THREATIQ | LABS

THREATIQ LABS FIELD NOTES

What CISOs Should Expect From Their SIEM

Moving beyond log storage to security outcomes.

FIELD NOTE #004

Your SIEM is working.
Are you?

Practical insights from real-world security engineering.

threatiqlabs.com

THE EXPECTATION GAP

You bought outcomes — but you’re measuring activity.

A SIEM should be more than a place where logs go to live.

What teams measure

Activity

- GB ingested per day
- Log sources onboarded
- Number of alerts generated
- Dashboards built

What leaders actually bought

Outcomes

- Time to detect and respond
- Percent of critical assets covered
- Detections that fired on real incidents
- Analyst hours saved

OWNING ISN'T OPERATING

A SIEM you own. A capability you operate.

A SIEM is not

— A compliance checkbox

— A log warehouse

— A dashboard factory

— An alert machine

— A set-and-forget project

A SIEM should deliver

Visibility
Answer what happened, where, and to what — fast.

Detection
High-fidelity alerts on real threats, not noise.

Efficiency
Analysts investigating, not babysitting the tool.

Reporting
Security data leadership can actually act on.

Improvement
Coverage and fidelity that measurably improve.

Owning a SIEM is not the same as operating a security capability.

FIVE QUESTIONS TO ASK THIS QUARTER

Five questions to ask this quarter.

Forward these to your SIEM team. Fuzzy answers are the gap to close.

1. If the SIEM disappeared tomorrow, what capabilities would we lose?
2. What percentage of our critical assets are actually covered by detections?
3. When did a detection last catch something before it became an incident?
4. How long does it take us to answer “what did this account do?”
5. Are we measuring outcomes — or just ingest volume and alert counts?

A SIEM isn’t valuable because of what it stores. It’s valuable because of what it enables.

A SIEM that simply stores logs is an expense. A SIEM that drives visibility, detection, and faster decisions is a capability. The difference isn’t the tool — it’s how you operate it.

WHAT GOOD LOOKS LIKE

Visibility • Detection • Efficiency • Reporting • Improvement

Wondering whether your SIEM is delivering outcomes? That’s a conversation worth having.

info@threatiqlabs.com · threatiqlabs.com