ResilientTech Advisors
June 2025

Why Your CISO Keeps Pushing for “SIEM” & “SOAR”

And why ignoring them could cost more than money, uptime, or trust.

Here’s the “*so what*” that every executive needs to understand…

Does your CISO seem fixated on logging, alerting, & automation platforms like SIEM (Security Information & Event Management) & SOAR (Security Orchestration, Automation, & Response)?

They’re not trying to pad the budget. **They’re trying to keep you & your organization from becoming the next headline.**

You can’t stop what you can’t see.

- **SIEM & SOAR platforms transform scattered technical noise* into real-time visibility across your digital ecosystem.**

- **This is your early warning system.** It allows your security team to detect when a threat actor is already in your network, moving laterally, escalating privileges, or quietly exfiltrating data.

*Examples of “technical noise”: User logins, network behavior, system alerts

You can’t stop what you can’t see.

Your organization might not even know it’s compromised until operations go dark or its data shows up for sale.

- Once an attacker successfully breaks into an organization’s systems, **it typically takes 11 days before the organization even realizes they’ve been breached.**
- Without modern detection capabilities - those **11 days often become weeks or even months.**[1]

[1] Mandiant. M-Trends 2024 Special Report. Google Cloud, 2024

SIEMs surface meaningful threats quickly.

SOAR automates the playbook - isolating affected systems, resetting credentials, and notifying responders - **so your team can act fast and stay focused.**

Attackers move faster than most legacy processes or overworked analysts can respond.

This speed translates into **real business outcomes**:

☑ Reduced dwell time = **less damage**.

☑ Faster containment = **lower recovery costs**.

☑ Proactive defense = **stronger customer & stakeholder trust**.

SIEM & SOAR are not plug & play

SIEM & SOAR require sustained investment in people, tuning, & training

The True Cost of Doing Nothing

Upfront spend includes licensing, staffing, & training.

But compare that to:

- **Weeks offline**
- **$ Millions lost**
- **Brand reputation damage**

And those are the quantifiable costs. Rebuilding trust is harder to price.

Here’s what you need to do now

- **Ask your CISO how you're detecting - not just defending.** Your firewalls won’t save you from compromised credentials or insider threats. SIEM & SOAR platforms help surface what traditional controls miss.
- **Fund the talent.** These tools are only as effective as the team configuring & managing them. Invest in people, not just tech.
- **Demand metrics, not magic.** Well-implemented SIEM/SOAR platforms can show measurable improvements in detection speed, incident response times, & reduced impact. Make sure your team is reporting on them.
- **Start with SIEM, graduate to SOAR.** Automating before you’re ready is risky. Visibility comes first.