

Healthcare XSIAM Buyer's Guide

Transforming Your SOC to Help Secure
Patient Care in the AI Era



Table of Contents

Bridging the Gap: Proactive Prevention in Modern SOCs	3
Transforming Healthcare Security Operations	7
Evaluating XSIAM for Your Healthcare Organization	10
Future-proofing Your Security Operations	12
Improving Your Critical SOC Metrics	15
Is XSIAM the Right Solution for You?	17
Get Started Today	19

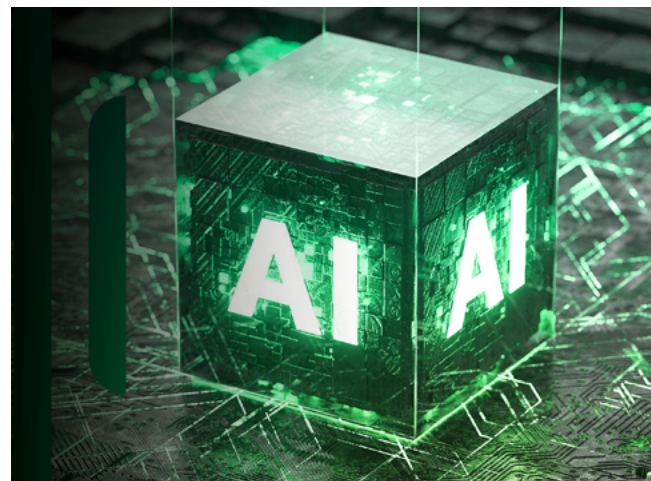
Bridging the Gap: Proactive Prevention in Modern SOC

In healthcare today, how you handle cybersecurity has a direct impact on how patients, clinicians, and hospitals share and receive care. Bad actors understand that care from anywhere is the new normal, from telehealth appointments to hospitals. And they know they can cash in on this expansive attack surface using sophisticated tactics and AI. The fact that legacy security solutions are no match for their methods only fuels their success.

As a healthcare 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 ago¹—and security 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 impacts patient care? This gap between postincident analysis and proactive prevention is at the heart of the evolving needs of modern SOC.

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.



1. 2025 Unit 42 Global Incident Response Report, Palo Alto Networks, February 25, 2025.

#1 ranked U.S. critical infrastructure sector for combined total of ransomware and data theft attacks.²

Given healthcare's status as a prime target, ransomware defenses must go beyond traditional prevention:

- **Ransomware-as-a-Service (RaaS)** detection to identify and stop emerging, subscription-based attack models.
- **Backup system protection and monitoring** to protect recovery data from compromise or encryption during an attack.
- **Business continuity planning** to maintain critical care operations even when ransomware attempts to disrupt systems.

77% of healthcare practitioners rated threat prevention the most critical capability when considering Internet of Medical Things (IoMT) security.³

20% yearly increase in SaaS adoption within the healthcare industry.⁴

2. [Internet Crime Report 2024](#), Federal Bureau of Investigation.

3. [Ibid.](#)

4. [Healthcare Software As A Service Market Summary](#), Grandview Research.

The siloed nature of many security tools can lead to challenges in providing secure “work from anywhere” and “care from anywhere” architectures that are pivotal to healthcare operations. Moreover, the lack of integration between proactive security functions (like vulnerability management) and reactive tools can hamper 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. Ultimately, this results 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. The disjointed process hampers the effectiveness of your security infrastructure and highlights the need for more advanced and adaptive threat detection methodologies.

Traditional SIEM struggles with healthcare's requirements



Clinical Workflow Disruption: Complex configurations and time-consuming integrations often interfere with clinical operations, creating security solutions that healthcare staff work around rather than with.



Medical Device Blind Spots: Traditional SIEM solutions often can't properly monitor or integrate with medical devices, leaving critical gaps in visibility across IoMT infrastructure.



Compliance Complexity: Healthcare organizations must navigate HIPAA, HITECH, and state-specific regulations while maintaining operational efficiency—something traditional tools can make increasingly difficult.



Alert Overwhelm in Critical Environments: Healthcare SOCs are overwhelmed by alerts while operating in environments where false positives can lead to dangerous “alert fatigue” that can cause real threats to be missed.

Healthcare security team challenges don't exist in isolation—they're part of a broader transformation across the industry.

Key Trends Impacting the State of Security for Healthcare Providers

1 Accelerating Digital Transformation

Healthcare providers are streamlining and optimizing clinical and IT workflows through advanced analytics and increased adoption of cloud-based technologies. With the shift to hybrid work and digital care models, remote access security is essential to safeguarding sensitive health information.

2 Improving Patient Experience

The expansion of remote patient monitoring, patient portals, and telehealth services enhances accessibility but widens the attack surface. Secure integration of [IoT and IoMT devices](#) is critical in protecting connected care environments.

3 Complying with Regulatory Requirements

Regulatory frameworks such as HIPAA and GDPR demand robust data privacy and security measures. Healthcare providers must balance compliance with the cost of adherence.

4 Enabling Data-Driven Personalized Healthcare

The use of AI/ML and advanced analytics supports population health management and evidence-based care. However, increased data sharing and cloud adoption introduce new attack surfaces that require proactive defense. As consolidation accelerates, organizations need secure onboarding of M&A assets and protection of intellectual property to help prevent data leakage and fortify operational resilience.

Transforming Healthcare Security Operations

Cortex XSIAM® offers a unified front-end and back-end platform that simplifies and accelerates security operations. For healthcare organizations, this means uninterrupted, secure care—anytime, anywhere. Through the power of platformization, we can help healthcare providers replace fragmented point solutions with an integrated, intelligent approach to cybersecurity. The result is stronger protection, reduced complexity, and enhanced resilience across the entire care delivery ecosystem.

- Security information and event management (SIEM)
- Security orchestration, automation, and response (SOAR)
- AI-ready security data lake
- Extended detection and response (XDR)
- Cloud detection and response (CDR)
- Network detection and response (NDR)
- Identity threat detection and response (ITDR)
- Exposure management
- Email security
- 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 (Healthcare Services)

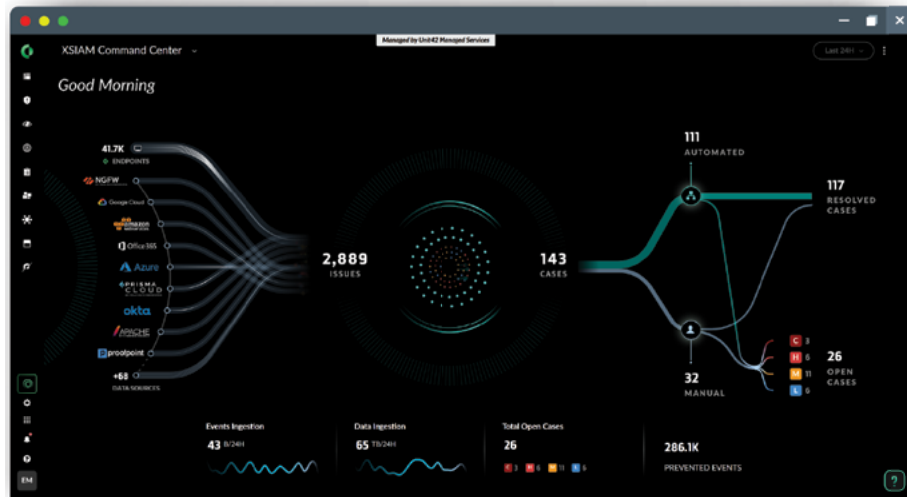


Figure 1. XSIAM Command Center

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.



With the introduction of XSIAM 3.0, the platform now bridges the gap between reactive and proactive security by adding native exposure management and email analytics capabilities that leverage the power of unified data, AI, and automation.

This consolidation eliminates the need for you to switch between multiple tools, reducing complexity and improving your healthcare 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.

The streamlined workflows and automation capabilities that XSIAM provides can fundamentally change how you handle security incidents and patient care continuity. 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—including clinical systems, IoMT, and administrative networks. This offers a comprehensive overview of incidents and risks in a single location. You can move beyond chasing a flood of individual alerts as XSIAM automatically takes raw telemetry, stitches it together to pinpoint stealthy threats, and uses [SmartGrouping](#) to consolidate all related activity into high-fidelity cases. This empowers your security team to stop analyzing fragmented alerts and start focusing on full-scope incidents, dramatically improving efficiency and building far greater resilience against even the most sophisticated attacks.

This intelligence and automation are crucial for modern security success. By handling the manual, low-level tasks, XSIAM gives your analysts back their time, allowing them to focus on high-value activities like proactive threat hunting and in-depth investigations. [Cortex XSIAM provides the rich, correlated data and context](#) your team needs to effortlessly uncover hidden threats that might evade traditional detection methods.

With 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 to patient safety. 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, you can optimize processes and interactions across your 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.

You have the flexibility to add, customize, or modify automations according to your 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.



With 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.

Evaluating XSIAM for Your Healthcare Organization

When considering XSIAM for your organization, it's essential to assess several key factors.

1. Evaluate your current security tool landscape and its complexity.

Consider how much time your team spends switching between different tools and correlating information manually. If you're struggling with tool sprawl and disjointed workflows between proactive and reactive security functions, consolidation provides significant benefits. The XSIAM unified platform can dramatically reduce overhead and improve your team's efficiency.

2. Consider your volume and unique data streams. Healthcare organizations generate an immense volume of highly diverse data—from clinical systems, medical devices, and operational applications to administrative workflows and research environments. This includes EHR audit logs, imaging system activity, connected medical device telemetry, lab system data, pharmacy transaction records, patient portal access logs, and identity management events. XSIAM is purpose-built to process and analyze these complex, high-volume data streams at scale. Whether data resides on-premises, in the cloud, or in hybrid environments, XSIAM can ingest it into a unified platform—correlating security events across silos and delivering real-time visibility into your enterprise-wide risk posture. For healthcare delivery organizations seeking to replace manual investigation and fragmented tools, XSIAM provides a game-changing foundation for intelligent, proactive cyber defense.

3. Examine the challenges you face with regulatory compliance.

From HIPAA and HITECH to evolving security requirements for connected medical devices, the ability to produce accurate, timely, and auditable reports is essential. XSIAM delivers robust reporting, advanced analytics, and built-in compliance support to help healthcare organizations streamline evidence gathering, reduce manual workloads, and accelerate audit response times.

Beyond regulatory compliance, XSIAM also supports cyber insurance readiness by delivering the visibility, telemetry, and incident response capabilities insurers increasingly demand. With centralized logging, automated correlation, and continuous monitoring across cloud, network, endpoint, and identity systems, XSIAM enables healthcare security teams to demonstrate due diligence, reduce risk exposure, and meet insurer expectations more effectively—helping secure both patient trust and organizational resilience.

Time Savings: Traditional SIEM vs. XSIAM

○ SIEM ● XSIAM

Threat Detection Development

Continuous processes to create alerts that adapt to the changing threat landscape.

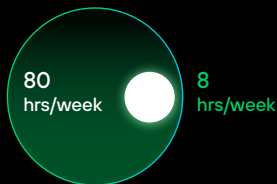


100
hrs/week saved

Outsourced most threat detection development to the XSIAM research team.

Alert Tuning

Continuous processes to improve alerts based on historic fidelity.



72
hrs/week saved

Outsourced tuning of endpoint alerts to the XSIAM research team.

System Maintenance

Log parsing, server patching, etc.



No change

Analytics

Creation of advanced alerts that take into account complex statistics and machine learning.

○ SIEM

[Capability gap]
Requires an add-on package and a BYOML model. Normalization is difficult.

● XSIAM

[New capability]
XSIAM has automated baselining and anomalous alerting through statistics and ML.

Time-Savings Result:

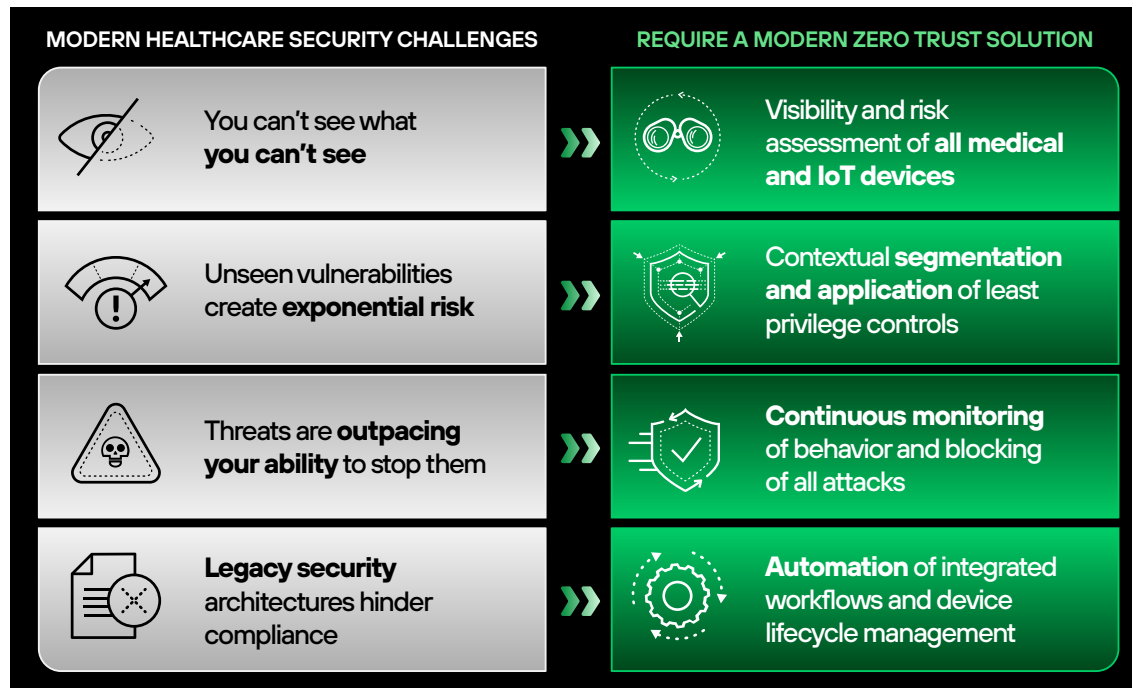
4.5 FTE
Total Effort Reduction

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 adjustments in how your team works. Contemplate the training and change management aspects of adopting a new AI-driven platform.

Future-proofing Your Security Operations

Healthcare organizations are at the forefront of digital transformation, making future-proofing security operations critical for long-term patient care delivery. XSIAM plays a crucial role in evolving healthcare 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 towards 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.





With XSIAM 3.0, the platform now unifies reactive incident response with proactive security posture management. It addresses two critical risk areas 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 2030⁵—and the top target for cyberattacks, this capability automatically removes malicious emails, disables compromised accounts, and isolates affected endpoints in real time.

As threats evolve and healthcare organizations move patient portals, telehealth platforms, and clinical applications to the cloud, XSIAM establishes unified security visibility across hybrid healthcare environments. XSIAM scalability allows it to 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 receiving protection against the latest threats, without the need for constant manual tuning and updating of your security tools.

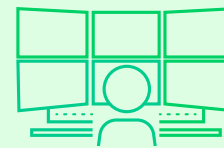
XSIAM learns from manual analyst actions and provides recommendations for future automations. This enhances the platform's ability to automatically resolve incidents and improve efficiency and accuracy over time, enabling you and your organization's security posture to improve every day.

5. Global Incident Response Report, Palo Alto Networks, February 25, 2025

Palo Alto Networks Cortex XSIAM, the AI-driven platform, 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 truly malicious behaviors. This significantly reduces false positives and improves detection and prevention capabilities, stopping attacks before they become security incidents.

Moreover, the [XSIAM Bring Your Own Machine Learning \(BYOML\)](#) capability allows you to integrate your own machine learning 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.

By adopting XSIAM, you're not just solving today's security challenges—you're 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's flexible, AI-driven approach aligns with healthcare's increasing adoption of artificial intelligence in clinical decision-making, enabling security to keep pace with healthcare innovation.



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

Perhaps most importantly, XSIAM offers continuous improvement through AI-powered machine learning.

Improving 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.

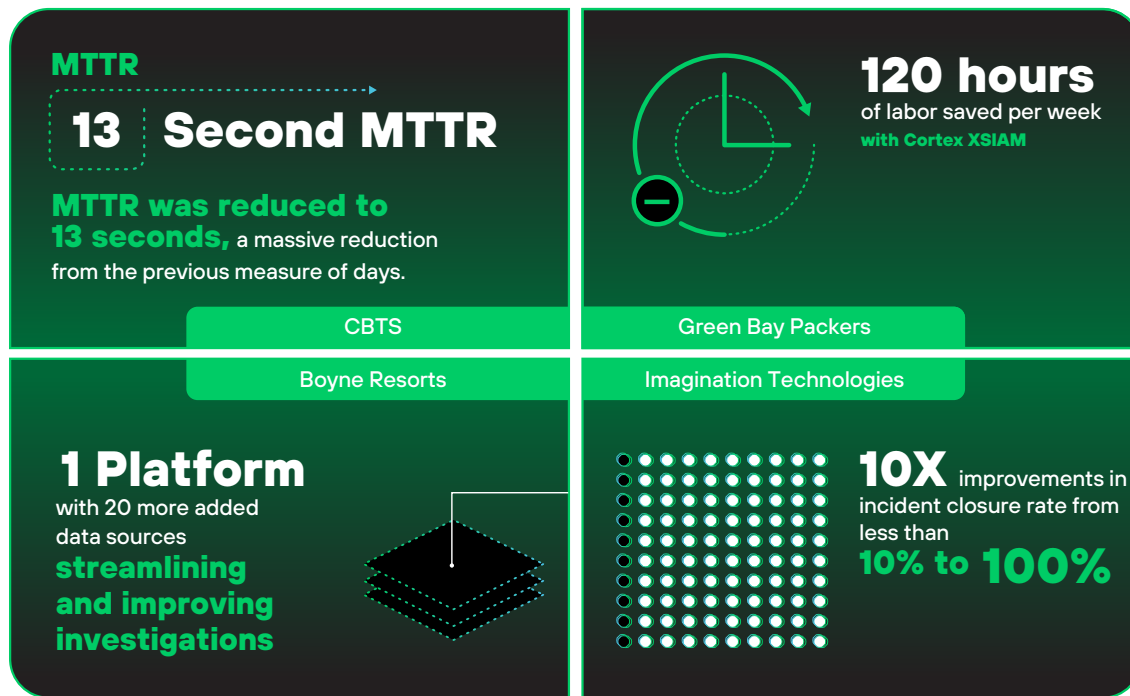
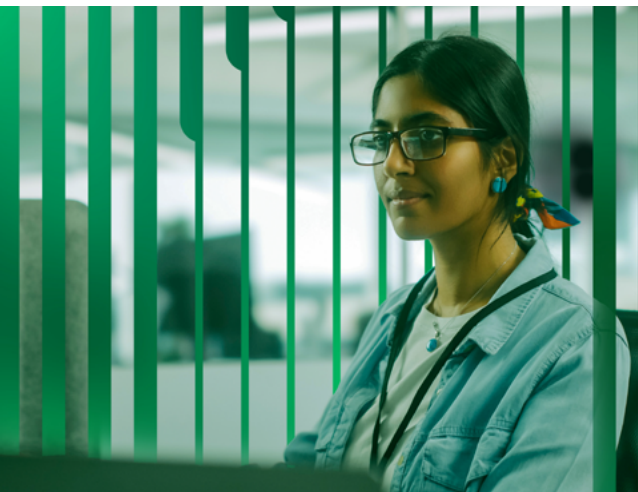


Figure 3. Examples of how customers measurably made improvements using XSIAM

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 case grouping, SmartGrouping, and case scoring, [SmartScore](#), from XSIAM. The platform's 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 3.0 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 automated playbooks and orchestrated workflows, 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 Precision AI models continuously evolve, keeping you one step ahead of potential adversaries. This means you're both improving your MTTD and MTTR today and 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.

“Because of the consistency and high percentage of true positives we get from the Palo Alto Networks platform, we have the confidence now to automate threat mitigation. That’s something we’ve never had the opportunity to do until now.”

– Joel Pfeifer, Principal Security Analyst,
HealthPartners

Is XSIAM the Right Solution for You?

1. Current SOC Challenges

- Do your security tools disrupt clinical workflows?
- 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 lack of integration?
- Do you struggle with high false-positive rates?
- Are there blind spots in your medical device infrastructure?

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?
- Do you need automated response that won't disrupt patient care?
- Do you want access to AI-driven scoring prioritized by patient care impact?

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?
- Are you in need of data correlation across EHRs, medical devices, and IT infrastructure?

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 for HIPAA and similar regulations?
- Are you looking for more comprehensive data analysis for regulatory standards?

8. Scalability

- Is your organization growing, requiring 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 (BYOML)?

13. 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?



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

Get Started Today

Discover how Cortex XSIAM helps you deliver uninterrupted care from anywhere. Our best-of-breed platform approach reduces the security gaps that come with using multiple point solutions. It provides continuous healthcare security with fewer resources for oversight and training, enabling patients, clinicians, and hospitals to share and receive care anywhere.

[Request a Demo](#)

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. 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.



**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

© 2026 Palo Alto Networks, Inc. A list of our trademarks in the United States and other jurisdictions can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies.

[cortex_eb_Healthcare_XSIAM_Buyer's_Guide_020226](#)