WHITEPAPER

IMPROVING THREAT DETECTION & RESPONSE BEFORE, DURING & AFTER A CYBERATTACK

How Continuous Monitoring and Analysis Enhances a Layered Security Approach

888-435-7986 | www.getgds.com

GLOBAL DATA SYSTEMS

INTRODUCTION

> Experts have long recommended a layered approach to cybersecurity that combines multiple security measures to detect and block threats.

However, attackers are employing increasingly stealthy techniques that are capable of sneaking past the best defenses. That's why it's critical to continuously monitor the network and systems for malicious activity, and to analyze files that have been allowed to enter the network for evidence of possible malware.

Continuous Monitoring Tools Can Help You Protect Yourself Against Attackers

Continuous monitoring tools can alert IT teams when they detect indicators of compromise. IT can then leverage threat intelligence and sandboxing to determine the nature of the attack and the potential threat to the environment.

These tools can also aid in effective security incident response by tracking system activity and the movement of files. IT can quickly contain the attack and determine the root cause. Remediation activities can be identified and prioritized, and defenses improved to prevent a similar attack.

A Look at the Layered Approach

The layered approach to security acknowledges that many cyberattacks use multiple techniques to infiltrate systems and networks.

An attack may begin with a phishing email that distributes malware and steals user credentials. The attackers may then use those credentials to gain access to the victim's computer, moving laterally through the network to gain higher-level credentials and ultimately exfiltrate sensitive corporate data.

Organizations Need a Blend of Security Measures

In order to combat blended threats and targeted attacks, organizations need a blend of best-of-breed security measures. A layered approach synchronizes those tools to create a whole that is many times stronger than the sum of its individual parts.

A core component of the layered approach is perimeter defense, which involves keeping malicious traffic from ever entering the network. Perimeter defense begins with a firewall, which forms a barrier between two or more networks and controls what data can pass through.

Hunting For Suspicious Activity

Intrusion detection systems supplement firewalls by hunting for suspicious activity and alerting administrators when they find it. Intrusion prevention tools go a step further by actively blocking attacks. These tools sit outside the network perimeter, in front of the edge router, analyzing and capturing suspicious packets.

Modern antimalware software uses "signatures" to block known malware, and static and dynamic file analysis to detect emerging threats. Active content filtering tools should also be used to block websites that could compromise security, and to prevent the unauthorized distribution of sensitive information.

Encryption is another important element of layered security. Strong encryption algorithms combined with encryption keys that are regularly rotated protect data at rest and in transit from potential compromise.

These Tools Are Essential to Effective Cybersecurity

All of these tools are essential to effective cybersecurity. However, they focus primarily on prevention and do little to defend against stealth malware and other threats that are able to get past these defenses.

Continuous Monitoring: Beyond Prevention

If it were possible to detect and block every threat, no organization would not fall victim to a security breach. However, many of today's threats offer few clues to their existence.

For example, 97 percent of malware uses polymorphic techniques that change characteristics for each target, rendering traditional indicators of compromise virtually useless. File-less malware uses tiny but malicious PowerShell scripts that are stored in memory or in the system registry, leaving no files or artifacts to be detected by traditional signature-based security tools.

Continually Monitoring Your Network is Critical

That's why it's critical to continually monitor and analyze network, system and file activity to detect possible threats that may have gotten past perimeter defenses. Even attacks that use sophisticated evasion techniques will ultimately take action to execute their malicious purpose. Continuous monitoring should be combined with threat intelligence to detect indicators of compromise, determine what part of the IT infrastructure is at risk, identify delivery mechanisms, and determine who the actors are and their motivation for attack.

Sandboxing is another essential component of threat detection. Network traffic is sent to a tightly controlled environment, or sandbox, where untrusted or unverified files and URLs are "detonated" without causing damage to the environment. Malware analysis is automatically performed, and cybersecurity personnel are provided with detailed information on any indicators of compromise. Sandboxing makes it possible to discover previously unknown, undocumented malware, including zero-day threats, and to assess the source of the threat, attack method and the potential impact of a breach.

Unlocking the Value 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." It combines data from logs, system reports, security feeds and alerts, and other internal and external sources, with processes and tools for gathering and analyzing that data. However, generic information without context will be of little value.

Best-in-class threat intelligence solutions incorporate both automated tools and human research to help security teams understand and effectively respond to threats.

Why Incident Response Is Critical

According to the 2018 Cost of a Data Breach Study conducted by the Ponemon Institute, the average cost of a data breach is $3.62 million, with an average cost per lost or stolen record of $148. Organizations with an incident response plan in place saw an average cost savings of $14 per record, or almost 10 percent, because they were able to respond more quickly and effectively.

As in previous studies, the Ponemon Institute found that the cost of a breach is directly related to the time required to identify and contain the breach. The mean time to identify a breach was 197 days and the mean time to contain a breach was 69 days.

Organizations that were able to contain a breach in less than 30 days saved more than $1 million compared to those that took longer.

RESPONDING TO SECURITY INCIDENTS

> **According to the Verizon 2018 Data Breach Investigations Report, there were more than 53,000 security incidents and 2,216 confirmed data breaches in 2017.**

External threat actors were responsible for 73 percent of these incidents, with financial gain the primary motive. Inside threats were responsible for the other 27 percent, including both malicious and careless or inadvertent actions.

Security Incidents

A security incident is any indication of attempted or imminent compromise of an organization's systems or data, even if unsuccessful. If a threat makes it past the organization's defenses, a security incident has occurred. That's why continual monitoring and analysis must be paired with incident response procedures and systems.

Incident Response

Incident response refers to the process of addressing a cyberattack in order to minimize downtime, damage and costs. According to the SANS Institute, incident response begins with proper preparation and planning, so that key personnel know the procedures they should follow. The incident response 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.

73% of security incidents

HAD FINANCIAL GAIN AS THE PRIMARY MOTIVE

Incidents should be categorized based upon the type of data involved, the type of perpetrator responsible, the scope of the event, and any legal or regulatory compliance requirements involved. Once a potential incident has been identified, the response team will likely need to conduct an investigation in order to understand what type of event they are dealing with. The initial investigation should be conducted as rapidly as possible in a way that preserves evidence.

The IT team can then work to contain and eradicate the problem and recover systems, applications and data. As a final step, the response team should assess the incident and how it was addressed, and look for ways to improve the process.

The Role of Continuous Monitoring in Incident Response

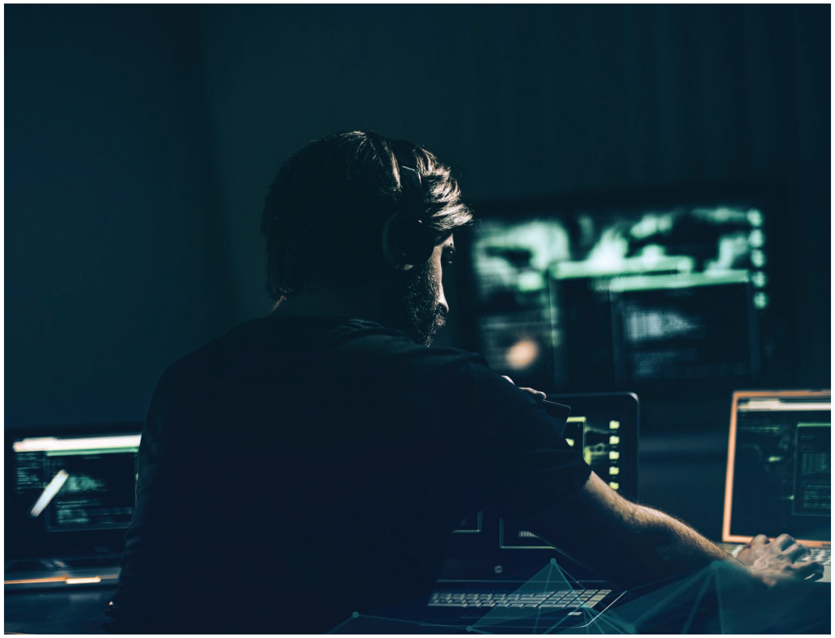
The continuous monitoring and analysis tools used for threat detection can be invaluable in incident response. Alerting systems not only warn IT teams of a detected threat but provide detailed information on the actions that the threat has taken.

Best-of-breed tool are capable of tracking the trajectory of malicious files across the environment, enabling IT to quickly quarantine any affected systems and block the threat from propagating further across the environment. IT can then analyze the affected systems to determine the root cause of the attack and develop an appropriate response.

Visibility into system activity provides insight into the objective of the attack. Security analysts may look at any files that were downloaded, websites that were visited, changes to the system registry and outbound connections to remote systems. This enables them to determine if the attack may still be present and the potential risk to the environment.

Continuous Monitoring Tools Can Help

Finally, continuous monitoring tools can help IT teams understand how the attack was able to get past the organization's defenses. For example, was malware distributed via a phishing email or did the attacker use stolen credentials or brute force methods to gain access to the affected systems? By answering these kinds of questions, these tools can help IT shore up the organization's defenses and prevent a similar attack.



CONCLUSION

Obviously, **organizations should do everything they can to prevent a cyberattack.** They should implement a layered security approach that incorporates next-generation firewall and intrusion prevention solutions, content filtering, advanced malware detection and robust encryption. However, organizations must also take steps to detect threats that are able to sneak through these defenses.

Continuous monitoring and analysis of network, system and file activity, coupled with threat intelligence and sandboxing, helps to protect the environment during and after an attack.

Cybersecurity personnel are alerted of suspicious activity so that they can analyze the nature and extent of the threat. In the event of a security incident, **these tools give IT teams the visibility and contextual insight they need to quickly isolate the threat,** determine the root cause, and develop and execute a remediation plan.

GDS can help you protect against cyberattacks
Contact Global Data Systems: 888-435-7986