Take your SIEM to the next level

SIEM (security and information event management) solutions collect data from sources generating log data, which is indexed and stored in a log repository. While they can be effective, they are running into hard limitations, including:

- **Alert fatigue:** SIEMs generate large numbers of false positives, false negatives, or low-priority events, making it difficult to identify genuine threats.

- **Lack of context:** Security rules and signatures provide limited context on security alerts, making it challenging to stay ahead of a complex, dynamic threat environment.

- **Incomplete data collection:** SIEMs often have compatibility issues, plus limitations in log sources and network configurations.

- **Storage limitations:** Storage costs and data retention policies result in incomplete log data for analysis.

- **Complex configuration and maintenance:** Setting up and maintaining a SIEM is complex, requiring expertise in configuring log sources and creating correlation rules.

- **Inability to handle large-scale data:** Big data volume and velocity lead to slow response times and delays in processing/analyzing data, missing time-sensitive events.

- **Limited threat intelligence integration:** While SIEMs incorporate threat intelligence feeds, their integration and updating processes with other security elements may not be seamless, leading to outdated or ineffective threat intelligence.

- **Difficulty in identifying advanced threats:** SIEMs focus on known patterns and signatures, but struggle to quickly identify sophisticated and evolving threats not matching predefined rules.

- **Poor scalability:** A lack of scalability impacts increasing data volumes, additional log sources, or distributed networks, and limits views of past events or potential risks.

- **Limited automation and response capabilities:** A lack of robust automation and response features against complex correlation requirements limits monitoring/threat detection in cloud environments, requiring manual investigation and responses to alerts.

There is a need for a more forward-leaning approach to stay ahead in the modern threat landscape while maximizing the value of SIEM investments. This requires thinking along three vectors:

Actioned Visibility

Take immediate action across security telemetry and supply chains to address potential threats. This requires visibility beyond the scope of traditional SIEMs by including threat/attacker insights augmented with curated and peer intel, delivering context beyond current SIEM storage limitations. This reduces cycle times from weeks to minutes.

Optimized Cyber Stack

Understand risk exposure, prioritize investments, and share intelligence to security controls to identify attacker TTPs and prevent breaches. Most stand-alone security solutions are not fully integrated with external resources such as ISACs or MITRE ATT&CK. Anomali integrates dynamic data sources into an actionable framework, turning analysts into a force multiplier.

Automated SecOps

Events come in at high volume, and security analyst burnout is pervasive. Implementing AI-supported workflows automates routine tasks such as intelligence analysis, trigger investigations, security gap identification, and security posture updates. Using Anomali, analysts are able to separate signal from noise, handle threat detection with precision and context, and reduce the stress associated with unsustainable workloads.

For further information on how Anomali's Security Analytics Platform can take your SIEM to the next level, please click here.