WHITEPAPER

USING THREAT INTELLIGENCE TO PROTECT AGAINST CYBERATTACKS

How organizations can effectively incorporate threat intelligence into their cybersecurity strategies to protect against cyberattack.

888-435-7986 | www.getgds.com

GLOBAL DATA SYSTEMS

INTRODUCTION

Threat intelligence provides the actionable information organizations need to enhance their security strategies.

Traditional Security Tools

Most security tools are designed to detect and defend against specific types of cyberattacks. Firewalls allow only trusted traffic to flow through, while intrusion prevention systems examine data packets and drop those that appear to be malicious. Antimalware solutions look for malicious software and take steps to prevent it from causing damage to systems.

These tools are very effective at combatting known threats. But as Gartner noted in a recent report, "leading indicators of risk to an organization are difficult to identify when the organization's adversaries, including their thoughts, capabilities and actions, are unknown." That's why **advanced persistent threats (APTs) and zero-day exploits are so hard to detect using traditional security tools.**

Threat Intelligence

Typically, however, there are clues. The challenge lies in uncovering those clues and using them to predict how and when a cyberattack might take place. That's the role of threat intelligence. **Gartner defines threat intelligence as "evidence-based knowledge**, including context, mechanisms, indicators, implications and actionable advice about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard." In other words, **threat intelligence tells organizations what tactics are being used, what systems or data are being targeted and the level of risk associated with the threat.** Armed with this information, IT teams can take appropriate action to prevent or at least minimize the damage to the organization.

To be successful, threat intelligence should focus not on gathering data but on ensuring that it is relevant and actionable.

What You'll Learn

This whitepaper will explain **how organizations can effectively incorporate threat intelligence** into their cybersecurity strategies to protect against cyberattack.

What Is Threat Intelligence?

The term "intelligence" is frequently used in a military context. It refers to the gathering and assessment of data about the enemy's size, movements and capabilities so that leaders can develop the best offensive or defensive strategy. Assessment is key.

The FBI has defined intelligence as "information that has been analyzed and refined so that it is useful to policymakers in making decisions — specifically, decisions about potential threats to our national security."

The same definition could be used for threat intelligence by substituting "policymakers" with "IT security professionals" and "national" with "organizational." **Threat intelligence isn't raw, unfiltered data but information that has been evaluated in the proper context. It is accurate, current and actionable, enabling security teams to respond to threats quickly and effectively.**

Threat intelligence can be internal or external.

Internal threat intelligence uses data gathered from security devices and systems within an organization. Security information and event management (SIEM), log management, risk management and incident forensics are some of the tools used for internal threat intelligence.

External threat intelligence uses data from sources outside an organization. Many organizations subscribe to data feeds, including free services from the SANS Internet Storm Center, the U.S. Computer Emergency Response Team (CERT) and some IT vendors. There are also fee-based services that aggregate and correlate multiple data feeds and provide customer-specific alerts. Other sources of external threat intelligence include crowdsourced platforms and information from industry groups, government and law enforcement.

Gartner divides threat intelligence tools into two broad types.

Tactical threat intelligence includes system and network-level indicators that humans and machines use to detect and respond to attacks. **Strategic threat intelligence** includes higher-level reports on cybercriminals, their capabilities and activities that humans use for planning and decision-making.

BENEFITS AND CHALLENGES

> **According a recent report from Technavio, the global threat intelligence market should see a compound annual growth rate of more than 19 percent through 2022.**

Demand for threat intelligence solutions is being driven by increasing numbers of cyberattacks and the diversity and volume of threat data. But can threat intelligence improve an organization's security posture?

For its recent study, "The Value of Threat Intelligence," the Ponemon Institute surveyed more than a thousand IT and security professionals in North America and the United Kingdom whose organizations use threat intelligence as part of their security program. **Eighty-six percent said threat intelligence is valuable to their organization's security mission and 84 percent said it's essential to a strong security posture.**

Almost two-thirds (63 percent) said that threat intelligence helps drive security decision-making, and slightly more than half (51 percent) said they use threat intelligence in incident response. However, just 41 percent rated their organization's ability to use threat intelligence as highly effective. The key challenges organizations face include a lack of expertise (cited by 71 percent of respondents), lack of ownership (52 percent), a lack of suitable technologies (48 percent) and unreliable or insufficient threat data 45 percent).

The volume and complexity of threat intelligence data is also a problem for 69 percent of organizations. In addition, 64 percent of organizations are struggling to integrate threat intelligence with other security tools, and 52 percent say threat analysis is not aligned with security operational processes.

86% say

THREAT INTELLIGENCE is VALUABLE to their SECURITY

41% say

THEY ARE USING THREAT INTELLIGENCE EFFECTIVELY

Maximizing the Value of Threat Intelligence

Those challenges should not dissuade organizations from adopting threat intelligence solutions.

Done right, **threat intelligence provides greater visibility of attacks** in context, and **improves accuracy and speed in detecting and responding** to attacks. It also enables organizations to fine-tune their security policies and strategies to address evolving threats. **Effective threat intelligence begins with comprehensive data collection.**

External feeds should include data from as many sources as possible, and the data should be analyzed by experienced security professionals who draw conclusions about the risk posed by detected threats and what steps should be taken to minimize their impact.

However, external data is not enough. External feeds should be combined with data collected from across the extended enterprise and integrated with the organization's security systems to gain the context needed for analysis.

Advanced Analytics

Advanced analytics are then applied to the contextual data to detect threats in real time. **Behavioral modeling** is used to identify known bad behavior such as scanning and brute-force login attempts, and to compare network activity against a baseline of normal behavior. **Machine learning** is used to correlate suspicious behavior seen locally, within the enterprise, with threat activity seen globally. This enables threat intelligence tools to detect unknown threats and provide alerts with a high level of confidence. This **context-rich intelligence should be tightly integrated with an organization's security tools and incident response procedures.** When threats are detected, security tools can take action automatically or provide in-house IT teams with the insight they need to rapidly contain and mitigate the attack. Sharing threat intelligence across multiple security systems also makes it possible to detect today's multi-vector exploits. For example, many attacks begin with a phishing email that contains a malicious link or attachment that launches malware that is capable of evading traditional defenses. **Threat intelligence "connects the dots" between the distribution of threat content and observations of malicious activity.**

What Is Incident Response?

Incident response refers to the process of addressing a cyberattack in order to minimize downtime, damage and costs. Incident response begins with proper preparation and planning, so that key personnel know the procedures they should follow when a security breach occurs. The plan should define what constitutes an "incident," which might include data exfiltration, unauthorized access, malware infection, denial of service attack and other security-related events. Once a threat has been identified, the response team will likely need to conduct an investigation in order to understand what they are dealing with. Only then can they work to contain and eradicate the problem and recover systems, applications and data. The response team should also assess the incident and how it was addressed, and look for ways to improve the process.

CONCLUSION

There are many security solutions on the market that are able to identify known cyberattack signatures. However, APTs, zero-day exploits and sophisticated malware don't offer many clues to their existence. **Organizations need to collect and analyze from logs, system reports, security feeds and alerts, and other internal and external sources in order to detect today's threats.**

Best-in-class threat intelligence solutions aggregate data from devices around the world and evaluate it using data analytics, machine learning and human research.

The result is actionable intelligence that organizations can leverage to increase the effectiveness of their security tools. It closes security gaps and helps IT teams respond more quickly and effectively to cyberattacks.

GLOBAL DATA SYSTEMS

Protect Your Organization Against Cyberattacks

Contact Global Data Systems: 888-435-7986