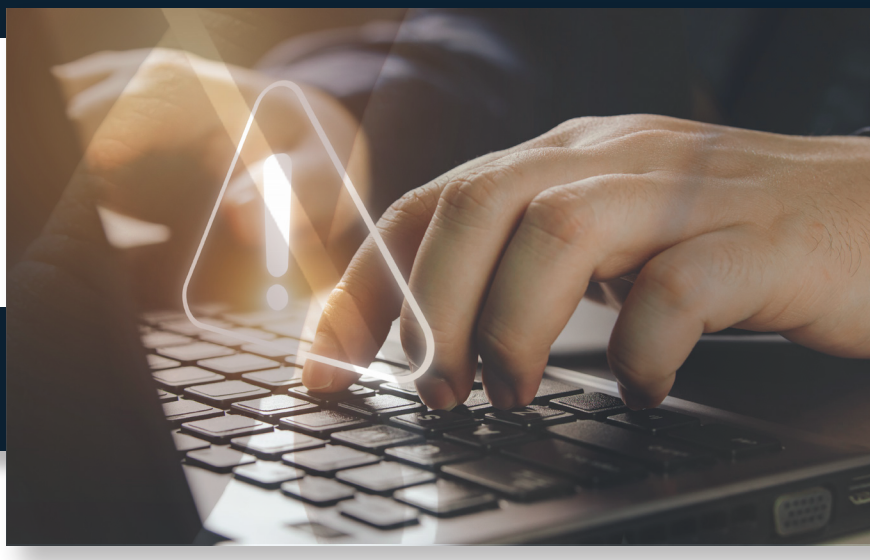
5 MUST-KNOW SIEM QUESTIONS ANSWERED

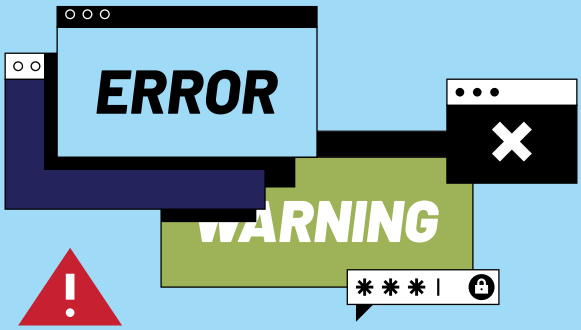
SIEM 101: Frequently Asked Questions



1 **What Does SIEM Stand for?**
SIEM = Security Information and Event Management

2 **What Is a SIEM?**
A SIEM is a 24/7/365 intelligent threat detection system. It collects logs and analyzes threat alerts across your network, so critical alerts get immediate remediation before they can cause serious harm to your business.

3 **Why Is a SIEM Important?**
Compliance: Compliance regulations require documentation and reporting. A SIEM solution provides *centralized, built-in,* real-time log collection, alerting and reporting features. **Visibility:** A SIEM solution provides *real-time visibility* into what's happening across your entire network — 24/7/365.
Remediation: Real threats are *identified, isolated and remediated* quickly before they can cause serious harm and costly business disruptions.



DID YOU KNOW?

It can take several days, even months, to identify a data compromise, and it's easy to see why. Modern security tools can generate millions of security alerts over the course of a day. A SIEM solution filters out the noise, so the real threats get immediate attention.

4

How Does SIEM Work?

E-R-I-N

Events

First, we collect millions of security alerts, or events, from your entire network.

Rules

Then, we apply rules to determine which events are actionable threats.
(These threats become incidents.)

Incidents

Next, the most critical incidents get immediate attention.

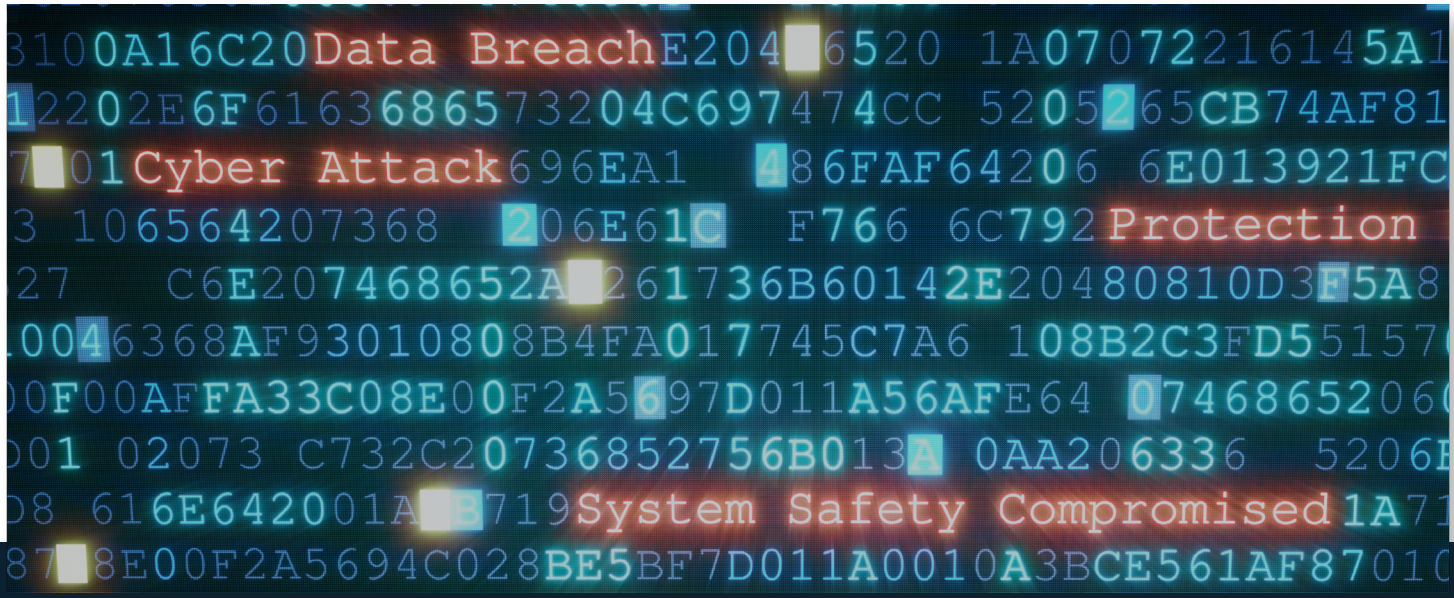
Notifications

Finally, your response team is instantly notified so remediation can begin.

5

Who Needs a SIEM?

With today's ever-evolving cybersecurity landscape, a SIEM solution plays a critical role in staying ahead of the latest threats. And while every business can benefit from a SIEM, those that must comply with industry and government regulations and those looking to qualify for cybersecurity insurance will find it essential.



Microtel Systems Corp

804-254-2057

www.microtelsystems.com