SOLUTION NOTE

ENRICH YOUR PALO ALTO NETWORKS CORTEX XSIAM AND XSOAR INTEGRATIONS WITH INFOBLOX

OVERVIEW

Infoblox, the industry leader in DNS, DHCP and IP address management (DDI) and DNS security, integrates directly with Palo Alto Networks Cortex XSIAM and Cortex XSOAR, which Palo Alto Networks describes as the first AI-driven SecOps platform. This integration provides deep DNS-layer visibility, enriched threat intelligence and SOAR automated workflows that accelerate detection and response.

Palo Alto Networks offers distinct ecosystem integrations for Cortex XSOAR and Cortex XSIAM which may be deployed together within a unified platform. This consolidation helps security teams to streamline operations, reduce tool sprawl and improve overall efficiency. By ingesting Infoblox telemetry such as DNS queries, DHCP leases, IP address management (IPAM) metadata and curated threat intelligence, Cortex XSIAM and Cortex XSOAR enable real-time correlation, contextual investigation and automated incident response. Note that while Cortex XSIAM and Cortex XSOAR can be deployed together within a unified platform, they operate as distinct integrations with separate licensing paths.

Cortex XSOAR is Palo Alto Networks' SOAR platform that empowers security teams to streamline incident response and threat mitigation. Through its integration with Infoblox, analysts can investigate prioritized threats using rich, contextual data directly within the Cortex XSOAR interface. The platform supports automated playbook execution, enabling rapid remediation actions, such as blocking malicious domains and IPs. By leveraging an on-premises XSOAR engine, organizations can securely connect to Infoblox APIs to ingest IPAM data and enrich security workflows.

Cortex XSIAM is Palo Alto Networks' next-generation SIEM platform, designed to unify data, analytics and automation for autonomous security operations. It enables incident creation based on custom thresholds and supports categorization of threat data by severity and domain. Cortex XSIAM also facilitates user-defined anomaly alerts and integrates seamlessly with playbooks for automated response. Each incident is assigned to a specific domain, such as security, IT, health or hunting. This allows teams to tailor workflows and maintain contextual boundaries. This streamlined approach reduces manual effort, improves response times and significantly enhances overall SecOps performance.

CHALLENGES

Security teams today operate in a dynamic and increasingly hostile threat landscape. They are overwhelmed by a continuous stream of alerts from a wide array of security tools, making it difficult to distinguish between routine activity and genuine threats. This alert overload contributes to analyst fatigue, slows down response times and diminishes the overall effectiveness of security operations.

One of the most critical blind spots in many SIEM deployments is the DNS layer. DNS is frequently exploited by adversaries for command and control, data exfiltration and malware delivery. Yet, traditional SIEM platforms often lack the ability to ingest and analyze DNS, DHCP and IPAM telemetry effectively. Without this visibility, security teams struggle to detect stealthy attacks or correlate network activity with malicious behavior.

Additionally, investigations are often hampered by fragmented workflows. Analysts must pivot between multiple consoles and tools to gather context, validate alerts and initiate response actions. This inefficiency delays remediation and increases the risk of missed threats. As organizations scale across hybrid and multi-cloud environments, the volume of logs and alerts grows exponentially, placing further strain on storage, performance and analyst capacity. To stay ahead of increasingly evasive threats, security teams need enriched data, unified visibility and intelligent automation.

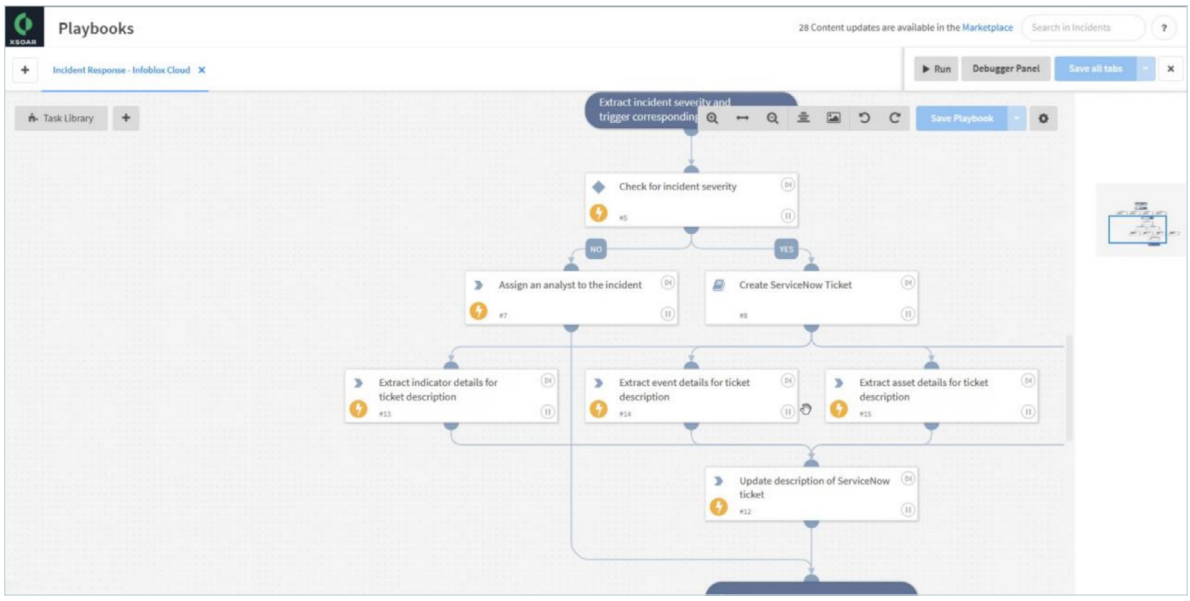

Figure 1. Infoblox and Palo Alto Networks for automated threat containment

KEY CAPABILITIES

Infoblox and Palo Alto Networks Cortex XSIAM and Cortex XSOAR together deliver:

Centralized Event Logging and Visibility:

Infoblox Threat Defense™ enhances security operations by centralizing event logging and visibility. It transmits DNS, DHCP and security event logs to Palo Alto Networks Cortex XSIAM using standard formats such as Syslog, CEF or LEEF. Cortex XSIAM ingests and normalizes this data within its advanced data modeling framework, enabling deep search and correlation across DNS and network activity. This integration enhances visibility into device behavior and threat indicators, accelerates detection of suspicious domains and lateral movement, and enables faster, more effective investigations.

Automated Threat Containment via RPZ

When Palo Alto Cortex XSOAR detects a malicious domain or IP address, it automatically initiates a SOAR playbook that triggers an API call to Infoblox. This action adds the identified threat to a custom response policy zone (RPZ), enabling real-time, network-wide blocking of DNS queries to the malicious domain and ensuring rapid containment of potential threats. This capability is delivered via the Infoblox NIOS integration pack available in the Cortex XSOAR Marketplace.

Proactive Vulnerability Management

Infoblox enhances vulnerability management by detecting new devices as they join the network. This detection can trigger a playbook in Palo Alto Cortex XSIAM that initiates a vulnerability scan using tools such as Qualys or Tenable. Scan prioritization is based on device type, location and threat context provided by Infoblox, enabling efficient and targeted risk mitigation.

BENEFITS

- **XSIAM Efficiency:** Centralize and normalize DNS, DHCP and IPAM data to improve detection fidelity, reduce alert noise and streamline threat triage.
- **XSOAR Effectiveness:** Automate incident response with enriched context and ready-to-use playbooks. This supports faster and more accurate remediation across hybrid environments.
- **Integration Simplicity:** Use native Cortex XSIAM connectors and APIs to onboard Infoblox telemetry quickly and efficiently, without requiring custom development or complex configuration.

- **SecOps Productivity:** Empower analysts with actionable insights, unified dashboards and automated workflows that reduce manual effort and shorten investigation time.
- **Scalable Threat Defense:** Strengthen your security posture with DNS-layer visibility and threat intelligence that scales seamlessly across cloud, on-premises and hybrid environments. The integration supports real-time alerts and investigations, enabling security teams to respond quickly and effectively across distributed networks.
- **Investment ROI:** Maximize the value of your Cortex XSIAM deployment by integrating curated threat intelligence and network metadata from Infoblox. This helps ensure your security investments deliver measurable impact. As a result, organizations benefit from reduced mean time to detect (MTTD) and mean time to respond (MTTR), streamlining SecOps workflows and enhancing overall threat response efficiency.

CONCLUSION

With Infoblox and Palo Alto Networks Cortex XSIAM working together, organizations enhance the performance of their security stack, improve operational efficiency and strengthen their overall security posture. This partnership not only boosts day-to-day SecOps productivity but also delivers long-term value by maximizing the return on SIEM investments.

By extending the integration to include Cortex XSOAR, security teams gain even greater automation and orchestration capabilities. XSOAR enables the creation of dynamic, cross-platform playbooks that streamline incident response, reduce dwell time and ensure consistent, repeatable actions across the SOC.

Together, XSIAM and XSOAR provide a unified, intelligent platform that empowers teams to stay ahead of evolving threats, whether operating in hybrid, multi-cloud or on-premises environments, and maintain a resilient, proactive defense strategy.

PREREQUISITES

Infoblox CSP Requirements

The user must have read-and-write access to Infoblox SOC Insights and IPAM services.

Palo Alto XSIAM Requirements

The user must have read-and-write access to Palo Alto XSIAM and must be authorized to use the APIs.

License Entitlements

IPAM, DHCP, Threat Defense, SOC Insights and Ecosystem.

ABOUT PALO ALTO

As the global AI and cybersecurity leader, Palo Alto Networks (NASDAQ: PANW) is dedicated to protecting our digital way of life via continuous innovation. Trusted by more than 70,000 organizations worldwide, they provide comprehensive AI-powered security solutions across network, cloud, security operations and AI, enhanced by the expertise and threat intelligence of Unit 42®. Their focus on platformization allows enterprises to streamline security at scale, ensuring protection fuels innovation. Explore more at www.paloaltonetworks.com.[1]

1. Palo Alto Networks Delivers Enterprise Wide Quantum Security Readiness for All Customers - Palo Alto Networks

infoblox.

Infoblox unites networking, security and cloud with a protective DDI platform that delivers enterprise resilience and agility. We integrate across hybrid and multi-cloud environments, automate critical network services and preemptively secure the business—providing the visibility and context needed to move fast without compromise.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Version: 20250925v1