution, and they need to know important details such as what to look for, and how to respond to attacks when they are detected or suspected. Because employees are the weakest link in the security of any organization, an informed staff is a critical element in defending against attacks.

Firewall Controls

Firewalls are not designed to be static devices that protect your network from a fixed set of attacks. Firewalls are the primary form of protection against attacks from the internet, and are designed to be dynamic and flexible to the needs of the network it protects. Threat intelligence can provide technical details necessary to ensure that your firewall can protect against the latest threats. Items such as

malicious IP address to block (or look for), ports to modify, protocols to monitor, all ensure that the firewall can continue to provide the protections it was designed for. However, without monitoring and administration, it will remain a static device with a limited skillet to protect your most sensitive assets.

IDS/IPS

Intrusion detection and prevention systems have a dual purpose. They are an excellent source of internal threat intelligence, and they are a key control for modification based on external threat intelligence data. Internally, IDS/IPS systems alert you to activities that may be suspect, providing detailed information that administrators can use to make informed decisions about the health of the internal network as well as what security controls may need to be modified to add additional protections. Externally, IDS/IPS systems can be modified to detect the latest threats and be configured on how to properly react to them (deny, allow, alert, etc.) Several IDS/IPS systems also can dynamically update themselves based on external technical threat intelligence feeds, either from the vendor, or from open sources such as STIX or TAXII.

SIEM

Security information and event management (SIEM) systems are designed around the concept of threat intelligence. A SIEM (pronounced "sim" with a silent e) correlates alert and log information from multiple sources on the network to generate real-time analysis of security alerts by applications and network hardware. Security first responders are fond of SIEMs because you can use them to search for Indicators of Compromise (IoCs), such as IP addresses, port numbers and URLs that malware uses to communicate or propagate. The technical elements of external threat intelligence can be used search the network to ensure that no malware is present that can elude detection.

Indicator of compromise (IOC) — *in computer forensics is an artifact observed on a network or in an operating system that with high confidence indicates a computer intrusion. Typical IOCs are virus signatures and IP addresses, MD5 hashes of malware files or URLs or domain names of botnet command and control servers.*

Web Filtering

Web filtering is a critical security control for organizations, but it is often configured to accept or block websites based on their type (i.e. business, personal, banking, entertainment, etc.). When paired with threat intelligence, web content filtering becomes a more robust tool, able to block command and control access for malware, block known malicious sites, block data exfiltration and help integrate web filtering into a series of controls that can effectively block attacks even if another security control fails.

Servers and Workstations

Because servers and workstations house the type of data bad actors are looking for, they are under constant attack. Keeping them protected goes well beyond patching and configuration. Threat intelligence can provide the specific details necessary to configure workstations and servers against the latest advanced threats, and provide guidance about what controls your organization needs to have in the future. Supply chain management, vendor management, hardware selection and hardware/software lifecycles should all be informed (and strengthened) by threat intelligence.

Mobility

Smart phones and tablets have extended the perimeter of the business well beyond its physical walls. In today's corporate environment, most users have email access on either their personal systems or on a company-issued device. This represents a significant threat if mobile systems are not protected properly. Protection cannot rely on an initial device configuration or a management app that uses a static set of rules. 30% of new threats target mobile systems and their applications. Threat intelligence can inform organizations of new threats based on configurations, malicious applications, new methods of data interception and social engineering.

Operational intelligence is produced using automated processes, from data identification, log collection and correlation. A common example of operational threat intelligence is the automatic detection of distributed denial of service (DDoS) attacks, whereby a comparison between indicators of compromise (IOCs) and network telemetry is used to identify attacks much more quickly than a human analyst could.

Strategic intelligence is produced by identifying and analyzing threats to an organization's core assets, including employees, devices, applications, and vendors. An example of strategic intelligence is reading data from multiple information sources; identify trends; educate employees and customers; study attacker tactics, techniques, and procedures (TTPs); and make necessary modifications to security controls.

Home Users/Telecommuting/Travelers

Home users, telecommuters and travelers present a unique level of exposure to organizations. Working outside the perimeter of the organization exposes devices to attack and data to interception. In addition, the same methods employees use to work from home can be exploited by attackers to gain access to the internal network from remote locations. Threat intelligence lets administrators know what techniques attackers are using to access networks and how to detect and defeat them.

Putting it all together

Threat intelligence is more than just alerts from your systems and emails from security distribution lists. Threat intelligence is a process for the analysis of data from multiple sources to ensure that your information systems are protected from the most current attack types and methodologies. When utilized properly, it provides guidance for your IT staff so that controls currently in place can be strengthened, and guidance for your employees so that they are informed about the latest social engineering attacks. Accume partners advises every institution to develop a threat intelligence program and to subscribe to a threat intelligence service to be informed, aware and alert of attacks, threats and trends that can impact your organization.

Don't know where to start? Contact Accume Partners and we will get you on the proper path to a threat intelligence solution that works for you