The 10 Questions Your SIEM Alerts Can't Answer, But Attackers Hope You Never Ask

Your SIEM can tell you a lot about a security event. What happened, which user or asset was involved, what detection fired, and what activity was observed. But those answers often stop short of explaining why the event was possible in the first place.

Was the security control that should have stopped it actually enforcing? Did the right policy apply? Was an exception in place? Did a configuration change weaken protection? Are other assets exposed to the same condition?

Without that context, analysts have to leave the investigation, jump between consoles, reconstruct policy and configuration history, and chase control owners to understand what went wrong. Even after the incident is contained, the underlying control weakness can remain in place, leaving the environment open to repeat events and more alerts.

START WITH "WHAT HAPPENED?", THEN KEEP GOING

UNDERSTAND THE EVENT

What happened, and what was affected?

UNDERSTAND THE PROTECTION

What should have stopped it?

FIND THE ROOT CAUSE

Why was the event allowed to happen?

PREVENT THE NEXT EVENT

What else is exposed, and what needs to change?

HOW TO USE THIS CHECKLIST

CHECK AGAINST YOUR CURRENT SOC WORKFLOW

For a typical alert, can your analysts answer each question with the evidence already in their workflow?

CHECK IT ONLY IF THE ANSWER IS READILY AVAILABLE

No manual digging, console-hopping, or chasing another team.

Every unanswered question is investigation friction, an unresolved control weakness, and a future alert waiting to fire.

Score your SIEM alerts

Check each box only if your analysts can confidently answer the question during an investigation using the evidence available in their normal SOC workflow.

01 WHAT ACTUALLY HAPPENED?

Can you clearly determine what activity triggered the alert and what occurred? Your analysts should have enough event evidence to understand the behavior without spending excessive time reconstructing the incident from raw logs.

- Detection or event details
- Relevant user, process, network, or application activity
- Timeline of the observed behavior

02 WHAT ASSET, IDENTITY, OR WORKLOAD IS AFFECTED?

Can you quickly understand what is at risk? An alert has different significance depending on whether it affects an internet-facing server, privileged identity, executive endpoint, production workload, or low-risk system.

- Asset or identity involved
- Business or security importance
- Relevant environment and exposure

03 WHICH SECURITY CONTROLS SHOULD HAVE STOPPED IT?

Can you identify the protections that were supposed to prevent the activity? Knowing that malicious activity occurred does not explain which defensive control should have prevented it.

- Relevant endpoint, network, identity, email, cloud, or SaaS control
- Expected preventive capability
- Security policy intended to protect the affected asset

04 WERE THOSE CONTROLS ACTUALLY ENFORCING?

Can you determine the live state of the relevant security control? A control can exist without actually protecting the asset involved in the alert.

- Enforcement state, and enabled or disabled protections
- Whether the relevant capability was actually active
- Whether protection applied at the time of the event

05 DID THE RIGHT SECURITY POLICY APPLY?

Can you verify that the affected asset, identity, or workload was covered by the intended policy? A security capability may be enabled while the wrong policy, rule, profile, or scope leaves the affected asset unprotected.

- Policy coverage, and rule or profile assignment
- Scope and targeting
- Gaps between intended and actual protection

06 DID AN EXCEPTION OR OVERRIDE WEAKEN PROTECTION?

Can you see whether an exception, exclusion, or override contributed to the event? Temporary exceptions and security overrides can quietly become persistent exposure and generate more alerts in the future.

- Policy exceptions, allowlists, or exclusions
- Disabled protections
- Approved or unapproved overrides

☐ 07 DID A CONFIGURATION CHANGE CREATE THE OPENING?

Can you see what changed before the incident? Understanding configuration history can turn an investigation from speculation into a specific root-cause finding.

- What changed, and when it changed
- Who made the change
- Before-and-after configuration state

☐ 08 WHAT ELSE IS EXPOSED TO THE SAME WEAKNESS?

Can you identify other assets, identities, or workloads affected by the same condition? The alert may involve one asset, while the underlying control weakness affects many more.

- Other assets with the same configuration
- Other systems covered by the same weak policy
- Similar exceptions or control gaps elsewhere, and the scope of the broader exposure

☐ 09 DO YOU KNOW EXACTLY WHAT NEEDS TO BE FIXED?

Does the investigation lead to a specific corrective action? Containment addresses the immediate event. Analysts should also know how to correct the underlying control weakness.

- Specific control or configuration to change
- Clear remediation action, and the relevant policy or rule
- Owner of the fix

☐ 10 CAN YOU VERIFY THE WEAKNESS IS ACTUALLY GONE?

Can you confirm the control is properly configured and enforcing after remediation? Closing an incident without validating the underlying fix can leave the same attack path open and invite more alerts in the future.

- Corrected configuration and restored enforcement
- Confirmed policy coverage
- Continued validation for future drift

YOUR SCORE

0–3 CHECKED

EVENT DATA ONLY

Your alerts may tell analysts what happened, but major questions about protection, root cause, and broader exposure remain unanswered. Analysts are likely spending significant time gathering context outside the investigation, and the same root causes keep generating new alerts.

4–7 CHECKED

PARTIAL INVESTIGATION CONTEXT

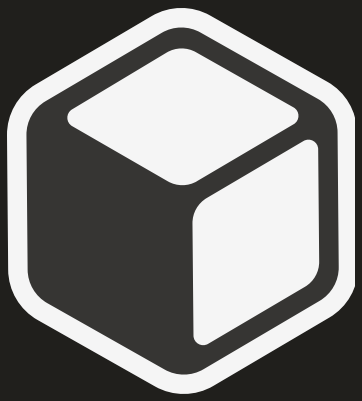
Your analysts have some useful evidence, but important questions still require manual pivots, additional tools, or handoffs. Control failures can remain difficult to identify and fix consistently.

8–10 CHECKED

PREVENTION READY

Your analysts have the context to move quickly from detection to root cause, remediation, and prevention. Every root cause you fix removes a source of repeat alerts, which reduces alert volume. Keep validating that the evidence remains accurate as controls, policies, and configurations change.

Give every alert the security control evidence to act faster



Traditional SIEM and detection tools provide critical evidence about security events. But they rarely explain whether the security controls that should have prevented the event were actually protecting the affected asset. Reach adds that missing security-control context directly into SOC workflows.

For every alert, Reach connects the event to the controls expected to protect the affected asset, identity, or workload. Analysts can see whether protection was enforcing, whether the relevant policy applied, whether an exception weakened it, and whether configuration changes or drift created the opening. That gives analysts the evidence to investigate faster, prioritize based on actual exposure, fix the underlying control weakness, and identify what else may be exposed.

01

TRIAGE FASTER. PRIORITIZE BETTER.

See control state, policy coverage, configuration history, and actual exposure alongside the security event. Give analysts more evidence to determine which alerts require immediate action and which assets are actually protected.

02

FIND THE CONTROL FAILURE

Connect the alert to the protection that failed, was missing, misconfigured, overridden, or no longer applied as intended. Understand why the event was allowed to happen, instead of stopping at what happened.

03

FIX THE ROOT CAUSE

Give teams specific guidance to correct the underlying policy, configuration, exception, or control weakness. Reduce investigation handoffs and turn incident response into an opportunity to improve the defenses already deployed.

04

PREVENT REPEAT ALERTS

Identify other assets exposed to the same weakness, remediate the gap, and continuously validate that the control remains properly configured. Fixing the underlying control weakness helps prevent repeat security events and reduce recurring alert volume.

Faster answers. Stronger controls. Fewer repeat alerts.

Enrich every SOC alert with the security-control context analysts need to investigate, remediate, and prevent recurrence.

Request a Demo

reach.security