paloalto NETWORKS

# Leading the charge –

## AI-driven SOC transformation with Palo Alto Networks and Orange Cyberdefense

orange™ Cyberdefense

# Introduction

## The future of Security Operations Centers – smarter, faster, stronger

Security Operations Centers, or ‘SOCs, have been evolving since the 1980s, steadily adapting to new threats and technologies. But today’s cyber landscape is different. The explosion of AI-driven services, skyrocketing data volumes, and an unprecedented surge in sophisticated cyber threats demand a radical shift. The old way of running security operations simply can’t keep up.

With cyber and physical battlefields converging, the stakes have never been higher. Attackers are faster, more organized, and leveraging AI just like we are. If SOCs don’t transform now, businesses risk falling behind - and becoming easy targets.

## Our vision for the SOC of the future – smarter, faster, always on

The future of SOCs is here, and it’s driven by AI. With ultra-fast, automated defenses, Palo Alto Networks and Orange Cyberdefense are working together to transform the way businesses detect, respond to, and neutralize threats.

Our AI-powered solutions cut down reaction times and enhance decision-making, while comprehensive, always-on security ensures businesses stay protected 24/7. Palo Alto Networks and Orange Cyberdefense are leading the charge, empowering organizations to stay one step ahead in an evolving threat landscape.

# Contents

# The time to act is now.

The numbers are telling us loud and clear: **SOC transformation is no longer optional.** According to the Orange Cyberdefense Security Navigator 2025[1], the number of **cyber extortion victims have jumped by 15.29%** over the past year, with small and medium-sized businesses seeing **a staggering 53% rise in attacks**. This shows just how critical it is to ramp up your threat detection and response capabilities, now more than ever.

**When it comes to Operational Technology (OT) environments, the risks are even higher. A shocking 81% of OT-related cyber-attacks are carried out by criminals, further underlining the need for specialized SOC measures to defend our most critical infrastructure.**

And with **over 264,000 vulnerabilities cataloged globally,** it's clear that traditional security methods won't cut it anymore. It's time to adopt more dynamic, automated approaches that can keep up with the pace of today's threats.

> *The average cost of a cyberattack that resulted in a breach was $4.35 million in 2022.[1] The repercussions of cyberattacks are far-reaching and costly, with data breaches costing an average of $4.88 million in 2024.[2]*

The writing's on the wall: SOC transformation isn't just a trend, it's the future of cybersecurity. If you want to stay ahead of emerging threats, secure your organization, and ensure your operations are future-proof, transformation is essential.

[1] Report: AI cybersecurity market projected to exceed $133 billion | Security Magazine

[2] Cost of Data Breach in 2024: $4.88 Million, Says Latest IBM Study - SecurityWeek

# AI - the next step in the evolution of your SOC.

**AI has turned IT upside down as organizations scramble to both apply the technology and respond to the complexity it presents. With your SOC at the front line, SecOps teams don't have the luxury of waiting.**

AI is impacting many if not all aspects of our lives and security is no stranger to that change. Not only are IT organizations scrambling to determine how to best apply AI, but just as pressing is the question of how to combat the looming threats that AI poses.

> *"…the application of AI has led to an increase in cybercrime, according to 85% of cybersecurity professionals. In 2024, internet users are projected to spend $9.22 trillion as a result of AI's personalized attacks, adaptability to defense systems, and attack speed and volume. To counter evolving threats, users are encouraged to stay vigilant and utilize updated systems to counter evolving threats."*[3]

*The SOC is the front-line defence and is both vulnerable to these threats and in a unique position to take advantage of the technology to make SecOps and IT Ops jobs easier.*

[3] Report: AI cybersecurity market projected to exceed $133 billion | Security Magazine

# Preparing for the SOC of the future.

## The best time to start planning for AI in your SOC and security solutions was yesterday. The second best is today.

Cyber threats are evolving at an unprecedented pace, and they're not slowing down. To stay ahead, transforming your SOC is a must, but it doesn't happen by chance. It takes careful preparation and strategic action. As businesses look ahead, there are real opportunities to enhance your security operations and be ready for whatever's next.

**Here's what you need to prioritize:**

# Priority 1

### Transform your SOC to stay ahead of evolving cyber threats.

In cybersecurity, change is the only constant. This makes having a clear and effective strategy for your SOC transformation business critical. Many organizations struggle with visibility into their current security posture, making it challenging to create a roadmap for SOC transformation. This lack of visibility can hinder their ability to evolve and consolidate operations efficiently, leaving them vulnerable to emerging threats.

Through expert consultancy, strategic planning, and a focus on industry-specific needs, it's imperative to plan for the 'SOC of the future'. The design needs to ensure that you can identify risks and vulnerabilities not just today, but in the future, including supply chain exposures. It's important to develop clear, prioritized roadmaps by working with all stakeholders in your organization, from planning to deployment, ensuring continuous improvement.

By combining Palo Alto Networks' cutting-edge technology with Orange Cyberdefense's global managed security expertise, we provide a comprehensive approach to SOC transformation. Our partnership ensures that you have the visibility and strategic planning needed to stay ahead of evolving threats, with continuous improvement and proactive risk management.

# Priority 2

## Overcome the skills gap to effectively manage your SOC.

> *"Two items stand out from this year's study: the need for (and lack of) adequate security staff levels, and the constant need for user security awareness training. Both are long-term problems, and neither are solvable. Cybersecurity teams are consistently understaffed. This study found more than half of breached organizations faced severe security staffing shortage."* [4]

There is an acute skills shortage of security professionals. Companies that are short-staffed are more likely to experience breaches.

If you are concerned that your own internal resources are not trained appropriately or if you fear that you might not have the expertise required to navigate into the future, looking into solutions that include managed services could be an excellent way for you to shore up your defenses.

It is imperative that your team is comfortable using newer security solutions such as Prisma SASE, Cortex XSOAR™, and Cortex XSIAM™ to give you advanced security without requiring specialized internal expertise. Managed services provide an effective way to ensure that these tools are operated and monitored effectively. By combining technical skills, threat intelligence, and managed services, we ensure you are protected 24/7, providing localized, global support that's scalable and flexible.

Orange Cyberdefense's managed services bridge the skills gap by providing access to specialized security expertise and advanced tools. We ensure that your SOC is equipped with the latest technologies and operated by experienced professionals, offering 24/7 protection and scalable support to meet your evolving security needs.

[4] Cost of Data Breach in 2024: $4.88 Million, Says Latest IBM Study - SecurityWeek

# Priority 3

**Leverage AI to enhance threat detection and response.**

Pre-configured detection rules refined based on your industry, geography, and specific requirements can serve as a useful tool for scalability and agility. One excellent use case for AI is to help process large volumes of data in real time, helping with the detection of behavioral threats and automating risk calculations and responses aligned with your policies. AI-driven XDR services have advanced to continuously monitor and manage threats across endpoints, networks, cloud environments, and identities.

**"Artificial Intelligence (AI) and automation hold great potential for security operations. According to the report, 61% of SecOps leaders believe AI can manage up to 30% of security tasks, with 17% projecting this number to rise to 50% in the coming years."[5]**

Some other potential use cases to explore include using AI in chatbots or GenAI for improving customer experience, and AI to predict threats using CTI (Cyber Threat Intelligence) data for enhanced exposure management.

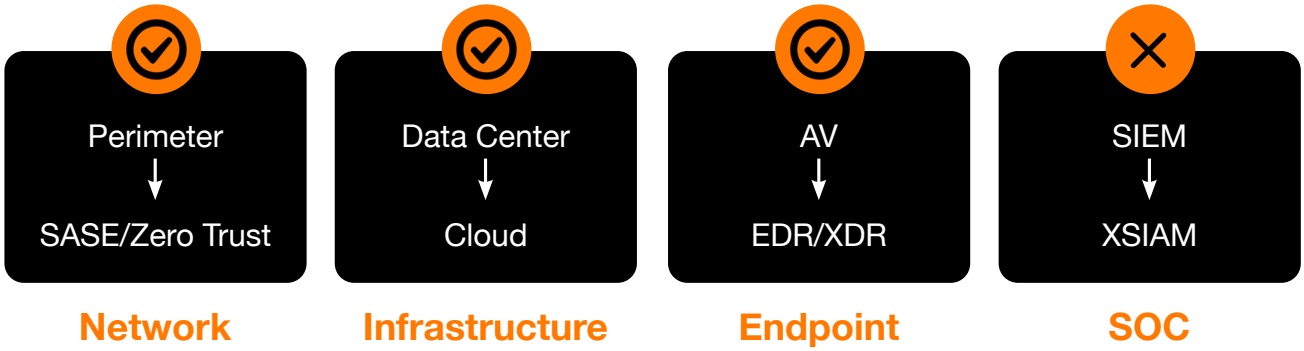
By integrating AI-driven technologies with our managed services, we enhance your threat detection and response capabilities. Our AI-powered solutions provide real-time analytics and automated responses, ensuring that your SOC can handle advanced threats efficiently. With our global expertise and continuous monitoring, we offer a proactive and adaptive security posture.

[5] Top 5 Security Operations Challenges Facing Organisations Today

# What is Cortex XSIAM and how can it can help?

## What is XSIAM?

Extended Security Intelligence and Automation Management (XSIAM) is revolutionizing security by blending AI with automation to streamline security operations. Designed with operations at its core, XSIAM integrates data and automates processes that were once cumbersome, offering a more efficient, centralized solution for managing your security posture. as illustrated below:




Think of XSIAM as your security powerhouse, centralizing your data to power advanced analytics.

With automation and AI at the heart of it, XSIAM delivers faster threat detection and response at half the cost of legacy solutions.

Centralized data means quicker responses to threats, and with innovative technologies backing you up, you'll always be ahead of the game.

Designed to be a hub for all SOC activity, XSIAM replaces SIEM and specialty products by unifying a broad range of functionalities into one holistic solution. With features like data centralization, intelligent stitching, analytics-driven detection, incident management, threat intelligence, automation, and attack surface management, XSIAM empowers your SOC with everything it needs to stay ahead of the cyberthreat curve. All conveniently delivered within an intuitive, task-orientated user experience (UE).

## Cortex XSIAM doesn’t just collect data.
## It turns data into action.

**By centralizing threat data and structuring it for maximum visibility and searchability, XSIAM automates threat detection and mitigation.**

With an intuitive, task-driven user interface, XSIAM provides the right information exactly when you need it, helping your SOC stay ahead of evolving threats.

XSIAM builds on traditional security foundations and offers a clear path forward for SOCs struggling with SIEM. It provides the robust data foundation and speed needed to quickly respond to threats, ensuring your SOC remains agile and proactive.

# The role of managed services

## The real power of XSIAM comes to life when it's paired with expert managed services. Enter Orange Cyberdefense.

Through our strategic partnership with Palo Alto Networks, we offer a comprehensive, all-in-one solution that combines cutting-edge technology with deep operational expertise. Our managed services bridge the skills gap, providing specialised security know-how and 24/7 support to keep your SOC running at its best.

This includes our Managed Threat Detection (MTD) and Managed Detection and Response (MDR) services. the cornerstones of our managed portfolio. MTD delivers proactive, intelligence-led monitoring across endpoints, networks, and cloud environments, detecting and escalating threats early. MDR takes it a step further, providing an always-on, human-led capability that combines advanced analytics, threat hunting, triage, and incident response to neutralise threats in real time.

But our support doesn't stop there. Orange Cyberdefense offers a full spectrum of managed SOC services, including:

- Managed Threat Intelligence: Actionable insights to stay ahead of adversaries.
- Managed Vulnerability Management: Continuous scanning and prioritisation of exposures.
- Co-managed and fully-managed SOC: Flexible models to extend or outsource your SOC operations.
- Digital forensics and incident response: Rapid expert support when breaches occur.

By integrating these services with Palo Alto Networks' Cortex XSIAM, we turn intelligence into action, giving you a proactive, adaptive, and resilient security posture that evolves with your business.

# Palo Alto Networks and Orange Cyberdefense as trusted security partners

**Palo Alto Networks** is recognized as a leader in cybersecurity, providing solutions that support efficient and automated SOC operations. Key credentials include:

### #1 in SOC Automation:
Known for automating security operations to enhance response times and reduce manual effort.

### Leader in XDR (Extended Detection and Response):
Positioned as a leader in the 2024 Forrester Wave, ensuring comprehensive visibility and threat detection.

### MITRE Engenuity ATT&CK® Evaluation:
Highly regarded for its effectiveness in detecting and responding to complex cyber threats.

### Gartner Magic Quadrant Leader for Network Firewalls:
Recognized for providing reliable and effective network security.

### ESG Security Validation:
Acknowledged for leveraging analytics and automation to modernize SOC operations.

With over 25 years of experience, **Orange Cyberdefense** is a trusted partner for securing organizations across industries. Some of our key strengths in SOC operations include:

### SOC-specific Expertise:
With extensive experience managing Security Operations Centers, we offer proactive and tailored support for every stage of SOC evolution, from design to continuous operation.

### Security Certifications:
Orange Cyberdefense holds numerous industry certifications, including ISO 27001, PCI QSA, and CREST, demonstrating our commitment to best practices in security management.

### Proven SOC Capabilities:
Our SOC services are trusted by organizations globally, with a clear focus on both risk mitigation and incident management. This includes services like threat detection, incident response, and continuous improvement, ensuring your SOC adapts to evolving threats.

**Find out more**
about our Threat Map services.

# 8 reasons why Palo Alto Networks and Orange Cyberdefense are your ideal partners for SOC transformation

**AI-powered security operations:** Detection is only the beginning, our real value comes from stopping threats before they happen. Our AI-driven, automated SOC solutions work at lightning speed to predict, prevent, and neutralize attacks in real time, keeping your business secure 24/7.

**Unrivaled threat intelligence:** Our continuous feed of insights from Palo Alto Networks' XSIAM into the Orange Cyberdefense intelligence database creates a powerhouse of threat intelligence. With 38% of our data being exclusive to us, we see what others can't, giving you a level of visibility no other provider can match.

**Next-gen security platforms:** AI. Automation. Machine learning. Palo Alto Networks' Cortex XSIAM platform brings it all together to deliver smarter, faster, and more effective threat detection and response—because speed and precision matter when you're fighting cyber threats.

**Proven and trusted CyberSOC model:** We bring years of expertise in SIEM technologies to deliver next-gen security without sacrificing reliability. Our AI-enabled, fully integrated approach gives you the confidence that your security operations are running at peak performance, every second of every day.

**Global intelligence advantage:** We're plugged into over 400 data sources, including exclusive telecom data, giving us a unique edge in spotting and stopping cyber threats before they become a problem. With over 50,000 customers worldwide, we don't just react to threats, we stay ahead of them.

**Optimized security, real business impact:** Stronger security shouldn't mean more complexity or higher costs. Our solutions streamline operations, reduce your total cost of ownership (TCO), and give you the flexibility to build, expand, or fully outsource your SOC, whatever works best for yo ur business.

**AI-driven, human-led expertise:** Security is about more than just technology. It's about people. Our teams of experts work alongside AI-powered automation to deliver a perfect balance of speed, intelligence, and hands-on expertise, so you're always one step ahead of cybercriminals.

**A security ecosystem built for the future:** This is more than just a SOC upgrade - it's a transformation. Our unique intelligence, cutting-edge tech, and proven expertise create an ecosystem designed to evolve with you, keeping your business secure while you focus on growth and innovation.


Cyberdefense