paloalto NETWORKS | CORTEX BY PALO ALTO NETWORKS

Enhancing SOC Efficiency: Defend at Machine Speed

TABLE OF CONTENTS

USING AI TO REVOLUTIONIZE THE SOC

Too much happens today for traditional approaches to keep pace with modern threats.

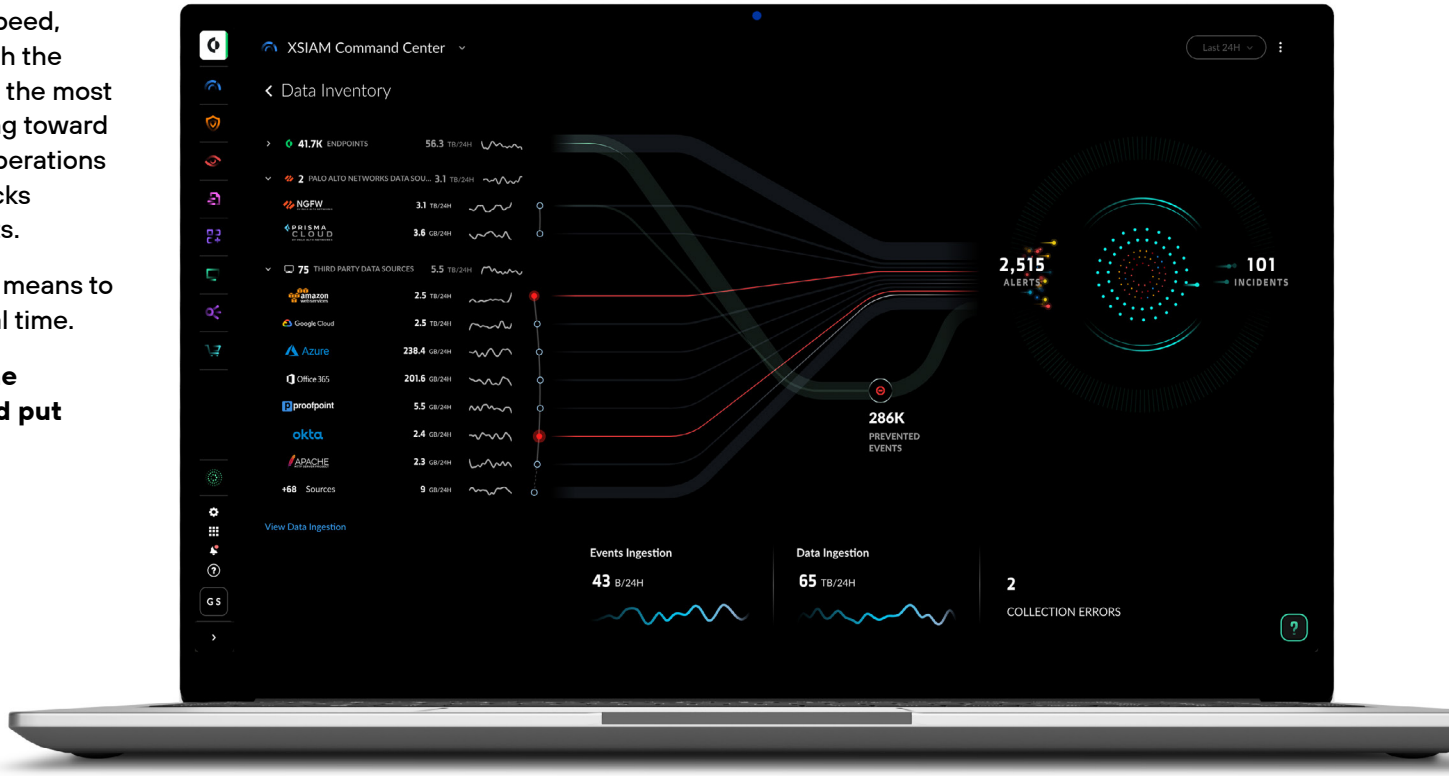
Manual processes force analysts into a mode of managing alerts rather than detecting and eradicating threats. The cloud is still a huge blind spot. Securing development pipelines still proves elusive. Mergers and acquisitions create as much risk as they do opportunity. Basic cybersecurity hygiene like patch and vulnerability management feels practically impossible for most organizations.

Meanwhile, attackers are working at greater speed, scale, and sophistication than ever before. With the help of AI, they're getting better at pinpointing the most valuable and vulnerable targets. They're turning toward more destructive tactics to disrupt business operations for employees and customers alike. Such attacks commonly reach the billion-dollar mark in costs.

Until now, the SOC has lacked the tools or the means to ingest and analyze threat detection data in real time.

But times are changing. Defensive AI has the potential to turn the tables on attackers and put SOC teams in control.

> If we keep working in the traditional ways, we will always be falling behind on threats, alerts, and hardening security.
>
> — Clay Brothers
> Unit 42 Technical Consulting Senior Director, Palo Alto Networks



Here you see the XSIAM Command Center, your real-time operational hub 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.

THE TRANSFORMED SOC

Defensive AI transformation doesn't have a firm finish line, because it isn't a one-and-done effort. It is a permanent evolution toward a better way of working, defending, and adapting.

However, these markers and metrics indicate the effectiveness of your transformation efforts.

Drastically Reduced Response Times

AI insights identify attacks sooner. Median time to resolution shrinks from days and weeks to minutes.

Automated Incident Resolution

Enhance their operational efficiency, reduce response times, and better protect their organization's assets against cyberthreats with the help of AI-automated incident resolution.

With the power of AI, customers achieved 75% fewer incidents requiring investigation* and nearly 100% closure rates.

Lower Engineering Overhead

Automate data normalization to reduce the engineering effort to integrate data sources, making sure analysts have a full view of threats without needing to pivot between solutions.

Truly, the mark of a transformed SOC is that the tables have turned on the attackers themselves. Teams can proactively anticipate threats, harden their postures, and mitigate risk. By working smarter, we can force attackers to work harder, to make critical errors, and ultimately fail in their malicious attempts to extort and disrupt.

In short, a transformed SOC is prepared to win the day, every day.

Scale and Harden Security with Less Staff Burnout

AI takes on more of the prevention and detection burden so teams can focus on proactive measures like tabletop exercises, purple teaming, and threat hunting exercises to harden the organization's overall posture.

Faster Investigations

By harnessing the power of AI technologies, SOC teams can streamline their investigative workflows, improve operational efficiency, and strengthen overall cybersecurity defenses to proactively detect and respond to threats.

Instead of juggling 10—20 dashboards and data sources, analysts have a single source for all investigations with normalized data from all sources.

> "AI is real. It's not hype anymore. It's absolutely real because we are seeing value because of it. We are seeing meaningful business impact, which we can quantify through the outcomes we're able to achieve.
>
> — Meerah Rajavel
> Chief Information Officer, Palo Alto Networks

PILLARS OF THE MODERN SOC

Now comes the question of how to get to a transformed SOC.

If there were one word to describe most SOCs, it would be "overwhelmed." The sheer volume of alerts, data, tools, vulnerabilities, and misconfigurations is prohibitive to making actual headway. The ever-increasing complexity of the IT environment exacerbates these challenges to such a degree that even basic cybersecurity hygiene becomes a never-vending struggle.

Consolidating the Security Stack

Using fewer tools and using tools that work better together are essential to reducing complexity and streamlining operations.

Combines SIEM, EDR, XDR, SOAR, ASM, and other security functions into a single platform. XSIAM automates analysis and response, allowing analysts to focus on critical incidents.

Brings together best-in-class CDR with the next version of Prisma® Cloud's leading CNAPP for real-time cloud security.

Augments and accelerates your cyberdefenses with 24/7 monitoring, expertise, threat hunting, and remediation.

The following are the pillars that uphold the transformed SOC and solve many of cybersecurity's most long-standing challenges.

1. Transforming SOC Efficiency

In Unit 42's 2025 Global Response Report, we found that attackers leveraged three points of entry on average. In 75% of incidents, critical evidence of the initial intrusion was available, yet defenders couldn't put the pieces together because of a disjointed security tool stack. To detect attackers as they rove across numerous domains to mount their attacks, all data must flow into a centralized hub for analysis (performed by AI and machine learning).

For most SOCs, this hub is the SIEM. However, even the best SIEM comes with a debilitating degree of complexity and fragmentation, engineering overhead, and manual workflows. They are simply not built for the realities of the modern SOC, making it impossible to:

- Ingest vast volumes of data at scale, particularly in hybrid environments.
- Consolidate numerous security functions and cover all the team's needs.
- Provide full visibility, from endpoint to network to cloud.

Throwing more tools into the mix won't solve the problem. A "platformization" approach extends capability while reducing complexity, redundancy, cost, and engineering overhead.

Outcomes
The SOC achieves full visibility across all environments and endpoints.
All data, including cloud data, flows into a single hub for analysis.
The SOC has far fewer tools to juggle and maintain.

2. Rapid, Comprehensive Incident Response

A multitude of siloed security tools ceaselessly blasting analysts with alerts has become more of a hindrance than a help. IBM reported that one-third of the SOC's workday is spent investigating incidents that aren't a real threat. A 451 Research report sponsored by Palo Alto Networks found that on average SOC teams are unable to investigate 43% of incidents in a typical day.

SOCs are also plagued by a lack of data. SIEM systems strip away the contextual metadata, often due to the cost structure, which would give analysts a fuller picture of the threat. For example, an alert might indicate a suspicious login attempt from an unfamiliar IP address, but without additional context such as the user's recent travel history, VPN usage, or device information, analysts cannot quickly determine if this is a legitimate employee or a potential security breach.

AI-driven intelligence solves the data conundrum:

- Smarter filtering clears the analyst's deck of incidents that don't merit investigation, often cutting alerts by over 90%.
- The full incident story is at the analyst's fingertips, built from alerts from disparate tools and contextual metadata.
- Of the incidents worthy of investigation, defensive AI tools prioritize the most critical incidents and recommend the most efficient paths to remediation.

Defensive AI helps analysts work far more efficiently. When the AI discovers a potential attack path, it can identify which remediations will provide the most coverage. The analysts can remediate, say, three key points along the attack path rather than all 20 points on the attack path. Additionally, AI copilots allow analysts to accomplish all this without juggling an array of tools. Copilots bring the information directly to the analyst, saving hours of manual work and driving down response times. When new analysts join the team, AI copilots can help them uplevel their skills without detracting from more experienced analysts' work.

Outcomes

Security data is delivered through a unified user experience—a single source of truth that surfaces critical threats and enables efficient response.

Powered by a unified backend that streamlines the integration and minimizes the daily maintenance of all of your sources into a single harmonious UI.

SIEM, XDR, ASM, automation, and cloud security all speak the same language, powered by a unified backend that stitches together the data to provide a complete threat picture and orchestrated automation to address the root cause of incidents.

Analysts investigate fewer incidents while covering more risk, reaching incident closure rates nearing 100%.

Analysts can detect threats earlier and respond with precision, leading to faster detection and response times.

The security team now has the bandwidth to conduct better patch and vulnerability management, along with proactive threat hunting and other exercises.

3. Agile Threat Defense: AI in Action

New technologies, threats, and frameworks create a moving target for SOCs. Organizations must implement systems that learn on their own and improve over time to stay ahead of malicious actors.

By integrating with global threat intelligence feeds, cutting-edge tools can shift focus with the latest indicators of compromise, tactics, techniques, and procedures. Similarly, these systems can detect changes in compliance frameworks like GDPR and PCI DSS and adjust security policies accordingly. Self-healing systems can remediate vulnerabilities automatically and dynamically update tools to reflect changes in infrastructure without manual intervention.

In this model, humans are kept in the loop. Analysts provide feedback to refine AI models and workflows to ensure continuous improvement based on organizational experience and real-world developments. In the wake of an incident, automated systems can analyze root causes, and then update detection rules and response playbooks to prevent the same thing from happening again.

Outcomes

Through AI, SOAR playbooks are refined with each incident to improve response efficiency, requiring minimal effort from the team.

Risk-scoring and prioritization functions become more accurate in the face of new intelligence and shifting attack patterns.

Lowers the barrier to entry for new analysts, allowing junior team members to perform at a higher level faster.

Behavioral baselines across multiple data models become more accurate to protect against insider threats and subtle attack patterns.

Lower engineering overhead because AI continuously adjusts firewall rules, correlation logic, and detection thresholds based on real-world trends.

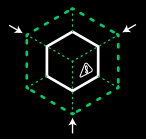
Key AI Capabilities

Automated Data Integration and Analysis

AI-driven platforms like Cortex XSIAM® automatically integrate and analyze data at a massive scale, providing comprehensive threat detection across endpoints, cloud, and network

ML-Driven Alert Aggregation and Triage

Machine learning models aggregate alerts and triage incidents, reducing the time analysts spend processing data and enabling faster, more accurate investigations.



Advanced Threat Detection

AI detects anomalous patterns across multiple data sources, providing alerts with context and minimizing blind spots. This ensures threats are detected and mitigated promptly.

Specialized Analytics

Machine learning models establish baselines for applications based on your unique organization and then detect deviations like unusual file system interactions and resource utilization.

4. Automated Workflows

Common automation capabilities simply don't move the needle enough for the SOC. Analysts must still manually trawl through excessive alerts, retrieve contextual data, fine-tune detection rules, and continuously update playbooks.

A transformed SOC greatly simplifies the analyst's workload by achieving what has long seemed impossible: the seamless integration between the SIEM and other tools like extended detection and response (XDR) platforms, firewalls, identity management systems, and others.

This hardens defenses from both proactive and response perspectives.

Prevention

More intelligent correlation rules, real-time integration with threat intelligence, automated updates to detection rules, and automated contextual data enrichment—such capabilities simplify and accelerate the proactive security hygiene tasks that insulate the organization from threats.

Response

In the transformed SOC, automation extends farther into the IR lifecycle. Adaptive, customizable playbooks can handle many response steps like isolating compromised endpoints, revoking credentials, and blocking malicious IPs without analyst intervention. This speeds up response and allows analysts to pursue high-level tasks.

Outcomes

A higher percentage of incidents can be resolved without analyst intervention, allowing analysts to focus on more complex investigations—altogether lowering mean times to detect and respond.

Logging and reporting becomes fully automated for better compliance and more thorough monitoring of SOC performance.

Dwell time of threats decreases, as does the scope and impact of risks.

5. Cloud-Native Architecture

Of the hundreds of incidents we helped our clients investigate in 2024, 30% were related to cloud assets. In our 2024 State of Cloud Native Security Report, we found that 80% of organizations would benefit from a centralized security solution across all cloud accounts and services.

The SOC must gain command of the cloud. That means eliminating its blind spots and bringing it into the fold of the greater security function.

This transformation starts by merely ingesting the vast troves of real-time data generated by cloud services. Cloud-native, context-driven defense provides coverage for cloud-native assets like containers, serverless architecture, CI/CD development pipelines, and cloud applications from code to cloud to SOC.

More advanced cloud security transformation includes automating tasks like auditing cloud configurations, deploying patches, and enforcing compliance policies across hybrid environments. As with threat detection in other environments, it's pivotal for tools to score incidents and vulnerabilities by risk and prioritize them for the analyst.

In the transformed SOC, the team sees not just an attack in progress, but the cloud exposures that made it possible. With runtime insights mapped to cloud risk, investigations become faster, more precise, and tied to real-world attack paths.

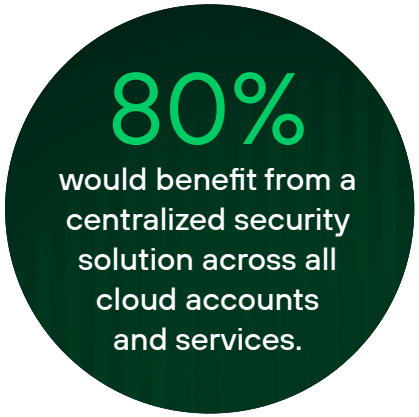
Outcomes

Real-time cloud data can be incorporated into broader machine learning-driven analysis.

The cloud attack surface shrinks dramatically through microservices security, workload isolation, and other features that limit unauthorized access and lateral movement.

The cloud posture is hardened against supply chain risks and attacks.

Multicloud and hybrid environments can maintain uniform security processes across multiple providers.



TRANSFORMATION SUCCESS WITH PALO ALTO NETWORKS

When it comes to SOC transformation, Palo Alto Networks is trusted by the best. 97 of the Fortune 100 work with us, as do 76% of the Forbes Global 2000. All six branches of the U.S. armed forces trust us to execute their security strategies and goals.

Here are just a few SOC transformation success stories we've helped our clients achieve.

Oil and Gas

A Fortune 500 oil and gas company faced an avalanche of false positive alerts from a legacy SIEM, which the security team had to manually investigate using several tools. The SIEM couldn't ingest or automate the high volume of data required to meet the demands of the business.

By adopting Cortex XSIAM, Palo Alto Networks AI-driven SecOps platform, the company ingested more data sources while reducing alert noise. Its improved alert quality allows them to detect, respond, and prevent potential threats faster.

> "We used to have thousands of garbage alerts. Now we have five events a week we really need to investigate. That's how good the systems are working. It's very easy to investigate.
>
> — IT Security Leader

0
false positives decreased from 90% to virtually none

4X
fewer incidents requiring investigations daily, from 1,000 per day to 250

59
minute median time to resolution reduced from multiple days

Manufacturing

A global semiconductor manufacturer's security stack of point solutions obscured visibility and forced teams into a mode of manual, reactive intervention. The company's lean security team was overwhelmed, limiting the company's ability to scale and putting its intellectual property at risk.

Palo Alto Networks consolidated multiple point vendors into an intelligent, unified security stack that included Next-Generation Firewalls powered by machine learning and Cloud-Delivered Security Services, all feeding into the Cortex XSIAM platform. More importantly, our team helped shift security left within the engineering-led organization.

> "Our philosophy is 'do it right, do it once' – and Palo Alto Networks gives us that capability. Across network, endpoint, and cloud security, the technologies are proven, agile, and highly flexible."
>
> — Paul Alexander
> Director of IT Operations, Imagination Technologies

1
minute mean time to repair

92%
of incidents resolved through automation with no analyst intervention needed

24/7
managed threat hunting

Consumer Tech

An American home security technology provider faced an increase in hostile threats against its systems. To preserve its reputation and provide a safe, smooth experience to its customers, the company set out on an ambitious modernization effort to drive zero trust across the organization. They needed to meet the challenges of their multi-cloud environment, hybrid workforce, and over 9 billion daily alerts.

Palo Alto Networks helped modernize their existing infrastructure by upgrading firewalls, simplifying SecOps processes, and expanding automation. By adopting our Next-Generation Firewalls and Cloud-Delivered Security Services, the company broke down silos between its networking and security teams to achieve better collaboration and more efficient processes. Through the Cortex® product suite, they enhanced threat detection and unlocked security at scale.

> "We've consistently seen significant, double-digit efficiency gains year over year. That's driving efficiencies back into the business so we can do more."
>
> — Rick DeLoach
> Director of IT Security, ADT Security

3
hour median time to resolution, down from several days

92%
of incidents resolved through automation with no analyst intervention needed

9
billion events transformed into a manageable number of incidents

Start Your AI Security Journey

Transforming the SOC with AI, automation, and unified data is not just an upgrade—it's a necessity for keeping pace with today's threats. By focusing on outcomes and leveraging advanced technologies, SOCs can achieve unprecedented levels of efficiency, effectiveness, and resilience.

The journey to a modern SOC begins with a commitment to change and the adoption of platforms that enable this transformation. As one SOC leader using XSIAM noted, "XSIAM is the best single pane of glass I've seen in cybersecurity. We went from looking at 10 datastores to just XSIAM in our investigations."

By embracing this transformation, SOCs can move from a reactive stance to a proactive, intelligence-driven operation capable of defending against the most sophisticated threats of today and tomorrow.

Your AI security journey starts with a conversation. See how we can empower your team to defend at machine speed. Contact us today for a personal demo.

> "Machines will do what humans do, just they're going to do it much faster and in a much more scalable way. So that's the idea behind using AI in the SOC to detect attacks and stop them.
>
> — Nir Zuk
> Chief Technology Officer, Palo Alto 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_Enhancing-SOC-Efficiency_060625