paloalto® NETWORKS | CORTEX®

5 Essential Steps to SOC Transformation

Elevate Your SOC with Automation and AI Capabilities
Designed for the Modern Threat Landscape

The Modern Security Landscape Is Changing Fast

Since the first security operations center (SOC) was established in the mid-1970s, it has continued to evolve—both in what it does and the role it plays in the enterprise. Today, with the widespread digitalization of nearly every business function, the SOC is critical to the overall health and growth potential of organizations across industries.

Enticed by the expanding attack surface, threat actors have grown increasingly sophisticated and persistent, but not all SOCs have kept pace. Many companies are still running SOC configurations and tools they developed years ago—systems designed to deal with yesterday's threats through manual efforts and complex processes.

But those systems are no longer adequate. Not by a long shot. They simply can't keep up with threats aimed in every direction—at servers, networks, applications, endpoint devices, and websites—around the clock.

Today's SOCs Are Facing a Barrage of "More"

- **More attacks, period.** The sheer volume of cyberattacks has increased—yet many companies are still using manual efforts to investigate and mitigate them. It's a losing battle.
- **More threat actors that are more organized.** Today's cybercriminals rarely resemble the "lone wolf" of pop culture. Rather, they're more likely to be part of a well-funded entity that can wage sustained and sophisticated campaigns.
- **More devices and data that need to be protected.** From network to endpoint to edge, security teams must secure a large and growing estate that cannot be contained behind a corporate firewall. The ongoing popularity of hybrid work ensures that attacks—like work—can happen anywhere.
- **More security tools that create more complexity.** The number of security solutions and vendors has exploded in recent years, leading to a dizzying array of products that often don't work well together—or at the very least, must each be integrated, managed, and maintained.
- **More regulations from more agencies.** From the SEC to state and local government agencies, reporting requirements are becoming more onerous. Security teams are expected to detect attacks, assess their impact, and report on that information—or face potential fines or penalties.
- **More specialized focus areas that create more silos.** As security professionals specialize in different things, they can increasingly be isolated from each other, working in their own area of expertise without sharing their insights—or seeing beyond their own purview.

How can the SOC modernize to meet the current threats, demands, and pressures?

96%

of security professionals had experienced at least one breach or incident in the past year. Of those, 57% reported 3+, and 24% were aware of 10+.[1]

84%

of security professionals agree they have seen more security incidents due to hybrid work.[1]

Examining the SOC to Determine What Needs to be Fixed

A modern SOC must act as a responsive, fast-moving entity that combines threat intelligence with tools that prevent, detect, investigate, and eliminate threats of all kinds. But how can security teams actually reach this ideal state?

Developing a best-in-class SOC requires a closer look to determine how legacy models can be transformed to handle the needs of today's security operations centers.

This guide outlines five key challenges that limit SOC efficiency and effectiveness, paired with practical solutions and tangible benefits organizations can achieve in the process of SOC transformation.

[1] *What's Next in Cyber: 2022 Global Survey*, Palo Alto Networks, 2022.

Even the Most Difficult SOC Challenge Has a Solution

	THE CHALLENGE	THE SOLUTION
1	Tool Sprawl Creates Complexity and Risk	Simplify the SOC with a Consolidated Security Stack
2	Alerts Generate Constant Noise but Little Insight	Gain Clarity with AI-driven Intelligence
3	Security Analysts Are Bordering on Burnout	Elevate SecOps with Automation and AI-enabled Solutions
4	Context Gaps Create Blind Spots	Uncover the Story Behind the Data
5	Threat Containment Takes Too Long	React Fast with Integrated Incident Response

Tool Sprawl Creates Complexity and Risk

Most SOCs change direction as security leaders and priorities rotate over the years—and it shows. Teams often adopt the security approach or solution du jour without accounting for the difficulty involved in maintaining that piece of software (and the next, and the next) over a period of years.

But without careful oversight, the SOC can begin to resemble a garage filled with various half-finished experiments. The security stack becomes a jumble of point solutions from different vendors, each with unique datasets, UIs, and agents. Each of these must be maintained and monitored, and each also comes with an operational cost, from workstreams to skill requirements to learning curves.

Juggling multiple solutions is not only time-consuming and resource-intensive—it also makes the SOC less efficient than it could be.

Disparate Tools Distort Visibility

Many solutions found in the typical SOC are not interoperable. They don't share data, yet many gather data on the same things and deliver findings in different ways. Trying to piece events and alerts together across these tools without making a mistake? That's the challenge every day.

The net result is a chaotic, and sometimes conflicting, view of the environment. Analysts may take away varying conclusions based on the tool they're working in. There is no shared, holistic view.

Complexity Drives Up Costs

Over time, a SOC can become so intricate and multilayered that it requires considerable institutional knowledge to cultivate and configure at a level the organization requires. Because life happens: Teams change. Individuals come and go. Leadership changes focus. Some solutions are forgotten, while others are neglected.

Ultimately, these organizational cycles cause drift and create new security exposures and risks. Because this level of complexity is nearly impossible to maintain without error.

Inevitably, alerts are missed or a tool is misconfigured, a breach is undetected, and the business incurs damage or loss.

Simplify the SOC with a Consolidated Security Stack

Reducing chaos requires letting go of the complexity. But that's easier said than done. Determining what to eliminate and what to keep requires a thoughtful, systematic process.

Audit Your Environment

Identify all the assets your SOC is currently protecting, from networks to servers to endpoints. Of these, which are high-risk and low-risk? What is missing from this list? Where are the gaps?

Consolidate Vendors and Tools

How many different tools, systems, and datasets are your teams currently using? How many are considered best-in-class, and which have seen better days? Which tools are monitoring the same things? Where can you eliminate and consolidate?

Implement a Unified Approach to Management

The phrase "a single pane of glass" has turned into industry jargon, but the metaphor is still valuable. A cohesive system that integrates all of your data sources, applies embedded intelligence to these sources, and offers consolidated workflows can greatly boost SOC efficiency.

Benefits

Better Analyst Focus

Without the need to continually switch contexts, your analysts can focus on a consistent set of tools. More clarity allows them to spot issues faster and better identify important or urgent information.

A Unified View

A central console provides a consistent view of incidents, issues, and exposures across the organization. When everyone has the same view, you can make decisions faster.

A Truly Informed Approach

By adopting tools that bring data sources, intelligence, and analysis into a shared system, there are fewer gaps. Your SOC is no longer a container for disconnected systems but an intelligent hub that continuously improves.

Alerts Generate Constant Noise but Little Insight

Many cybercriminal groups are emulating the tactics of advanced persistent threats (APTs), which are expert attackers with extensive resources that allow them to use multiple different attack vectors to achieve their objectives.

It's no wonder that security teams are dealing with alert overload. Security incidents are continuous—24/7/365—creating near-constant alerts. Analysts spend hours investigating alerts and determining which are credible and which are not.

When Everything is Urgent, Nothing is Urgent

Many of the tools that produce alerts are poorly tuned and redundant, producing a stream of false positives, but analysts can't ignore them. Rather, they must plod through hundreds or thousands of alerts to find any that might be relevant. When they do identify potential threats, they have to manually correlate them into a cohesive view.

Meanwhile, because analysts have to wade through so much noise, true threats remain undetected for longer. According to data collected by Palo Alto Networks Unit 42®, the median dwell time observed for ransomware attacks was 28 days. Left alone, attackers are able to wreak havoc before teams even know they're there.

On average, SOC team members spend **one-third of their typical workday** investigating and validating incidents that aren't a real threat.[2]

56% of large companies handle at least **1,000 alerts per day.**[3]

[2] *Global Security Operations Center Study Results*, IBM, March 2023.

[3] *"56% of Large Companies Handle 1,000+ Security Alerts Each Day,"* Dark Reading, July 10, 2020.

Gain Clarity with AI-driven Intelligence

Reducing the volume of false positive alerts should be a top priority for teams looking to transform the SOC.

Leverage Playbooks to Automate Alert Handling

- Use playbooks that utilize behavioral detection and threat intelligence to rapidly classify alerts.
- Customize this classification by identifying specific attributes you deem important.
- ML-powered solutions can gather, integrate, and analyze data to reach conclusions faster and close many alerts without human intervention.

Quickly Tune Alerts to Improve Accuracy

- Reduce false positives with solutions that make alert tuning fast and simple. With fewer, higher-quality alerts, analysts can direct their time and attention toward those that pose an actual threat.

Benefits

A Proactive Stance

By relieving your analysts of the task of manually sorting alerts, your SOC shifts from reactive to proactive.

Better Analyst Productivity

With a radical reduction in ticket volume, analysts are free to focus on issues that pose an actual threat.

Improved Business Continuity

By identifying true threats faster, SOC teams can limit damage to the business.

A More Effective SOC

Results improve without adding more people.

Security Analysts Are Bordering on Burnout

Cybersecurity pros are essential to a high-functioning SOC. But let's face it: Many are frustrated at work. They want to hunt down adversaries and make a difference, yet they're spending their days scrutinizing low-fidelity alerts or completing routine tasks that have to be repeated again the next day.

A workday full of manual investigations and low-stakes triaging makes them feel inefficient—like they're stuck in a never-ending game of Whac-A-Mole. So much busywork, so few breakthroughs.

But mundane workflows are only one problem. Outdated tools that are difficult and frustrating to use are another. Worse, analysts are often siloed in their own domain, away from others in the SOC. Everyone is focused on their own tool or area, and there's little synergy or a shared sense of accomplishment.

One in six organizations with 10,000+ employees **fields teams consisting of just one to three people.**[4]

The average modern SecOps team is responsible for **over 40 things.**[5] Security specialists spend an average of **only 26 months** with an organization.[6]

[4] *State of Security Automation Report*, Palo Alto Networks.

[5] Kathryn Knerler, Ingrid Parker, Carson Zimmerman, *11 Strategies of a World-Class Cybersecurity Operations Center*, MITRE, 2022.

[6] Christopher Crowley, Barbara Filkins, *SANS 2022 SOC Survey*, SANS, May 16, 2022.

The Danger of Analysts Losing Their Edge

When analysts are bored and overwhelmed with repetitive tasks, they stop thinking like attackers. Not because they aren't capable and willing, but because rote work dulls a sense of urgency and focus. Visions of stopping criminals and protecting the business start to fade after the thousandth alert ticket.

Not only does this raise the risks for the business, but it also makes analysts vulnerable to better job opportunities. With cybersecurity talent in short supply, savvy analysts are tempted with offers. Why should they stay in an organization with legacy technology they dread using?

Yet again, this puts the business at risk. Many SOC teams are small, and when an analyst with specialized knowledge leaves, the gap can create a vulnerability. Someone else on the team must scramble to fill in, and there's a good chance the newly assigned person will miss something.

Elevate SecOps with Automation and AI-enabled Solutions

Bringing excitement and strategic thinking back into your SOC team starts by eliminating low-value tasks.

Leverage AI to Help Solve Threats and Handle Incidents

- Implement automation that works alongside human decision-making by automatically detecting anomalous patterns across multiple data sources and providing alerts with context.
- Arm your SOC teams with insights that enhance and support their own expertise, using AI-powered solutions that can gather, organize, and interpret data with intelligence gleaned across millions of attacks.
- Incorporate AI solutions to augment and complement human security experts, for faster investigations and fewer blind spots.

Reduce Busywork by Automating Key Functions

- Protect your staff from burnout and improve retention with smart use of automation.
- Solutions that automate repetitive, low-level tasks won’t replace your analysts but will allow them to focus on the things they were trained to do and actually enjoy: investigating true threats.

Create a More Engaging and Satisfying Work Experience for Analysts

- Acknowledge concerns and changes caused by automation, and focus on how these tools can ultimately make their work more meaningful.
- Integrate teams and dissolve silos to grow a sense of ownership and shared accountability across the SOC.
- Develop a culture of continuous learning. Cross-train all team members across domains—including alert triage, incident response, threat hunting, and context—to provide more coverage across the SOC and help everyone think like an attacker.
- Upskill team members quickly and empower them to work in a new space and learn new skills. They'll have the capacity once automation relieves some of their workload.

Benefits

Empowered Analysts

When security analysts are enabled to focus on the work they actually enjoy, they are more likely to perform better.

Stronger Security Stance

Organizations with high-performing modern SOCs have a stronger chance of attracting and retaining talented team members.

Streamlined Incident Handling

By automating incident tickets and rapidly routing them to the right person when needed, teams can handle and close incidents faster.

Fewer Silos, More Shared Knowledge

Reduce reliance on a single person or people who have specific knowledge; instead, give more people the ability to understand the bigger picture and take action.

Context Gaps Create Blind Spots

In a legacy SOC, the ability to collect, process, and contextualize threat intelligence data is often missing. Even as the attack surface expands with more networks, devices, and other endpoints, the SOC can't ingest all of those sources or scale to accommodate a high volume of data.

But data points without context are just numbers. Knowing why attacks are coming from a particular source, or how attacks are related, is essential to forming the correct response. For example, a business expanding to overseas locations may expect to be targeted by foreign adversaries who did not previously view them as a threat. New attacks are then anticipated and easier to manage.

Context is also about relationships—knowing how devices or data objects or environments are related. Context requires the ability to stitch together historical data and current events, including real-time data from real-world sources, to better understand the nature and intent of the threat.

Without a single system ingesting every data source and analyzing it as a whole, the SOC has limited visibility. Lacking a cohesive, context-aware view across the business, teams struggle to understand true risk levels and implications.

Limited Visibility Slows Decision-making and Threat Response

When visibility and context are limited, security teams are understandably reluctant to make quick decisions or respond until they recheck everything manually. This could be the right choice—or it could give an attacker more time to exfiltrate data.

Visibility and context are also critical after an incident occurs. As teams work to integrate data sources and create a cohesive timeline with information gathered across disconnected security tools, they often have to play a guessing game.

What is really happening? Teams can usually figure out what happened after the fact—even in a legacy SOC. But it's very difficult to do in real time. Without an integrated, context-aware platform, organizations lack comprehensive, data-driven insight in the moments that matter most.

Uncover the Story Behind the Data

When data is integrated and in sync, it can tell the story of what happened, when, and how—giving SOC teams confidence about what moves to make next.

Integrate Data Sources into a Single Place

- Gather data across networks, clouds, endpoint devices, and more to generate a complete view of everything impacting your business.
- Implement a platform that combines data on threats, vulnerabilities, and business context into one unified view.

Leverage Intelligent Analytics for Context and Insight

- Use tools that stitch together a complete timeline to understand how threats moved, what tactics they used, and their overall pattern, approach, and impact.
- Take advantage of high-level machine learning capabilities that go beyond data points to deliver a story about how everything is connected.

Benefits

Critical Context

The full story provides insights that point to vulnerabilities and show how threats are evolving.

Impact Clarity

When analysts have complete, context-based information, they can better understand the scope and impact of an incident.

Better Preparedness

With context and visibility, teams are able to bolster defenses and prepare for future attacks.

Threat Containment Takes Too Long

While analysts toil to investigate and close alerts, true threats often remain undetected for weeks or even months. When teams do detect a breach, containing the threat requires a coordinated response that can be difficult with multiple point solutions.

Closing off access points across networks, clouds, and endpoints may involve multiple systems and team members. Complexity inevitably means that it takes more time to fully contain and eliminate the adversary.

On average, security teams take **145 hours (~6 days) to resolve a security alert.** 60% of organizations take longer than 4 days to resolve security issues.[7]

Organizations that used AI and automation capabilities extensively within their security approach experienced, on average, **a 108-day shorter time period** to identify and contain the breach.[8]

[7] *Cloud Threat Report*, Unit 42, 2023.

[8] *Cost of a Data Breach Report*, IBM, 2023.

Delays Multiply Losses and Impact

When a threat is still active and working to exfiltrate data or do damage, every minute counts. Delays put the business at risk of significant damage, including high costs, data loss, and reputational impact. The best way to combat long containment times is prevention, but when a breach occurs, speed is essential.

Once a threat is stopped, teams need to understand the total scope. Was any data exfiltrated? Which parts of the business were affected? Were any customers impacted? All of this information is vital, as it helps teams to formulate a response plan and determine next steps.

React Fast with Integrated Incident Response

From ransomware to supply chain attacks to DNS spoofing, having a coordinated plan prepared beforehand helps your SOC react quickly and decisively.

Understand the Total Impact

- Use advanced AI-driven tools to collect and analyze evidence about the incident and its scope.

Contain and Eliminate the Attacker

- Use solutions with integrated remediation capabilities so that networks, identity management, and devices can be quarantined centrally.
- Benefit from the ability to implement global updates versus going to each individual system to update a policy or enforcement point.

Strengthen Threat Prevention Capabilities

- Implement a 24/7/365 threat monitoring service.
  - › Most SOC teams can't be available around the clock—yet attackers never rest. An MDR service can help you maintain visibility at all times, without overburdening your team.
- Prepare in advance.
  - › Simulate attacks to train the team on how to react quickly and effectively when an incident occurs.

Benefits

Reduced Risk

Faster containment reduces the impact on the business and limits potential damage.

Improved Security Posture

With insights gleaned from the incident intelligence, teams can identify and close vulnerabilities.

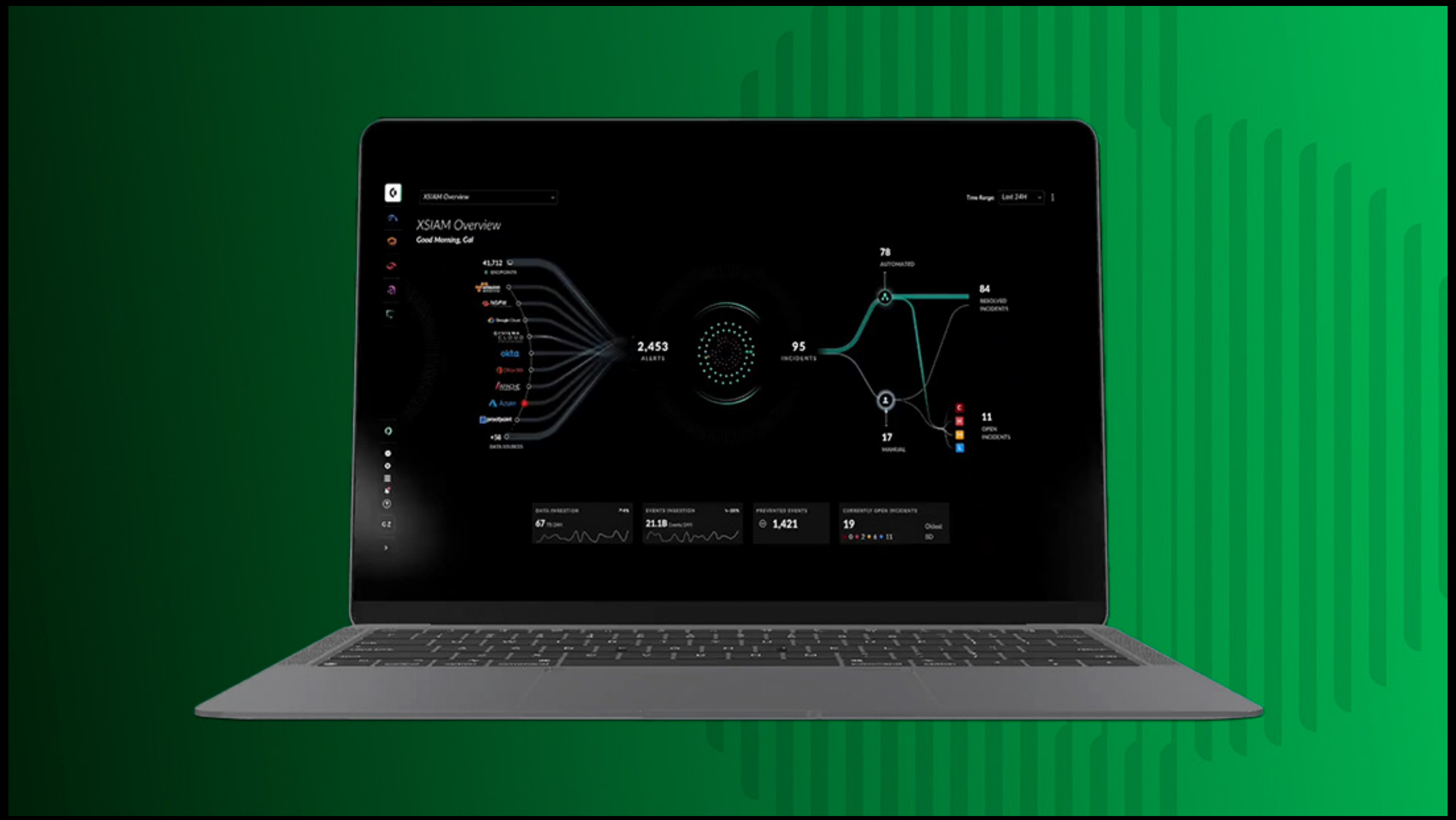
Greater Confidence

Advanced training exercises and simulations build readiness across your team.

A Solution for Total SOC Transformation

Palo Alto Networks® understands the difficulties and frustrations of legacy SOCs. Cortex XSIAM® is the AI-driven security operations platform for the modern SOC, harnessing the power of AI to simplify security operations, stop threats at scale, and accelerate incident remediation.

Reduce risk and operational complexity by centralizing multiple products into a single, coherent platform purpose-built for security operations. Built for modern IT environments, XSIAM operates across cloud and enterprise security operations, enabling comprehensive threat management everywhere.



Cortex XSIAM: Where Essential Security Capabilities Converge

To tackle the issue of SOC complexity, XSIAM brings together multiple capabilities that are often delivered by different products, including:

- Security information and event management (SIEM)
- Endpoint detection and response (EDR)
- Security orchestration, automation, and response (SOAR)
- Attack surface management (ASM)
- Identity threat detection and response (ITDR)
- Threat intelligence management (TIM)

In XSIAM, these core security offerings are offered in a single platform, within an intuitive user experience supported by intelligence automation.

Help SOC Teams Turn the Tables on Modern Threats

XSIAM starts by simplifying the security stack within the SOC and introduces AI-powered capabilities that help teams become more efficient and effective. With the support of an autonomous security platform, analysts can identify true threats, respond faster, and safeguard the business against adversaries.

Simplify Security Operations with a Converged Platform

The convergence of SOC capabilities—such as XDR, SOAR, ASM, and SIEM—onto a single platform is a game-changer for security operations. It eliminates the hassle of console switching, providing a streamlined experience. The platform offers broad integration support, making it easier to onboard various data sources without the need for extensive engineering and infrastructure work.

This allows SOCs to effortlessly ingest more security-relevant data, enhancing their analytical capabilities. Moreover, the platform ensures continuous collection, stitching, and normalization of raw data, going beyond just alerts. This empowers SOC teams with superior and simplified investigation, enabling them to identify and remediate threats faster and more effectively.

Stop Threats at Scale with AI-driven Outcomes

Out-of-the-box AI models go beyond traditional methods, connecting events across various data sources and offering a comprehensive overview of incidents and risks in a single location. This empowers organizations to enhance their detection, analysis, and response capabilities.

By leveraging alert grouping and AI-driven incident scoring, Cortex XSIAM seamlessly connects low-confidence events, transforming them into high-confidence incidents. This prioritization is based on the overall risk, enabling security teams to focus their efforts efficiently.

Accelerate Incident Remediation with an Automation-first Approach

With hundreds of tried-and-tested content packs in the Cortex Marketplace, SOCs can optimize processes and interaction across their entire security program. By automating previously manual tasks, embedded automation saves time and effort in responding to incidents or managing risks, such as attack surface exposures.

Moreover, users have the flexibility to add, customize, or modify automations according to their specific needs. The platform also features alert-specific playbooks that trigger automatically, ensuring security tasks are executed promptly and risks are addressed, even before an analyst gets involved. Additionally, XSIAM learns from manual analyst actions and provides recommendations for future automations. This continuous learning process enhances the platform's ability to automatically resolve incidents, improving efficiency and accuracy over time.

CASE STUDY SPOTLIGHT

An Oil and Gas Company Transforms Its SOC with Cortex XSIAM

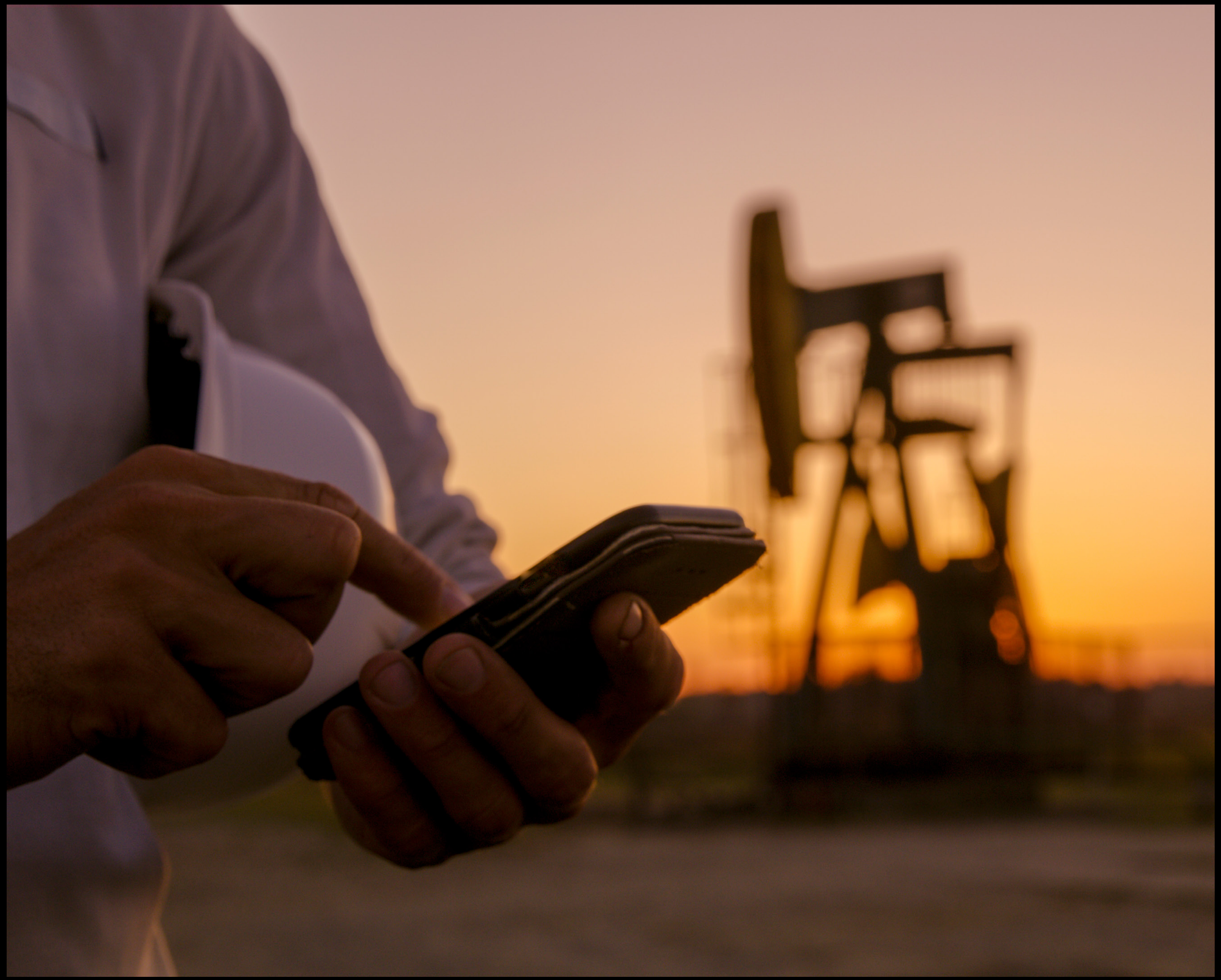
The company's legacy SIEM was generating alert overload, including a torrent of false positives, which put pressure on security teams to manually investigate across multiple security tools.

After implementing XSIAM, the company saw rapid results:

- False positive rate reduction from **~90% to near-zero**
- **75% fewer** incidents requiring investigation

Today, it is able to detect, prevent, and respond to potential threats faster and is on the path to a best-in-class SOC.

> "We used to have thousands of garbage alerts. Now we have five events a week we really need to investigate. That's how good the systems are working."
>
> – IT Security Leader, Oil and Gas Company



READ THE FULL STORY

CASE STUDY SPOTLIGHT

Boyne Resorts Boosts Analyst Efficiency and Preparedness with Cortex XSIAM

A company with ski and golf resorts across the US and Canada wanted to strengthen its SOC capabilities and gain more visibility across distributed environments—without expanding its team.

After implementing XSIAM, Boyne Resorts achieved:

- **70X growth** in data ingestion
- **65% reduction** in open incidents from 80–100 to 35 per day, due to reductions in false positive rates and duplicate incidents
- **95% reduction** in vendors and tools from 20+ tools and dashboards needed for investigations to one

Today, with a SOC that is leaner and more powerful, the security team has more visibility and insight and is better prepared to meet modern threats.

> "With XSIAM, we have more visibility and faster investigations. Seamless data onboarding and automation setup are game-changers."
>
> – Mike Dembek, Network Architect, Boyne Resorts

READ THE FULL STORY

Make Progress Toward a High-performing SOC

With an integrated platform that combines best-in-class SOC tools, security teams can count on XSIAM to deliver the robust detection, response, and investigation capabilities they need to protect the business—for whatever the future holds.

Learn More About Palo Alto Networks Cortex XSIAM

GET STARTED

paloalto NETWORKS | CORTEX

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com/cortex/cortex-xsiam