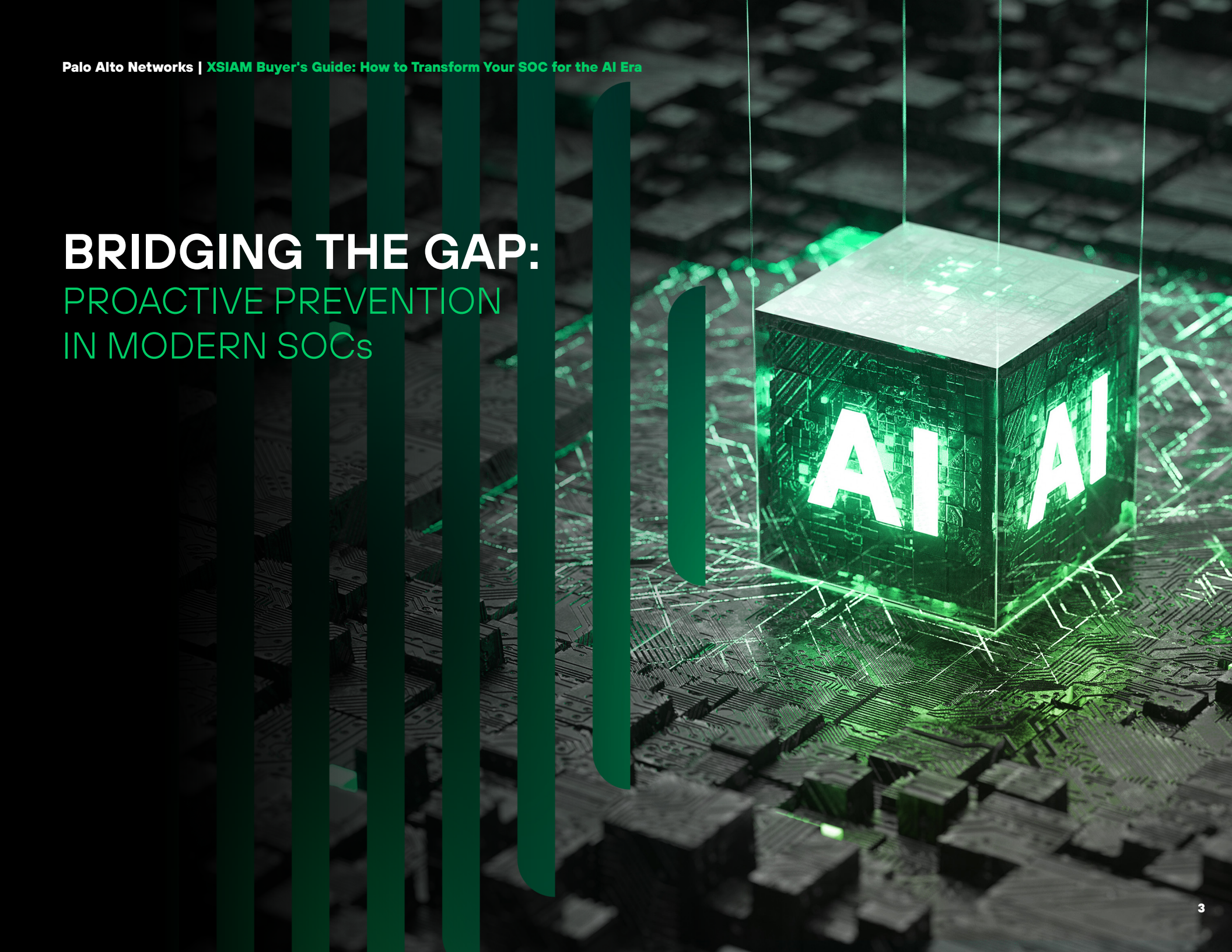
paloalto NETWORKS | CORTEX XSIAM®

XSIAM Buyer's Guide:
How to Transform Your SOC for the AI Era

TABLE OF CONTENTS

BRIDGING THE GAP:
PROACTIVE PREVENTION IN MODERN SOCs



The cybersecurity landscape is rapidly evolving, presenting organizations with unprecedented challenges. Today's threat actors are more sophisticated, using advanced techniques and AI to bypass traditional security measures. As a security professional, you're likely experiencing firsthand how the needs of your security operations center (SOC) have changed dramatically. The old ways of detecting and responding to threats are no longer sufficient in an era where breaches can occur in a matter of hours—down from 24 hours just a year ago[1]—and regulatory requirements are becoming increasingly stringent.

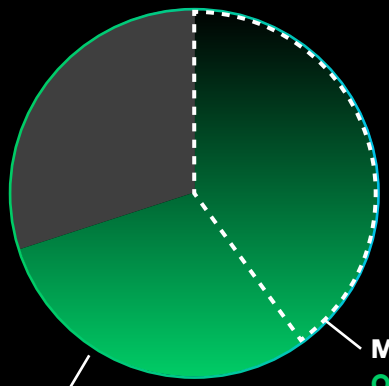
Every time a breach occurs, your security team can likely piece together what happened after the fact—how the system was compromised, which systems were involved, and what data was exfiltrated. This begs the question: If you have the information to understand an incident postbreach, why can't you prevent or stop it before it happens? This gap between postincident analysis and proactive prevention is at the heart of the evolving needs of modern SOCs.

Traditional security information and event management (SIEM) solutions, while once the cornerstone of many security operations, are struggling to keep pace. You might find yourself grappling with complex configurations, time-consuming integrations, heavy investments in detection engineering, and an overwhelming volume of alerts.

Multiextortion Tactics Continue to Rise

The landscape of ransomware attacks has evolved significantly in recent years, with multiextortion tactics becoming increasingly prevalent.

Data theft in ransomware cases:[2]



Late 2022:
Approximately 70% of cases

Mid-2021:
Only about 40% of cases

75% increase

in the occurrence of data theft during ransomware attacks over an 18-month period.

1. *2025 Unit 42 Global Incident Response Report*, Palo Alto Networks, February 25, 2025.
2. *2023 Unit 42 Ransomware and Extortion Report*, Palo Alto Networks Unit 42, September 28, 2025.

These challenges can leave your team feeling overwhelmed and your organization vulnerable. The siloed nature of many security tools leads to inefficient workflows, increased cognitive load for your analysts, and potential oversight of critical threats. Moreover, the lack of integration between proactive security functions (like vulnerability management) and reactive tools hampers real-time threat detection and delays incident response, putting your organization at risk.

Furthermore, relying primarily on static correlation rules and extensive detection engineering, exacerbated by the sheer volume of data, makes it difficult to identify meaningful relationships between security events across your environment, resulting in insufficient threat defense. This often leads to alerts appearing as disconnected data points, necessitating manual correlation efforts by your SOC team and leading to high false positive rates. This disjointed process hampers the effectiveness of your security infrastructure and highlights the need for more advanced and adaptive threat detection methodologies.

Quantified Impact: Real ROI from SOC Transformation

A Forrester® Consulting Total Economic Impact™ study commissioned by Palo Alto Networks examined Cortex XSIAM® deployments and found that a composite organization achieved measurable, business-critical results:[3]

257% | $5.6M | <6 months

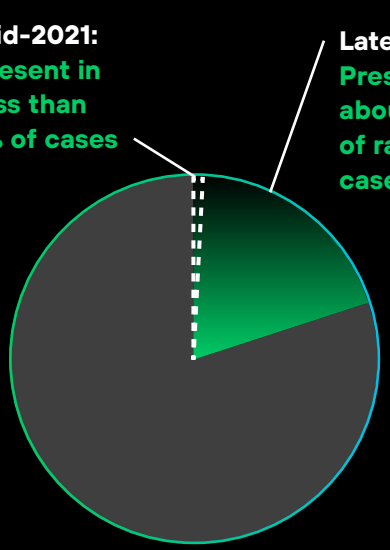
3-year ROI | Net present value | Payback period

85% | 70% | $3.1M

Reduction in MTTR | Fewer incidents requiring SOC investigation | Saved from tool consolidation

Multiextortion Tactics Continue to Rise (cont.)

Use of harassment as an extortion tactic:[4]



1,900% increase

in the use of harassment tactics by ransomware groups over the same period.

These statistics highlight a significant shift in ransomware strategies, with threat actors increasingly employing multiple pressure points to extort their victims. The dramatic rise in both data theft and harassment tactics underscores the evolving complexity and severity of ransomware threats faced by organizations.

Encryption	Data theft	DDoS	Harassment
Victims pay to regain access	Hackers threaten to release stolen data	DDoS attacks shut down public websites	Customers, business partners, and media contacted

3. *The Total Economic Impact™ Of Palo Alto Networks Cortex XSIAM*, Forrester Consulting, October 13, 2025.
4. Palo Alto Networks Unit 42, *2023 Unit 42 Ransomware and Extortion Report.*

TRANSFORMING SECURITY OPERATIONS

SOC transformation begins with Cortex® Extended Data Lake (XDL), an extensible, AI-ready foundation for platformized SecOps. Acting as the single source of truth for your SOC, Cortex XDL integrates, normalizes, and enriches all your security data.

Building on that foundation, Cortex XSIAM consolidates critical security functions into a single, transformative platform, including:

- Security information and event management (SIEM)
- Endpoint detection and response (EDR)
- Extended detection and response (XDR)
- Security orchestration, automation, and response (SOAR)
- Attack surface management (ASM)
- User and entity behavior analytics (UEBA)
- Identity threat detection and response (ITDR)
- Cloud detection and response (CDR)
- Threat Intel Management (TIM)
- Threat intelligence platform (TIP)

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

Figure 1. XSIAM Command Center

Cortex XSIAM transforms security operations by centralizing data, AI-powered defense, and automation in one platform. The XSIAM Command Center showcases a spectrum of data sources, ranging from endpoint and network to identity, cloud, application telemetry, and more, all while providing insights into the health and volume of data ingestion.

This consolidation eliminates the need for you to switch between multiple tools, reducing complexity and improving your team's efficiency. Instead of juggling various consoles and struggling with integration issues, you can manage your entire security operations from a single, coherent platform designed specifically for modern SOC needs.

Organizations deploying Cortex XSIAM have achieved measurable results. According to the Forrester Total Economic Impact™ study, a composite organization experienced an **85% reduction in alert volume requiring Tier 1 SOC attention by year three**, saving over **$930,000** in triage and Tier 1 operations. Additionally, organizations experienced a **70% reduction in cases requiring SecOps investigation** with an **85% decrease in mean time to remediation (MTTR) by year three**, valued at over **$1.2M**.[5]

The streamlined agentic AI and automation capabilities that XSIAM provides fundamentally change how you handle security incidents. The platform automates data integration, analysis, and triage, significantly reducing the manual effort required from your analysts. This automation allows your team to focus on what matters—addressing high-priority incidents that require human expertise.

The XSIAM 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.

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

The XSIAM platform ensures continuous collection, stitching, and normalization of raw data, going beyond just alerts. This empowers your SOC team with superior and simplified investigation capabilities, enabling them to identify and remediate threats faster and more effectively.

With Cortex XSIAM, you'll notice a marked improvement in your analysts' experience and productivity. The platform's AI-driven approach helps cut through the noise, reducing alert fatigue and allowing your team to concentrate on critical threats. This shift means your analysts spend less time on routine alert triage and more time developing their skills, conducting in-depth investigations, and proactively hunting for threats.

Moreover, the automation-driven approach of XSIAM accelerates incident remediation. With hundreds of tried and tested content packs in the Cortex Marketplace, plus native MCP server and client support, you can easily connect to your entire security ecosystem to integrate insights and orchestrate response. By automating previously manual tasks, embedded automation saves time and effort in responding to incidents or managing risks, such as attack surface exposures.

You have the flexibility to add, customize, or modify automations according to your specific needs. Playbooks can be scheduled, run on demand, or automatically triggered by alerts to ensure timely response and risk mitigation.

When it's time to investigate threats, Cortex Agentic Assistant puts an AI agent workforce at your command to tackle any security challenge. Embedded in XSIAM, it engages Cortex AgentiX™ agents to plan and execute advanced workflows—converting tedious manual effort into instant, expert action. Your team gains context-aware, step-by-step guidance with built-in controls, enabling them to move faster, respond decisively, and keep your business secure.

Cortex AgentiX provides persona-based AI agents grounded in real-world expertise to force multiply every member of your team. Built on more than a decade of security automation leadership, enriched with global threat intelligence, and informed by 1.2 billion executed playbooks, these agents function as always-on security experts. Analysts simply use natural language prompts, and the agents instantly plan and execute complex, multistage tasks with speed and precision.

5. Forrester Consulting, *The Total Economic Impact™*.

EVALUATING CORTEX XSIAM FOR YOUR ORGANIZATION

When considering Cortex XSIAM for your organization, it's essential to assess several key factors. First, evaluate your current security tool landscape and its complexity. If you're struggling with tool sprawl and disjointed workflows between proactive and reactive security functions, the XSIAM consolidated approach would provide significant benefits. Consider how much time your team spends switching between different tools and correlating information manually. The XSIAM unified platform dramatically reduces this overhead and improves your team's efficiency.

Second, consider the volume and variety of data your organization handles. XSIAM excels at processing and analyzing large amounts of diverse data, making it particularly well suited for organizations with complex, data-rich environments. If you're dealing with a mix of on-premises and cloud data, struggling to get a holistic view of your security posture, XSIAM can ingest and analyze data from various sources, which could be a game changer.

If you're operating in cloud or hybrid environments, the XSIAM cloud-native architecture and comprehensive visibility across on-premises and cloud assets would significantly enhance your security operations. Many organizations find that their traditional security tools struggle to provide adequate visibility and protection in cloud environments. XSIAM extends your SOC to the cloud, ensuring unified visibility and security operations across your entire infrastructure.

Third, review compliance requirements, which are another crucial factor. The robust reporting capabilities and comprehensive data analysis in XSIAM can help you meet various regulatory standards more effectively. Consider how much time your team currently spends on compliance reporting and how XSIAM could streamline this process.

Compared to traditional SIEM and other security platforms, XSIAM offers improved threat detection capabilities through its AI-driven approach. You'll likely see a reduction in operational complexity and potentially significant cost savings due to consolidated tooling and improved efficiency. When assessing ROI, consider not just the direct costs but also the value of freed-up analyst time and improved security posture. Think about how much faster your team could detect and respond to threats with the XSIAM automated triage and response capabilities.

The Forrester Consulting Total Economic Impact™ study documented real-world financial outcomes. The research found that organizations achieved **257% ROI over three years** with **less than six months payback period**. As one VP of global security reported in the study: "Mean time to detect and remediate dropped by over 80%. What used to take four hours to detect and two hours to remediate now takes 40–50 minutes total."[6]

> "Cortex XSIAM has transformed our security operations the way our previous SIEM could not. XSIAM has enabled automation and orchestration to our detection, investigation, and response workflows—which has been a massive improvement over the productivity and the security posture for LOLC.
>
> – Prasanna Siriwardena
> Chief Information Officer, LOLC Holdings PLC

6. Forrester Consulting, *The Total Economic Impact™*.

See the Improvements XSIAM Delivers Beyond SIEM Solutions Alone

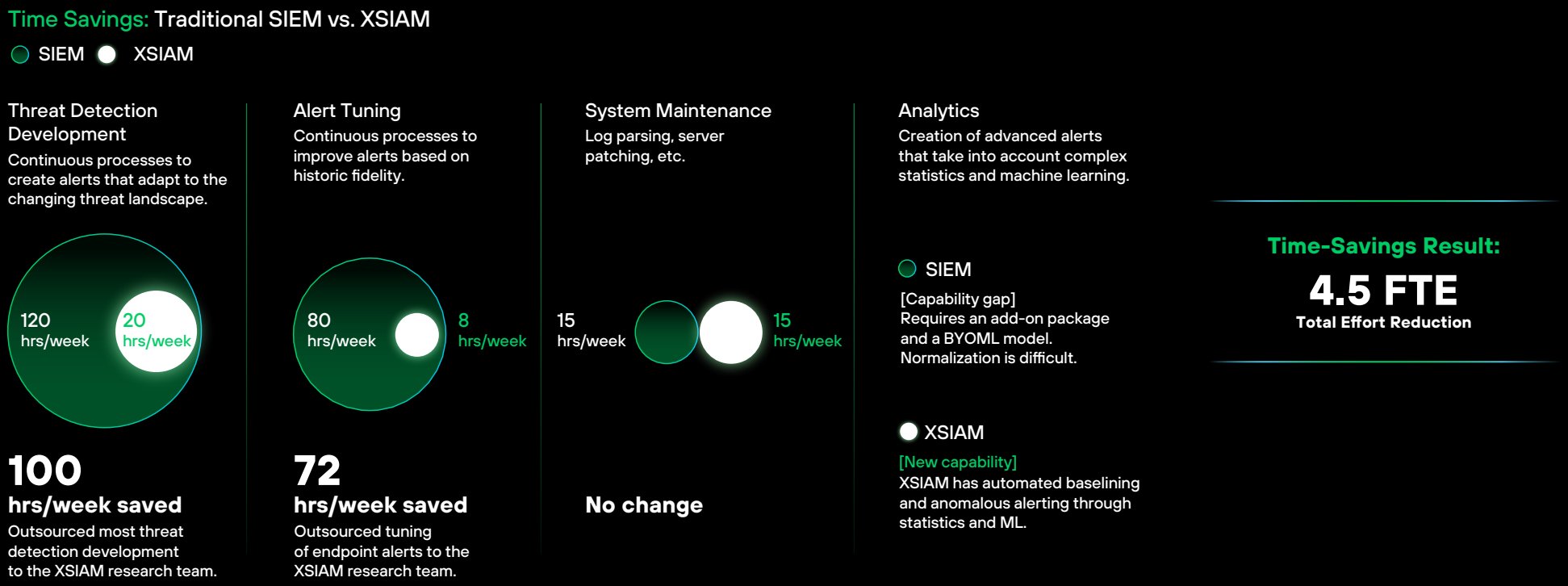


Figure 2. Time savings between traditional SIEM and XSIAM

Before adopting XSIAM, assess your organization's readiness for AI-driven security operations. Consider your team's current skills and processes, and be prepared for a shift in how you approach security operations.

While XSIAM can significantly improve your security operations, it might require some adjustment in how your team works. Consider the training and change management aspects of adopting a new, AI-driven platform.

FUTURE-PROOFING YOUR SECURITY OPERATIONS

Cortex XSIAM plays a crucial role in evolving security paradigms such as zero trust, secure access service edge (SASE), and security service edge (SSE). Its comprehensive visibility and advanced analytics capabilities align well with these modern security approaches, helping you future-proof your security operations. As you move toward a zero trust architecture, XSIAM provides deep insights into user and entity behavior that can help you implement and maintain a robust zero trust model.

The platform unifies reactive incident response with proactive security posture management. It addresses the two most critical risk areas for enterprises by providing:

- **Cortex Exposure Management:** Cut vulnerability noise by up to 99% with AI-driven prioritization and automated remediation spanning the enterprise and cloud. This disruptive approach focuses on the vulnerabilities with active weaponized exploits and no compensating controls, allowing you to prioritize the critical 0.01% of threats that matter.
- **Cortex Email Analytics:** Stop advanced phishing attempts and email-based attacks with LLM-driven analytics merged with industry-leading detection and response. With email remaining the primary communication tool—projected to reach 5 billion users by 2030[7]—and the top target for cyberattacks, this capability automatically removes malicious emails, disables compromised accounts, and isolates affected endpoints in real time.

As your organization grows and threats evolve, XSIAM scalability ensures it can handle increasing data volumes and adapt to new types of threats. The platform's AI models and detectors are continuously updated, providing the latest threat intelligence and detection capabilities without requiring manual updates from your team. This means you're always protected against the latest threats, without the need for constant manual tuning and updating of your security tools.

XSIAM learns from manual analyst actions and provides recommendations for future automations. This enhances the platform's ability to automatically resolve incidents and improve efficiency and accuracy over time, enabling you and your organization's security posture to improve every day.

XSIAM leverages mature security-specific ML data models, which automatically normalize and stitch vast amounts of data from various sources to detect security threats. These models are built based on learned behavior from tens of thousands of environments, helping to differentiate between anomalous and malicious behaviors. This significantly reduces false positives and improves detection and prevention capabilities, stopping attacks before they become security incidents.

Moreover, with XSIAM Bring Your Own Machine Learning (BYOML), you can integrate your own ML tools into the platform. This enables you to leverage the power of ML to hunt for threats using centralized and normalized data within XSIAM, further enhancing your ability to detect and respond to sophisticated threats.

Financial Impact of Consolidation

According to *The Total Economic Impact™ Of Palo Alto Networks Cortex XSIAM* by Forrester Consulting:[8]

$3.1M
saved eliminating 20+ legacy tools (3-year total)

$2.2M
value from 60% improved security posture

$5.6M
net present value over 3 years

By adopting XSIAM, you're both solving today's security challenges and positioning your organization to meet the cybersecurity needs of tomorrow. This forward-looking approach can give you confidence in your ability to protect your organization against an ever-evolving threat landscape. As new types of threats emerge and your organization's IT infrastructure needs to mature to meet demands, XSIAM delivers a flexible, AI-driven approach that ensures your security operations can adapt and respond effectively.

XSIAM enables SOC teams and the security posture of the organization to improve each day.

Perhaps most importantly, XSIAM offers continuous improvement through AI and machine learning. The platform regularly refines its detection and response capabilities based on new data and emerging attack techniques. This means your security operations become more effective over time, adapting to new threats and patterns without constant manual tuning.

7. *Email Statistics Report 2025-2030*, cloudHQ, April 24, 2025.
8. Forrester Consulting, *The Total Economic Impact™*.

IMPROVE YOUR CRITICAL SOC METRICS

Cortex XSIAM offers a revolutionary approach to slash your mean time to detect (MTTD) and mean time to respond (MTTR), dramatically enhancing your security operations. By leveraging advanced AI and machine learning, XSIAM automates the tedious task of data integration and analysis, enabling your team to identify threats in near-real time. This means you can spot potential breaches faster than ever before, often catching attackers before they can cause significant damage to your organization.

But detection is only half the battle. The XSIAM automation-first approach accelerates your incident response, turning hours of manual investigation into minutes of automated action.

Imagine your SOC team no longer bogged down by manual triage activities or spending precious time correlating data from disparate sources. Instead, empower your analysts to focus on what matters with AI-driven incident scoring and intelligent alert grouping from XSIAM.

Our unified approach to reactive and proactive security means you can both respond to incidents faster and prevent many of them from occurring in the first place. By integrating Exposure Management and Email Analytics directly into the SOC platform, XSIAM addresses two of the most common attack vectors with the same unified data, AI, and automation.

You'll see a dramatic reduction in MTTR as your team leverages advanced playbooks and Cortex AgentiX agents, allowing for swift and decisive action against threats. Perhaps most importantly, XSIAM continually learns and adapts to your environment, ensuring your security posture improves over time. As you face new and emerging threats, the XSIAM cutting-edge AI models continuously evolve, keeping you one step ahead of potential adversaries.

This means you're improving your MTTD and MTTR today, as well as future-proofing your security operations for the challenges of tomorrow. With Cortex XSIAM, you can confidently navigate the complex cybersecurity landscape, knowing that your critical SOC metrics are continuously optimized to protect your organization's most valuable assets.

Research shows evidence of these improvements. For one specialty retailer, alerts dropped from **25,000 to 4,500 per quarter**, according to their Director of SecOps. The study documented that for the composite organization based on interviewed customers, deployment required **three FTEs over two months**, with only **0.5 FTE for ongoing annual maintenance**.[9]

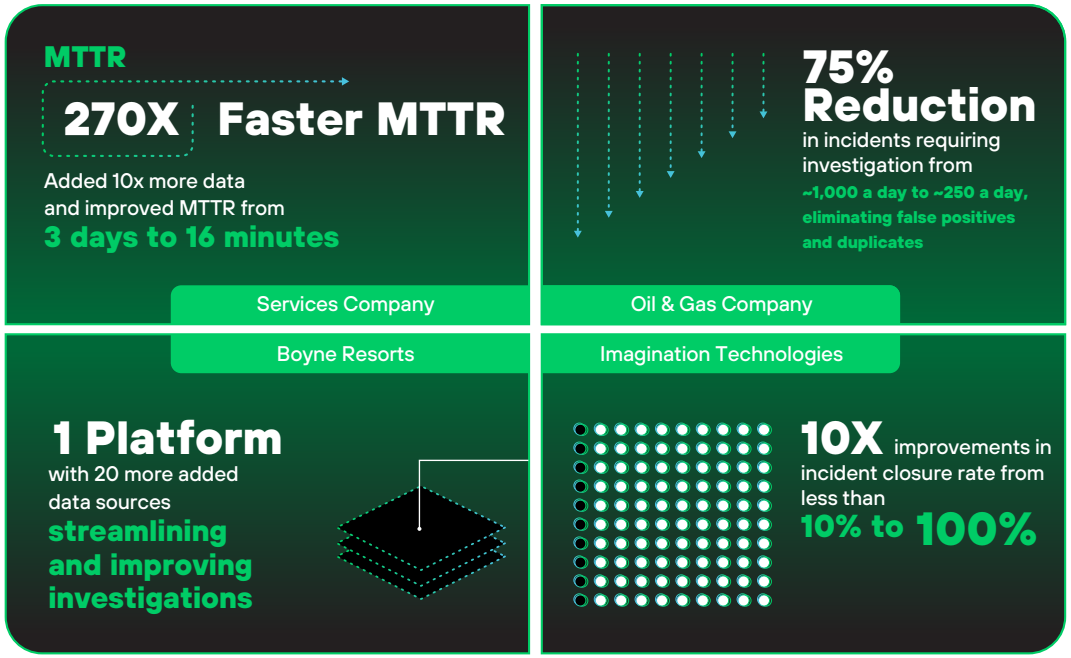


Figure 3. Examples of how customers measurably made improvements using XSIAM

> "We view XSIAM as the next frontier in moving towards a next-generation SOC as it integrates various features in a single unified platform. With XSIAM, we expect greater automation and greater empowerment to our Cyber Operations team.
>
> – Rob Jillson
> Head of Cybersecurity, Resolution Life Australasia

9. Forrester Consulting, *The Total Economic Impact™*.

IS CORTEX XSIAM THE RIGHT SOLUTION FOR YOU?

1. **Current SOC Challenges**
   - ☐ Are you struggling with complex configurations in your current SIEM?
   - ☐ Do you face time-consuming integrations between security tools?
   - ☐ Is your team overwhelmed by a high volume of alerts?
   - ☐ Do you have inefficient workflows due to siloed security tools?
   - ☐ Is there a disconnect between your proactive security functions and reactive incident response?

2. **Threat Detection and Response**
   - ☐ Are you relying heavily on static correlation rules?
   - ☐ Do you need to improve real-time threat detection?
   - ☐ Is your incident response process delayed due to a lack of integration?
   - ☐ Do you struggle with high false-positive rates?

3. **Data Management**
   - ☐ Do you handle large volumes of diverse security data?
   - ☐ Are you dealing with a mix of on-premises and cloud data?
   - ☐ Do you need better data normalization and correlation capabilities?

4. **AI and Automation Needs**
   - ☐ Are you looking to leverage AI for improved threat detection?
   - ☐ Do you want to automate routine security tasks?
   - ☐ Is reducing manual effort in incident triage a priority?
   - ☐ Do you need AI-driven vulnerability prioritization to cut through the noise?

5. **Unified Platform Requirements**
   - ☐ Do you need to consolidate multiple security functions, such as SIEM, EDR, XDR, SOAR, vulnerability management, and email security?
   - ☐ Are you looking to manage security operations from a single platform?
   - ☐ Do you want to bridge the gap between proactive and reactive security?

6. **Cloud and Hybrid Environment**
   - ☐ Are you operating in cloud or hybrid environments?
   - ☐ Do you need better visibility across on-premises and cloud assets?

7. **Compliance and Reporting**
   - ☐ Do you need to streamline compliance reporting processes?
   - ☐ Are you looking for more comprehensive data analysis for regulatory standards?

8. **Scalability**
   - ☐ Is your organization growing, requiring the handling of increasing data volumes?
   - ☐ Do you need a solution that can adapt to evolving threats?

9. **Advanced Analytics**
   - ☐ Are you interested in AI-driven incident scoring and alert grouping?
   - ☐ Do you need better correlation of events across various data sources?
   - ☐ Do you want to use AI to prioritize the most critical vulnerabilities?

10. **Team Readiness**
    - ☐ Is your team prepared to adapt to AI-driven security operations?
    - ☐ Are you willing to invest in training for a new, advanced platform?

11. **Future-Proofing**
    - ☐ Are you moving toward zero trust, SASE, or SSE security models?
    - ☐ Do you need a solution that continuously improves through AI and ML?

12. **Custom ML Integration**
    - ☐ Are you interested in integrating your own machine learning tools?

13. **Email and Vulnerability Management**
    - ☐ Do you need better protection against advanced email threats?
    - ☐ Are you struggling with vulnerability backlogs and prioritization?
    - ☐ Would you benefit from automated remediation of critical vulnerabilities?

If you answered "**yes**" to most of these questions, especially in areas that align with your organization's specific security challenges and goals, Cortex XSIAM would be a suitable solution for your SOC.

Get Started Today

Discover how Cortex XSIAM can help you and your organization simplify operations, unify proactive and reactive security, stop threats at scale, and accelerate incident remediation—today and in the future.

CONTACT US →

About Cortex XSIAM

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.

Cortex XSIAM unifies best-in-class security operations functions, including EDR, XDR, SOAR, ASM, UEBA, TIP, and SIEM. XSIAM centralizes all of your security data and uses machine learning data models designed specifically for security. With XSIAM, automate data integration, analysis, and response actions, enabling analysts to focus on the incidents that matter. To learn more about Cortex XSIAM, visit www.paloaltonetworks.com/cortex/cortex-xsiam.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main	+1.408.753.4000
Sales	+1.866.320.4788
Support	+1.866.898.9087

cortex_ebook_cortex-xsiam-buyers-guide_102125