Thank you, Kingsley, for your informative post about the new security technology. In the raise of using cloud-based systems, SIEM has become a greater focus on risk-based alerts. Substantially reduces the time it takes to discover risks, therefore decreasing the harm caused by such threats. Besides of high budget, there are a few dependents and limitations on SIEM that need to be aware of.

SIEM analysis is based on the collected log to provide threat intelligence, in other words, it is dependent on the log integrity and accuracy. For the organization having a customized application, integrating custom logs required additional correlation rules and consume time for the developer or CIO to review. Follow the best practices to collect security log data efficiently, excluding log data pertaining to tune out the noise and reduce false alerts (N-able, 2020). On the other hand, it would be much quicker and easier if organizations integrating with well-known or cloud services like Office 365, Cisco ASA, Okta, etc. The time difference could be reduced from 3-6 months to under 5 hours (Thu, 2020).

SIEM is alerting system to address the threat, the plan of response and reaction is important. SIEM could not be a suitable match for every environment and determining the right solution for the organization is a challenging task.

References:

N-able (March 2, 2020) SIEM Logging Best Practices. *Security.* Available from: https://www.n-able.com/blog/siem-logging-best-practices [Accessed 25 September 2021].

Thu, P. (July 14, 2020) Is Your SIEM Deployment Failing? The Hidden Costs of SIEMs. *Security Framework*. Available from: https://www.blumira.com/hidden-costs-siem-splunk-blumira/ [Accessed 25 September 2021].

<https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=275728>

Kingsley Onyeemeosi