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 3

Transforming Security Operations 6

Evaluating XSIAM for Your Organization 9

Future-Proofing Your Security Operations 12

Improve Your Critical SOC Metrics 14

Is XSIAM the Right Solution for You? 16

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 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 and regulatory requirements are becoming increasingly stringent.

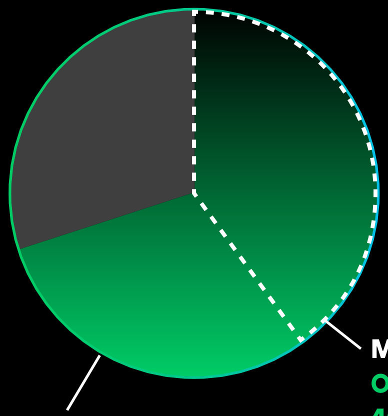
Every time a breach occurs, your security team can likely piece together what happened after the fact—how the system was compromised, which systems were involved, and what data was exfiltrated. This begs the question: if you have the information to understand an incident post breach, why can't you prevent or stop it before it happens? This gap between post incident 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 may 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. According to the 2023 Unit 42® Ransomware and Extortion Report:

Data theft in ransomware cases:



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.

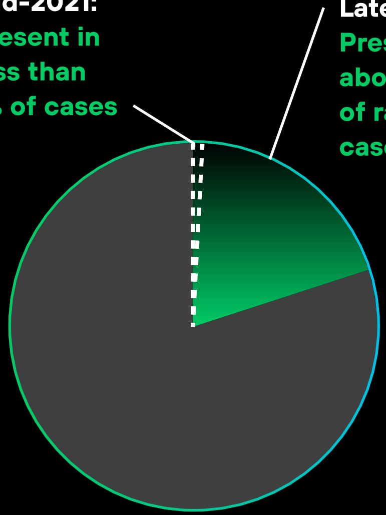
These challenges can leave your team feeling overwhelmed and your organization vulnerable. The siloed nature of many security tools leads to inefficient workflows, increased cognitive load for your analysts, and potential oversight of critical threats. Moreover, the lack of integration between tools 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.

Multiextortion Tactics Continue to Rise (cont.)

Use of harassment as an extortion tatic:



Mid-2021:
Present in less than 1% of cases

Late 2022:
Present in about 20% of ransomware cases

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.

Victims pay to regain access
Encryption

Hackers threaten to release stolen data
Data theft

DDosS attacks shut down public websites
DDoS

Customers, business partners, and media contacted
Harassment

TRANSFORMING SECURITY OPERATIONS

Cortex XSIAM® offers a transformative approach to address these challenges. By consolidating critical security functions such as SIEM, EDR, XDR, SOAR, ASM, UEBA, ITDR, CDR, and TIP into a single, unified front-end and back-end, XSIAM streamlines your security operations.

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.

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

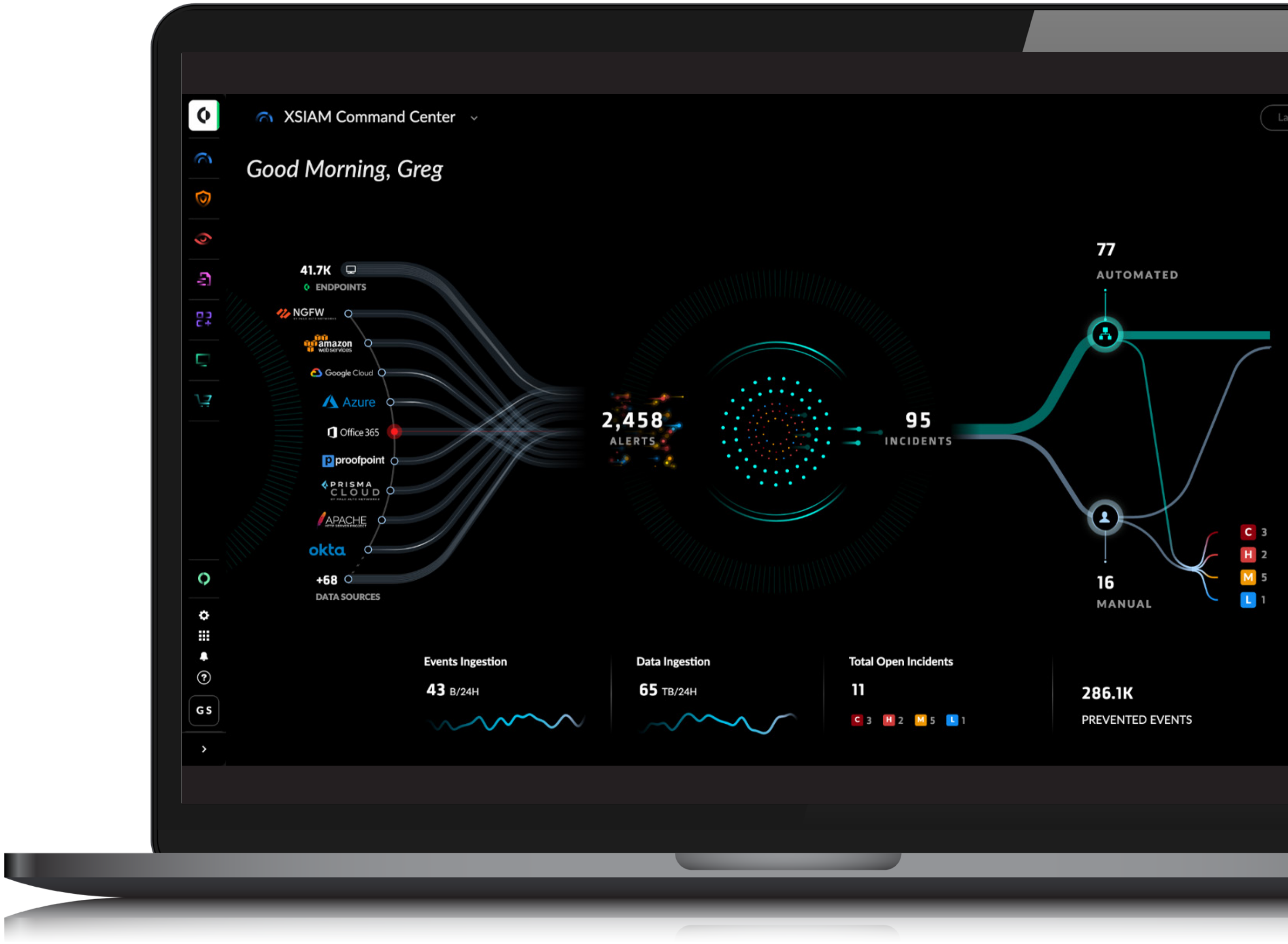


Figure 1: XSIAM Command Center

Cortex XSIAM transforms security operations by centralizing data, AI-powered defense, and automation in one platform. Here's the XSIAM Command Center showcasing 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.

XSIAM's streamlined workflows and automation capabilities 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. XSIAM's 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 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 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, XSIAM's automation-driven approach 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 ORGANIZATION

When considering 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, XSIAM's consolidated approach could provide significant benefits. Consider how much time your team spends switching between different tools and correlating information manually. XSIAM's unified platform could dramatically reduce this overhead and improve your team's efficiency.

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's ability to ingest and analyze data from various sources could be a game-changer.

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

Compliance requirements are another crucial factor. XSIAM's robust reporting capabilities and comprehensive data analysis 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 XSIAM's automated triage and response capabilities.

> “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

See the improvements XSIAM delivers beyond SIEM solutions alone:

Time Savings: Traditional SIEM vs XSIAM

● SIEM ○ XSIAM

Threat Detection Development

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

Alert Tuning

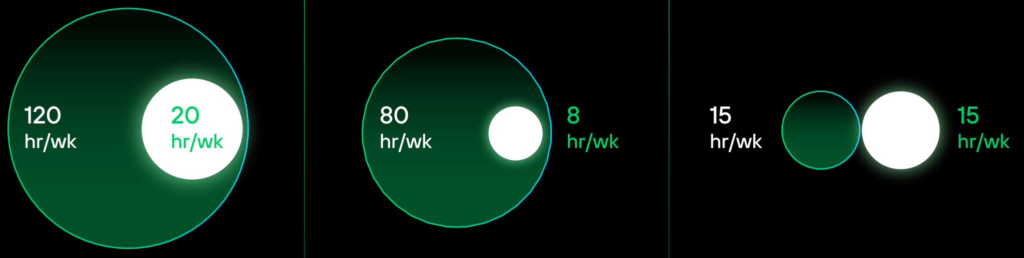
Continuous processes to improve alerts based on historic fidelity.

System Maintenance

Log parsing, server patching, etc.

Analytics

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



100
hr/week saved

Outsourced most threat detection development to XSIAM research team.

72
hr/week saved

Outsourced tuning of endpoint alerts to XSIAM research team.

No change

● SIEM

[Capability gap]
Requires add-on package and building your own machine learning 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

Figure 2: Time savings between traditional SIEM and XSIAM

Before adopting XSIAM, it's important to 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 may 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

XSIAM plays a crucial role in evolving security paradigms such as Zero Trust, SASE, and 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's ability to provide deep insights into user and entity behavior can help you implement and maintain a robust Zero Trust model.

As your organization grows and threats evolve, XSIAM's 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 you with 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, enhancing its ability to automatically resolve incidents and improving efficiency and accuracy over time, enabling you and your organization's security posture to improve every day.

Powered by Palo Alto Networks Precision AI™, 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 truly malicious behaviors. This significantly reduces false positives and improves detection and prevention capabilities, stopping attacks before they become security incidents.

Moreover, XSIAM's bring-your-own ML (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 ensures that your security operations can adapt and respond effectively.

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

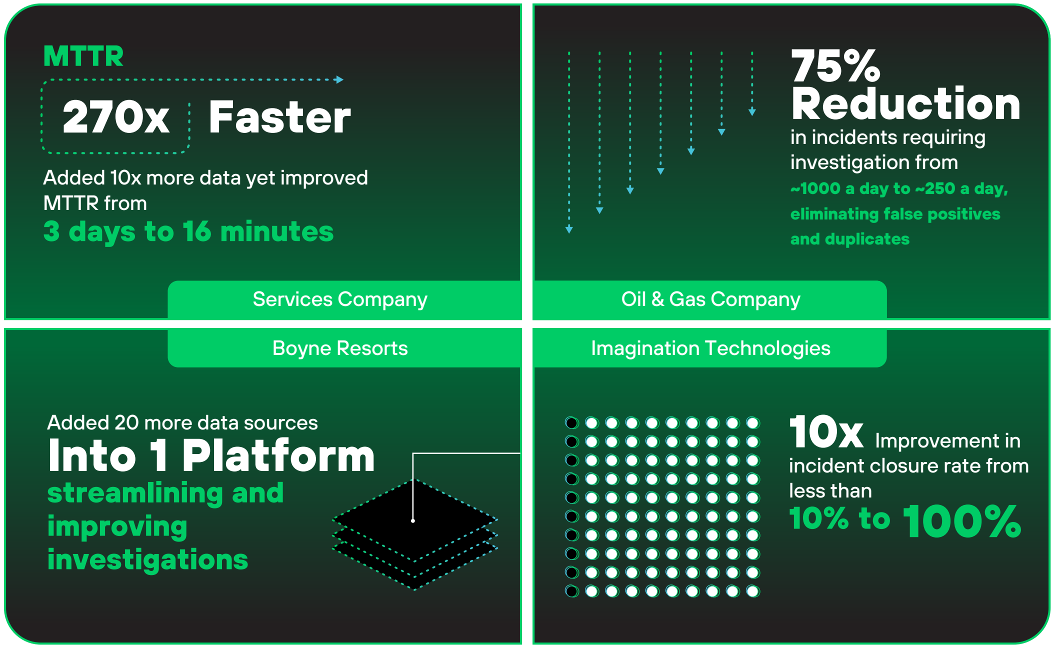
Perhaps most importantly, XSIAM offers continuous improvement through AI and machine learning. The platform regularly refines its detection and response capabilities based on new data and emerging attack techniques. This means your security operations become more effective over time, adapting to new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

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. XSIAM's 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, XSIAM's AI-driven incident scoring and intelligent alert grouping empower your analysts to focus on what truly matters. 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 that your security posture improves over time. As you face new and emerging threats, XSIAM's cutting-edge Precision AI models evolve, keeping you one step ahead of potential adversaries. This means you're not just improving your MTTD and MTTR today—you're 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.



MTTR

270x Faster

Added 10x more data yet improved MTTR from

3 days to 16 minutes

Services Company

75% Reduction

in incidents requiring investigation from

~1000 a day to ~250 a day, eliminating false positives and duplicates

Oil & Gas Company

Boyne Resorts

Added 20 more data sources

Into 1 Platform

streamlining and improving investigations

Imagination Technologies

10x Improvement in incident closure rate from less than

10% to 100%

Figure 3: Examples of how customers measurably improved their MTTR and more.

> “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 Australia

IS 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?

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?

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?

5. **Unified Platform Requirements**
   - □ Do you need to consolidate multiple security functions (SIEM, EDR, XDR, SOAR, etc.)?
   - □ Are you looking to manage security operations from a single platform?

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 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?

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)?

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

Contact us to discover how Cortex XSIAM can help you and your organization simplify operations, stop threats at scale, and accelerate incident remediation today and in the future.

3000 Tannery Way
Santa Clara, CA 95054

Main	+1.408.753.4000
Sales	+1.866.320.4788
Support	+1.866.898.9087

cortex_ebook_xsiam-buyers-guide_121024