

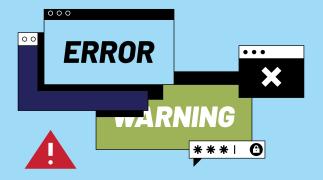
# 5 MUST-KNOW SIEM QUESTIONS ANSWERED

SIEM 101: Frequently Asked Questions



- What Does SIEM Stand for?
  SIEM = Security Information and Event Management
- 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.
- 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.



### **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.



### 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.

3100A16C20Data BreachE204 6520 1A07072216145A1
12202E6F6163686573204C697474CC 5205 65CB74AF81
7 01Cyber Attack696EA1 86FAF64206 6E013921FC
3 106564207368 206E61 F766 6C792Protection
27 C6E207468652A 261736B60142E20480810D3F5A8
.0046368AF93010808B4FA017745C7A6 108B2C3FD551570
00F00AFFA33C08E00F2A5697D011A56AFE64 07468652060
001 02073 C732C20736852756B013A 0AA206336 52060
08 616E642001A B719System Safety Compromised 1A71
87 8E00F2A5694C028BE5BF7D011A0010A3BCE561AF87010