







Cortex XSIAM vs. Splunk

Competitive Comparison

Modernize Your SIEM. Transform Security Operations.

Splunk may have defined SIEM, but Cortex XSIAM® defines the future. Explore why leading enterprises choose Cortex XSIAM for faster detection, automated response, and lower operational costs.

Capability	splunk> <small>a cisco company</small>	CORTEX XSIAM <small>BY PALO ALTO NETWORKS</small>
 Cloud Scale	Legacy Performance Issues Complex architecture slows onboarding and scatters context across consoles, delaying investigations.	Effortless Scalability, Zero Complexity A modern cloud-based solution for AI and analytics, enabling focus on innovation without scalability concerns.
 Unified Platform	Fragmented Tools, Fractured Workflows Lacks native EDR, ASM, or CDR, increasing reliance on multiple consoles and third-party tools.	Single Platform, Complete Visibility Fully integrated SecOps capabilities, including SIEM, EDR/XDR, SOAR, and ASM, in one intuitive platform, streamlining operations.
 Detection Coverage	Manual Detection, Delayed Response User-built correlation searches and separates ML add-ons, leading to upkeep and slow response.	Advanced Analytics & Detection 10K detectors and 2.6K ML models deliver 100% detection , accelerating triage and response.
 Native Detection and Prevention	No Native EDR Lack of first-party EDR agent forces reliance on third-party tools, creating inefficiencies and silos in response.	Real-Time Endpoint Prevention Industry-leading native XDR blocks exploits instantly and streams context to the SOC, cutting risk.
 Native Automation	Partial Automation, Heavy Manual Effort Separately licensed and managed SOAR that requires manual deployment, upkeep, and delivers an inconsistent experience during response.	End-to-End SOC Automation Integrated SOAR automates every SOC step, cutting manual effort and achieving up to a 98% faster MTTR .
 Migration Speed	Manual Rule Rewrites Teams (or costly services) must rebuild correlation logic rule-by-rule, extending projects and risking detection gaps.	AI-Guided Rule Mapping XSIAM Professional Assistant uses LLMs to align Splunk/QRadar rules with 10K+ built-in detectors (confidence-scored), shrinking cut-over from months to days.

Industry Validation and Customer Results

> Analyst Recognition

100% DETECTION

MITRE | ATT&CK® →

100% Detection and Industry-Low False Positives,
Zero delays or config changes

LEADER

FROST & SULLIVAN →

2024 Modern Security Information and
Event Management

LEADER

Omdia →
by informa techtarget

2024-2025 Next-Generation SIEM Solutions

LEADER

GIGAOM →

2023 and 2024 Autonomous Security Operations
Center (SOC) Solutions

> Real-World Customer Impact

BOYNE RESORTS

98% faster median time to resolution (MTTR).

GLOBAL OIL AND GAS LEADER

75% fewer incidents requiring manual investigation.

GLOBAL LOGISTICS PROVIDER

Reduced SOC tools from **7 down to 1.**

Experience the Real Power of SIEM

Schedule a demo



Take a guided
product tour



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

© 2025 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-xsiam-vs-splunk-competitive-comparison_060525