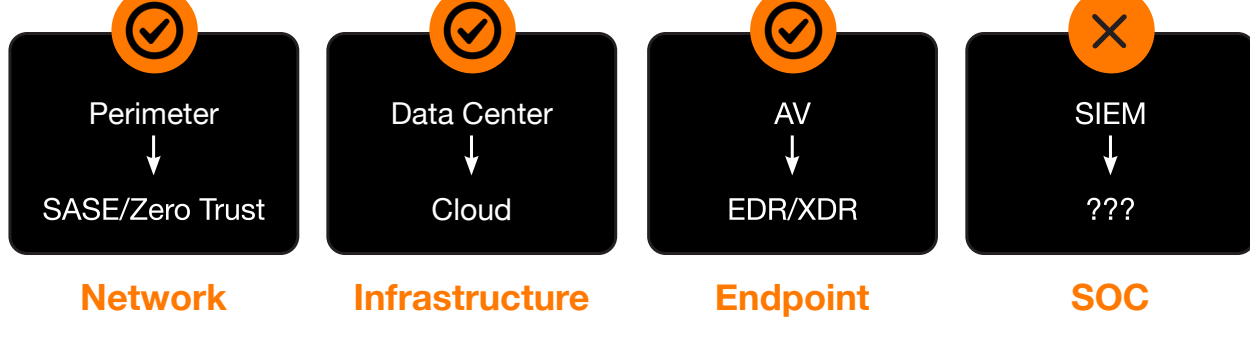


Supercharge your Security Operations Centre with AI

AI represents the next step in the evolution of your Security Operations Centre (SOC) – learn how Extended Security Intelligence and Automation Management (XSIAM) can help

Extended Security Intelligence and Automation Management (XSIAM) is a new security approach geared towards operations. It applies AI to automate many of the processes that are resource intensive or that a SOC lacks visibility into.



Exec summary section



Security Operations Centres (SOCs) have come a long way since their inception.

Despite the SOC progression, cyber risks and new technologies, such as AI, continue to pose issues.



The number and complexity of detected incidents has surged year-over-year, with many incidents originating from internal actors.



It is imperative that organisations apply the most innovative technologies that they can to adapt to the shape shifting risk of today.

Palo Alto Networks's Cortex XSIAM applies AI to provide heightened visibility and ensure that a SOC can respond to threats and better anticipate them than with traditional tools.

Build an intelligent data foundation | Accelerate response | Outpace threats

Cortex XSIAM, when combined with the right SOC provider, puts companies back in charge of their IT

Simplify and strengthen security and networking operations with an AI powered SOC with XSIAM



...the application of AI has led to an increase in cybercrime, according to **85%** of cybersecurity professionals... To counter evolving threats, users are encouraged to stay vigilant and utilize updated systems to counter evolving threats.



IT organisations are scrambling to determine how to best apply AI and how to combat the looming threats that it poses.



The SOC serves as a front-line of defence and is vulnerable to emerging threats while also being in a unique position to take advantage of the technology.



Cortex XSIAM, the AI-driven platform is from the #1 pure player in cybersecurity. Orange Cyberdefense has a +25-year track record in information security they provide a supercharged SOC.

It's imperative to have a SOC strategy



The average cost of a cyberattack that resulted in a breach was US \$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 SOC arose in recent history as a response to the increasing complexity of cyber risks. As the **cost of breaches increases** so too does the business exposure.



Ever changing threats and the associated cost of breaches mean that companies need to continually plan and adjust their IT and SOC to meet these challenges.



Palo Alto Networks and Orange Cyberdefense **help guide companies with their planning**, starting with assessments powered by Palo Alto Networks's Cortex. Our teams work closely with customers to develop clear, prioritised roadmaps, from planning to deployment, ensuring continuous improvement.

Enhance threat detection and response with AI-powered capabilities



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.³



As AI finds its place in the SOC, it's evident that it helps increase efficiency and detect risk.



In this challenging environment, businesses must stay ahead of cyber risks by adopting advanced security solutions that can keep pace with the rapidly evolving threats.



Palo Alto is the leader in security which, combined with Orange Cyberdefense's credentials, SOC's global footprint, make their XSIAM solutions a natural choice for companies that are seeking protection from threats – and the future.

Many organisations have a skills gap which leaves them vulnerable



More than half of those surveyed (58%) believe a shortage of skills puts their organization at significant risk, and **64%** say skills gaps present a greater challenge to securing their organizations than staffing shortages.



There is a shortage of the right **security experts** which leaves businesses vulnerable to increasingly sophisticated cyber threats.



It's critical that you have the **right people who adapt to new technologies** and interface your SOC. Training and certifications are excellent resources but working with the right managed service partner can fill any knowledge or resource gaps.



Orange Cyberdefense combines **technical skills, threat intelligence, and managed services, with 24/7 protection**, providing localised, global support that's scalable and flexible.

Tap into the power of the leading XSIAM solution backed by 3,000+ security experts available globally 24/7. Trust the SOC that is responsible for closing more than 40,000 suspicious websites every year.

To learn more about how to leverage AI as part of your SOC or to start planning for it, do this today.

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

³ Top 5 Security Operations Challenges Facing Organisations Today