Add Predictability to Long-Term Cybersecurity with the Right Solutions

Kynan Carver
Cybersecurity Lead, Defense Market
Maximus

Many of the technologies used to improve the security and efficiency of enterprises are also being used to attack them. Hackers are deploying machine learning and automation to increase the frequency and scope of cyberattacks, which requires agency leaders to continuously update their security posture. Essential and well-known functions for this are security information and event management (SIEM) and security orchestration, automation, and response (SOAR). What's less known is the differences among the many SIEM and SOAR products. Criteria to evaluate SIEM products include licensing costs, how much data they process, their alert features, and how easy they are to use. For SOAR products, considerations include how well they integrate with SIEM and existing systems, their support in cloud, multi-cloud, and on-prem environments, and also the ease of use. This session will inform attendees about the importance of SIEM and SOAR in a composable security infrastructure, and what to consider in a selection process, including having a common data format. As a technology agnostic systems integrator, Maximus can offer a valuable point of view on these tools and where they fit in a composable security enterprise.