T2022_12 Why should you Implement a SIEM solution on your network (20th June 2022)

What is A SIEM

SIEM is an acronym that stands for security, information, and event management. SIEM technology combines log data, security alerts, and events into a centralized platform to provide real-time security monitoring analysis. SIEM software helps organizations improve visibility across their environments, investigate log data for incident response to cyberattacks and data breaches, and meet local and federal compliance mandates.

How can it help your organization

SIEM active monitoring solutions deployed across your entire infrastructure significantly reduce the time required to detect and respond to potential network threats and vulnerabilities, assisting in strengthening security posture as the organization grows.

How Does it Work?

SIEM software collects log and event data generated by applications, devices, networks, infrastructure, and systems to perform analysis and provide a comprehensive view of an organization's information technology (IT).

SIEMs can be deployed on premises or in the cloud. SIEM solutions use rules and statistical correlations to drive actionable insight during forensic investigations by analyzing all data in real-time. SIEM technology examines all data, categorizing threat activity based on its risk level to assist security teams in quickly identifying malicious actors and mitigating cyberattacks.

Benefits of SIEM Technology

SIEM components can provide a wide range of benefits including:

- Real-time visibility throughout the environment
- Solution for centralized management of disparate systems and log data
- Reduced false positive alerts.

- Decreased mean time to detect (MTTD) and mean time to respond (MTTR) (MTTR)
- Data collection and normalization to allow for accurate and reliable analysis
- Ability to map operations with existing frameworks such as MITRE ATT&CK for ease of access and searching across raw and parsed data
- With real-time visibility and pre-built compliance modules, you can ensure compliance adherence.
- Dashboard customization and effective reporting

References

- Gast, K. (2022, April 29). *What is SIEM? And How Does it Work?* Reviewed from LogRhythm. https://logrhythm.com/blog/what-is-siem/

- Miller, J. (2022). *Essential Guide to SIEM Implementation and Optimization*. Retrieved from Bitlyft. https://www.bitlyft.com/resources/essential-guide-to-siem-implementation-and-optimization

- Rosencrance, L. (2020, February 7). *security information and event management (SIEM)*. Retrieved from SearchSecurity. https://www.techtarget.com/searchsecurity/definition/security-information-and-event-management-SIEM

- *What is Security Information and Event Management (SIEM)? | IBM*. (2022). Retrieved from IBM. https://www.ibm.com/topics/siem#:%7E:text=SIEM%20active%20monitoring%20solutions%20across,posture%20as%20the%20organization%20scales.