

Prepared for

/\/ nebulock

Stop Waiting for the Alert

Building a Proactive Security Operation

November 2026 EMA White Paper
By **Christopher M. Steffen, CISSP, CISA, CCZT;** VP of Research
Information Security, Risk, and Compliance Management

EMA™
IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Table of Contents

1 Executive Summary
1 Introduction
2 Alerts are Lagging Indicators
2 The Division was Never Natural
3 The CISO has Already Evolved
4 The Rise of the Security Engineer
5 Design the Workflow Around the Person
5 Proactive is a Discipline, Not a Slogan
6 Conclusion
7 Where to Start
7 Sources

Executive Summary

The teams that operate and manage the security operations centers are losing the war of alerts. Sixty-three percent of alerts go unaddressed, and 76% of organizations name alert fatigue as a top SOC challenge [1]. The bad guys know it and have studied which alerts are generally considered noise and which alerts are often just skipped. Then, they bury their real attacks under deliberate alert storms [2]. Worse, the enterprise adoption of AI is radically adding to the noise [3].

Key findings for security leaders:

- **63% of alerts go unaddressed [1].** Much of the signal organizations pay to collect never reaches a human.
- **Attackers exploit SOC blind spots by design [2].** An alert-first SOC effectively hands them a map of what gets ignored.
- **42% of CISOs now report directly to the CEO [4].** As the CISO moves toward enterprise risk, deep technical judgment has to live below that role.
- **95% of security teams report at least one skills gap [5].** AI is pushing analysts, hunters, and detection engineers into a single, hybrid security engineer role.
- **Only 37% of organizations have a formal threat hunting methodology [6].** That is down from 51% in 2024, even as hunting matters more than ever.

Addressing alerts faster is not the answer – security teams will never be able to operate at the speed of AI. They need a hunt-first workflow built around a converged role: the security engineer.

Introduction

Nearly every IT team and security operations center shares the same quiet confession: they are not looking at most of their alerts. Not because the people are careless, but because the math stopped working years ago.

At the same time, something more interesting is happening inside those teams. The lines between the analyst, the threat hunter, and the detection engineer are blurring. Sometimes that's by design, but more often than not, it is out of necessity.

Those two trends are connected, and how security leaders and their organizations react to these trends will shape what the SOC looks like for the next decade.

Alerts are Lagging Indicators

For twenty years, the SOC ran on a simple premise: the tools generate alerts and people work the queue, triaging according to severity and business risk. That model made sense when telemetry was limited, attacks followed predictable patterns, and reactions were at human speed. Fast forward to 2026, and the core processes for running the SOC changed significantly.

Seventy-six percent of organizations name alert fatigue as a top SOC challenge, and 63% of alerts still go unaddressed [1]. Once a team falls behind, triage rules harden into habit. Low-severity alerts are deprioritized by design, and that "acceptable risk" quietly becomes permanent [2].

The attackers have noticed and are taking advantage of it. They have access to the same response metrics as those they are attacking, and they know which detections are noisy and which alert categories get skipped [2]. Some are deliberately generating alert storms to bury the activity that matters. Enterprise AI adoption is piling even more noise onto an already-strained baseline [3].

Here is the part that gets lost in all the talk about faster triage: by definition, an alert only occurs after something has already happened. It only generates for things someone already knew to look for or configured their security tool stack to monitor. Responding to attacks discovered through alerts is reactive (not proactive), and while the tooling allows the SOC to respond more rapidly than in the past, one could also argue that it is just allowing the SOC to react more efficiently. Faster response may give the illusion of "better," but the SOC is still constrained to react to only the alerts that are next in the queue.

The Division was Never Natural

There is a certain amount of bureaucratic inertia about IT and security processes, and the way the SOC operates is part of it. When IT and security leaders are asked why they keep analysts, hunters, and detection engineers separate, most give some flavor of the same answer: "that's how SOCs are built." That answer deserves a harder look.

It is understandable, since the work (actually, all of the IT work today) is interconnected. Hunt findings become detection rules. Detection rules need hunting to validate coverage. Insider risk depends on the same behavioral analytics as threat hunting. Alert triage needs the same environmental context as all three.

For example, when looking at insider risk, 92% of CISOs who suffered a material data loss in 2025 attributed it to departing employees, up from 73% a year earlier [4]. That is a behavioral problem, not

a signature problem. Treating it as a separate discipline, in a separate tool, makes little sense. Yet, this is invariably how it is dealt with in the contemporary SOC.

Eventually, splitting these functions apart was a function of tooling and economics. To query data in a SIEM, a team had to ingest it first, and ingest was expensive. Hunting stayed in the SIEM. Detection engineering drifted toward EDR and XDR. Insider risk got its own UEBA tools. Separate tools produced separate teams, and separate teams hardened into separate disciplines. Ironically, as the tools matured, many of these tools absorbed some of the same functions (albeit as a secondary offering), with organizations paying for multiple tools that have the ability to accomplish many of the same functions, operating by different teams, and often with competing priorities.

Capacity locked it all in place. Alert triage alone could consume an entire team's day. Specialization was never really a strategy. It was a coping mechanism.

The CISO has Already Evolved

The convergence on the SOC floor mirrors a bigger change at the top. EMA research found that 89.5% of organizations now have a dedicated CISO [4], which at first glance looks like significant progress for the technical practitioners. However, that CISO looks very different than a decade ago.

In 2023, about 54% of CISOs reported to a CIO or CTO. By 2025, that share fell to 30%, and 42% now report directly to the CEO [4]. The talent pipeline is shifting, too. Security leaders once rose out of the SOC. Increasingly, they come from governance, risk, compliance, and legal [4].

Core Skill/Background	Legacy Technical CISO	Modern GRC/Legal CISO
Primary focus	Security operations and defenses	Enterprise risk and resilience
Language	Jargon and technical specs	ROI, financial risk, and impact
Talent origin	SOC/IT engineering	GRC/legal/audit
Key frameworks	MITRE ATT&CK/NIST	ISO 42001/EU AI Act

Source: EMA, The Evolution of the Chief Information Security Officer, May 2026 [4]

That is a healthy change for the board room. It also leaves a significant gap. As the CISO moves away from the lead technical practitioner toward a role of enterprise risk, the deep technical judgment has to live somewhere else. One CISO in EMA's research described the arc of the job this way:



"At the beginning, I'm hyper-technical; by the end – before I get bored and leave – I'm hyper board-focused."

— CISO, Health Care Company [4]

The Rise of the Security Engineer

When AI agents handle enrichment, scoping, and first-pass triage (traditionally a Tier 1 analyst responsibility), a human no longer needs to spend the day deciding whether an alert is real. That time (presumably) goes back to work that requires human-in-the-middle types of judgments. The analyst and the detection engineer stop being two jobs and become a single role: the security engineer.

The security engineer is a person who hunts, turns the findings into actionable detections, investigates insider risk, and oversees how alerts are handled. The AI agent can do the repetitive querying, correlation, and baselining underneath. To be clear, this is not about replacing people. It is effectively utilizing the tools available to offload simpler tasks, much in the same way that IT professionals have been using various types of automation for decades. It is about up-leveling the humans in the SOC.

ISC2's 2025 study of more than 16,000 professionals found that 95% reported at least one skills gap on their teams [5]. Seventy-three percent expect AI to create more specialized skills, while 66% expect it to require broader skillsets [5]. The role is getting deeper and wider at the same time. By definition, that is what a hybrid security engineer practitioner looks like.

The hybrid security engineer role also changes the career paths. The old ladder treated hunting as a reward for surviving the queue. When agents handle most of the triage, the new path builds investigation and detection skills from day one. It may also bring in people from outside the traditional security skills box because more generalized IT practitioners add value to hybrid roles, either from technical expertise, longevity experience, or business perspective.

Design the Workflow Around the Person

An organization that converges the roles but keeps the existing fragmented, alert-driven workflow and processes has rebuilt the same, existing problem with a new wrapper (and presumably fewer people). In 2025, 66% of CISOs reported facing excessive expectations, and 63% had experienced or witnessed burnout [4]. Fifty-eight percent admitted their organizations were unprepared for the very attacks they feared most [4].

Bolting an AI chatbot onto a legacy security infrastructure does very little to address this. A natural language interface on the same alert-first architecture is a new coat of paint on an old house.

A workflow built for the converged security engineer has a few non-negotiables, and these no-negotiables should serve as a part of a checklist for SOC modernization:

- **One shared context.** Hunting, detection, insider risk, and triage should draw on the same behavioral record of users, devices, and applications.
- **Behavior over indicators.** Attackers rotate infrastructure and file hashes easily. Changing how an attack behaves is much harder, so detection should target tactics, techniques, and procedures (TTPs).
- **Environment-specific baselines.** A generic verdict means little. What matters is whether this behavior is normal for this user, here, right now.
- **A closed loop from hunt to detection.** Every finding should become a tested, versioned detection without a manual handoff.
- **No forced migration.** The workflow should work with the SIEM, data lake, and tools already in place.
- **Transparent automation.** Agents should show their evidence and reasoning, and the engineer must be able to override them.

Proactive is a Discipline, Not a Slogan

“Proactive” is one of the most overused terms in the security world. For clarity, a proactive cyber-security team goes looking for adversary behavior and vulnerabilities before existing alerting infrastructure generates the alert.

In a hunt-first model, hunting is the default activity rather than something saved for quiet days. Agents query telemetry continuously, and alerts become one input among many. The hardest threats are the ones that look fine – valid credentials at an odd hour, or a legitimate admin tool used in an unusual sequence. Only behavioral baselines catch those, or a very experienced security engineer who understands the nuances of corner case threats and business requirements.

Proactive work also compounds an organization's security maturity. A review or exercise that finds nothing still validates coverage, whereas a review that discovers a potential vulnerability or exploit blazes a new path for detection. Agentic SOC agents can test an unlimited number of potential hypotheses against live telemetry, handing off the promising leads to the SOC analyst for judgment and triage. The process is always on – it never stops, even when the analyst goes home for the day.

Unfortunately, the industry is moving the wrong way on discipline. The SANS 2026 Threat Hunting Survey found only 37% of organizations have a formally defined hunting methodology, down from 51% in 2024 [6]. Only 40% formally measure whether hunting works [6]. For the first time, data quality outranked skilled staff as the top barrier [1]. A modern workflow should fix that by capturing hypotheses, findings, and detections automatically.

Conclusion

AI is causing the roles in the cybersecurity space to evolve, from the top down. The CISO has moved from lead practitioner to enterprise risk and regulatory steward. Beneath that shift, the analyst, the hunter, and the detection engineer are becoming a single, hybrid role. Some may see it as a cost-saving exercise, but they will continue to struggle, because the real opportunity is recognizing that the work was always connected and that the tools finally let people work that way.

The biggest risk is moving people without refining the existing processes. Understanding the optimized workflow has to come first, and security teams have to stop waiting to be told something is wrong. Attackers already know which alerts are ignored. The only real answer is to go find them first.

Where to Start

Most organizations can start with the alert telemetry and tools they are already using in their infrastructure. Here are three practical considerations for first steps:

- **Measure the gap.** Determine what share of alerts never receive a human review, and which alert categories are deprioritized by default.
- **Map the overlap.** Document where threat hunting, detection engineering, insider risk, and triage live today, including the tools, teams, and data each one uses.
- **Evaluate against the non-negotiables.** Use the six workflow requirements in this paper as the scorecard for any platform under consideration.

Consider a short, scoped pilot on live data. It will be the fastest way to see what the alert queue is missing, and how a tool or process will address that deficiency. It will also give cybersecurity leadership the direct evidence needed to secure budget, instead of just another tool in the security stack that doesn't address the promise of faster, more productive alert triage.

Sources

[1] Cybersecurity Insiders **Pulse of the AI SOC Report**, August 2025.

[2] Intezer, **2026 Intezer AI SOC Report for CISOs**, February 2026.

[3] Cloud Security Alliance, **Research Note: AI SOC Alert Noise**, September 2026.

[4] Enterprise Management Associates (EMA), *The Evolution of the Chief Information Security Officer: The Shift from Technical Guardian to Enterprise Risk Architect*, May 2026.

[5] ISC2, **2025 Cybersecurity Workforce Study**, December 2025. Skills gap figures via **SecurityInfoWatch**.

[6] SANS Institute, **SANS 2026 Threat Hunting Survey: The Evolution of Threat Hunting**, September 2026.



About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading IT research and consulting firm dedicated to delivering actionable insights across the evolving technology landscape. Through independent research, market analysis, and vendor evaluations, we empower organizations to make well-informed technology decisions. Our team of analysts combines practical experience with a deep understanding of industry best practices and emerging vendor solutions to help clients achieve their strategic objectives. Learn more about EMA research, analysis, and consulting services at **www.enterprisemanagement.com** or follow EMA on **X** or **LinkedIn**.

This report, in whole or in part, may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. "EMA" and "Enterprise Management Associates" are trademarks of Enterprise Management Associates, Inc. in the United States and other countries.

©2026 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common law trademarks of Enterprise Management Associates, Inc.

2770 Arapahoe Road, Ste 132 - 544, Lafayette, CO 80026 +1 303.543.9500 **www.enterprisemanagement.com**

4817.110926