SIEM Tools Best Practices Unlock Powerful Cyber Security Capabilities

SIEM tools (Security Information and Event Management) provide an effective way for organizations to both achieve regulatory compliance and respond swiftly to security threats. Because they can collect, analyze, and correlate security data from various sources in real time, they provide critical visibility. But choosing the right SIEM solution and deploying it properly requires a substantial learning curve.

Security teams should understand both the challenges and best practices involved with implementing SIEM tools. With this knowledge, they can then implement SIEM as an essential part of a larger cyber security strategy.

SIEM Use Cases

Depending on how the organization configures its SIEM solution, the tools can accomplish several important tasks. For example, using predefined or custom rules, SIEM tools can detect violations of security and compliance policies. This might include alerting security personnel to unauthorized access of protected health information or changes to financial data.

SIEM tools also help the organization demonstrate regulatory compliance by providing dashboards and reports as evidence of security measures taken. Compliance reports provide a detailed analysis of any compliance violations detected. This includes the specific events that triggered the alert, the root causes, the impacts, and the evidence collected.

Similarly, SIEM tools play a critical role in incident response. In the case of ransomware, for instance, the tools may provide an early warning of the attack. They can then automate incident response actions such as isolating infected hosts. And they provide investigation tools to help forensics drill down into details of an event and trace its root cause.

Common SIEM Challenges

While properly configured SIEM tools deliver significant benefits, the technology does come with some risks. One common challenge involves alert fatigue. With potentially thousands of devices and events triggering alerts, the security team may receive many false alarms. When this happens, real problems may get buried or ignored.

Additionally, SIEM tools depend on quality data to develop a baseline from which to determine anomalies. Log files from corrupted endpoints will deliver inaccurate data and skew the baseline, reducing the effectiveness of the tool.

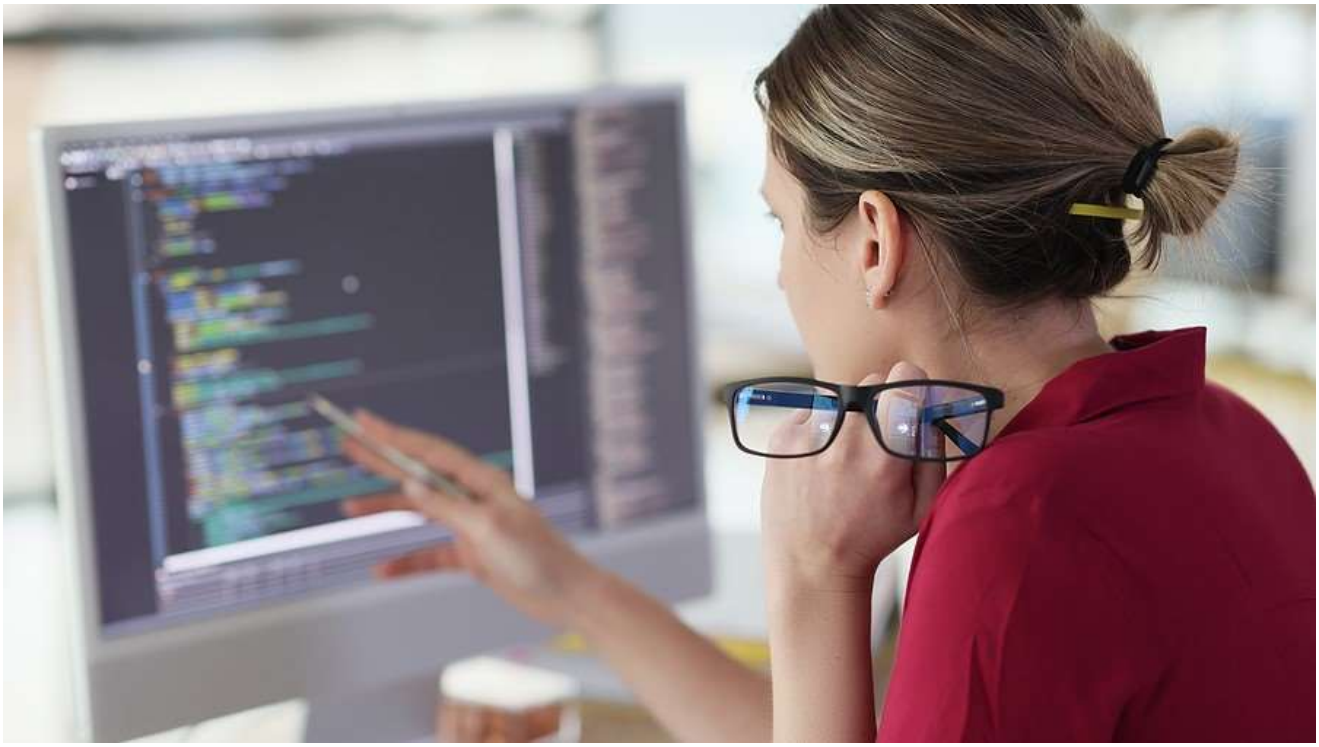
Finally, SIEM tools can prove expensive and complex to deploy and maintain. They require specially trained personnel, as well as sufficient storage space and bandwidth to handle the volume and variety of data ingested.

Best Practices for SIEM Implementation

Several best practices will help organizations meet these challenges and get the most value out of their SIEM solution.

- **Continually fine-tune the SIEM configuration** – When it comes to SIEM data and alerts, choose quality over quantity. This will involve prioritizing the most critical sources of data and carefully defining SIEM rules and alerts to match your specific threat landscape.
- **Pair automated SIEM technology with expert review** – Even with highly-automated SIEM technology, a human expert should provide "eyes on" analysis and incident response guidance. This combination of technology and human expertise will help ensure proper remediation of events.

- **Choose SIEM solution carefully** – When researching SIEM solutions, consider the size and complexity of your IT environment. SIEM tools will need to integrate with existing tools and platforms. Also look at the types and sources of security data to collect, as well as the level of customization and scalability required.



- **Improve SIEM effectiveness with supporting technology** – By integrating SIEM tools with related technologies, the organization greatly enhances its security posture. For instance, integrating SIEM with security orchestration, automation, and response (SOAR) technology allows the security team to streamline incident response processes.
- **Consider using managed services** – Managed services can help reduce costs and complexity. By implementing an option such as eCare SOC from eMazzanti, organizations benefit from 24x7 monitoring and the assistance of trained cyber security experts.

SIEM Tools as Part of a Comprehensive Security Strategy

By themselves, SIEM tools will not fully protect against cyber threats and ensure regulatory compliance. However, they play an essential part in an overall security strategy. Contact the cyber security experts at eMazzanti to learn more about SIEM solutions and related technologies.