Initial post

◄ Initial Post

Initial Post ►

Display replies in nested form

Settings

Initial post

by Samer Saleem - Wednesday, 22 May 2024, 8:33 PM

It is a fact that logging is the main factor in detecting and monitoring events and errors in our networks and systems, Security monitoring is central to the identification and detection of threats to your IT systems. It acts as your eyes and ears when detecting and recovering from security incidents and enables you to ensure that devices are used per your organizational policies.

Effective monitoring relies on proportionate, reliable logging and device management practices. This guidance is designed to advise system and network admins on the logging and monitoring options available on modern platforms, if an organization has the resources available, one solution is to establish a security operation center (SOC). This will help you manage and monitor security risks to your organization generally.(NCSC, 2021)

Since logging is the main source for monitoring, this imposes a different kind of challenges, some of which are related to the fact that devices and systems and operating systems might vary in a network, which means logging and reading the logs will be difficult due to the different source platforms used to generate these logs, While Syslog offers numerous benefits for network management and troubleshooting, it has some limitations that administrators should be aware of. The protocol lacks authentication mechanisms, making it vulnerable to playback attacks. Moreover, Syslog relies on UDP transport, which may result in lost messages, and its inconsistent formatting can pose challenges in log data analysis.

Despite these limitations, Syslog remains a valuable tool for network monitoring, especially when integrated with other monitoring tools and configured with best practices in device security and authentication. (Sliceup, 2024)

These challenges could be overcome by using Processes to aggregate these disparate logs and trigger alerts when particular events occur are often automated today. (Ekelhart et al, 2019)

One solution might be using Log Analyzers to help humans understand and correlate events in a better and more efficient way, example: FortiAnalyzer is a powerful log management, analytics, and reporting platform that provides organizations with a single console to manage, automate, orchestrate, and respond, enabling simplified security operations, proactive identification and remediation of risks, and complete visibility of the entire attack landscape. Integrated with the Fortinet Security Fabric, FortiAnalyzer enables Network and Security Operations Teams with real-time detection capabilities, centralized security analytics, and end-to-end security posture awareness to help analysts identify advanced persistent threats (APTs) and mitigate risks before a breach can occur. (Fortinet, 2024)

References:

NCSC (2021) Managing deployed devices: Logging and protective monitoring. Available at: https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/logging-and-protective-monitoring (Accessed: 22 May 2024).

Sliceup (2024) What is Syslog?. Available at: https://www.sliceup.co/post/what-is-syslog#:~:text=However%2C%20it's%20important%20to%20note,its%20reliance%20on%20UDP%20transport (Accessed: 22 May 2024).

Ekelhart, A., Fenz, S., and Neubauer, T. (2019) 'Taming the logs - Vocabularies for semantic security analysis', International Journal of Information Security, 18(2), pp. 129-145.

Fortinet (2024) FortiAnalyzer. Available at: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortianalyzer.pdf (Accessed: 22 May 2024).

Permalink Reply

Re: Initial post

by Samer Saleem - Wednesday, 22 May 2024, 10:04 PM

Since logging is important part of having a healthy and safe monitoring environment, we should never ignore the fact that logging is also a service that might be impacted by breach or can have a vulnerabilities as other systems do.
Log4j is an example of how logging can be target, in which a vulnerability was found in Log4j, an open-source logging library commonly used by apps and services across the internet. If left unfixed, attackers can break into systems, steal passwords and logins, extract data, and infect networks with malicious software.(NCSC, 2021)
Log4j runs across many platforms — Windows, Linux, Apple's macOS, Cisco, AWS, IBM...etc. — and is present in hundreds of millions of devices. (Ojasvi Nath, 2022)

Reference:

NCSC (2021) Log4j vulnerability - what everyone needs to know.https://www.ncsc.gov.uk/information/log4j-vulnerability-what-everyone-needs-to-know#:~:text=What's%20the%20issue%3F,infect%20networks%20with%20malicious%20software. (accessed: 22 May 2024)

Nath, O. (2022) Log4j Flaw: Top 10 Affected Vendors and Best Solutions to Mitigate Exploitations. Available at: https://www.spiceworks.com/it-security/vulnerability-management/articles/log4j-flaw-top-10-affected-vendors-and-best-solutions-to-mitigate-exploitations/ (Accessed: 22 May 2024).

Permalink Show parent Reply

Re: Initial post

by Oi Lam Siu - Friday, 31 May 2024, 3:25 AM

Peer Response

Hi Samer,

Thank you for your detailed post on the importance of logging in network and security management. Your insights into the role of security monitoring and the challenges posed by varied systems are very informative. I appreciate your suggestion of using FortiAnalyzer for comprehensive log management and security analytics. This is indeed a powerful tool to centralize and streamline logging efforts.

In addition to your suggestions, I would like to propose a couple of additional strategies to further mitigate risks like the Log4j vulnerability:

1. Regular Updates and Patch Management:
Ensuring that all logging libraries, including Log4j, are kept up-to-date with the latest patches can significantly reduce the risk of exploitation. Automated patch management tools can help maintain this consistency.

2. Implementing Input Validation and Sanitization:
By enforcing strict input validation and sanitization, we can prevent malicious data from being logged, thus minimizing the risk of code injection attacks.

These additional measures, combined with your proposed solutions, can help create a more secure and resilient logging infrastructure.

Best,
Helen

Reference:

NIST. (2022) Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology. DOI: https://doi.org/10.6028/NIST.SP.800-40r4

OWASP Top10. (2021) OWASP Top 10 - 2021. Available from: https://owasp.org/Top10/ [Accessed 14 May 2024]

Maximum rating: -

Permalink **Show parent** **Reply**

◄ Initial Post **Initial Post ►**