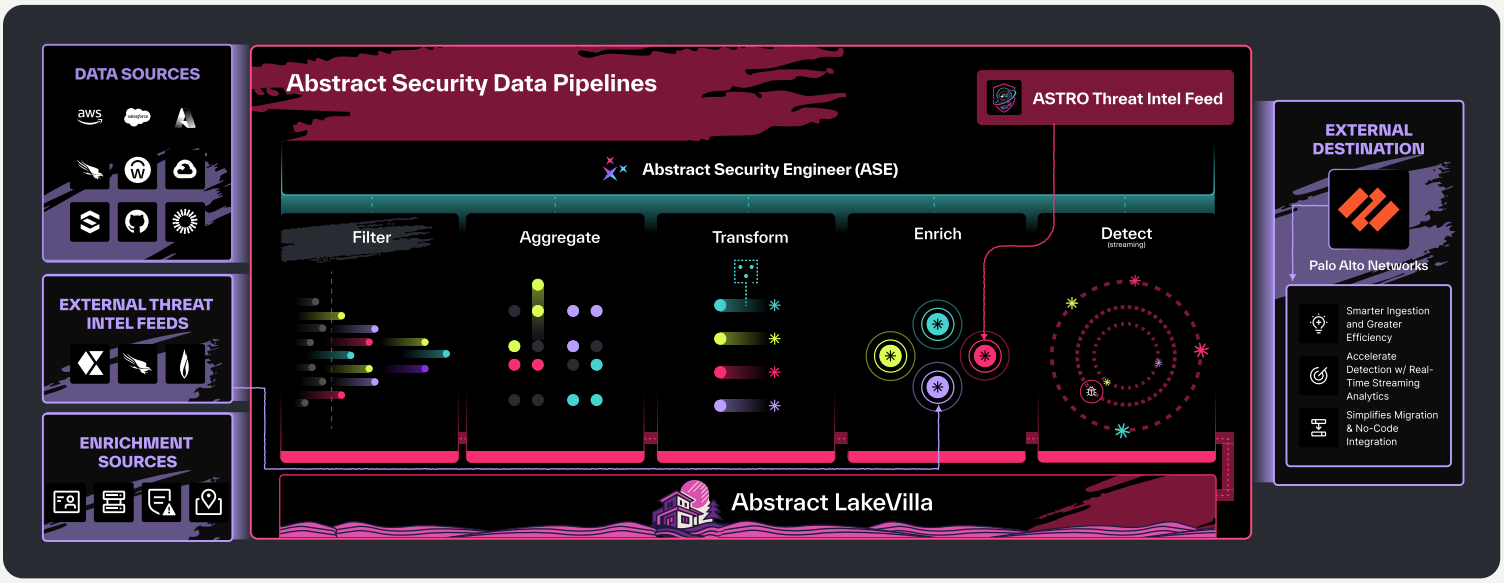
abstract security

Abstract + Palo Alto Networks: Get All Your Data Into Cortex XSIAM — and Make Every Byte Count

Palo Alto Networks' Cortex XSIAM delivers powerful analytics and automation across endpoints, cloud workloads, and network telemetry. Abstract Security expands that reach with 200+ SaaS, identity, and threat-intel integrations—adding live enrichment and cross-source correlation that extend Palo Alto's analytics beyond its native data.

The result: a more complete, efficient, and intelligent SOC. Palo Alto's AI-driven analytics meet Abstract's precision data pipeline and in-motion detections, helping teams **cut noise, control costs, and act on threats faster across hybrid environments.**



Top 3 Reasons Abstract Security and Palo Alto Networks Are Better Together

01. Expanded Visibility Across SaaS and Identity Data

- **Cortex XSIAM** delivers deep analytics across Palo Alto's native ecosystem—endpoints, networks, and cloud workloads—but many SaaS and identity data sources remain out of reach.
- **Abstract** closes that gap with 200+ prebuilt connectors, bringing visibility into collaboration apps, authentication systems, and business platforms that attackers increasingly exploit.
- **Together,** organizations gain a unified, cross-environment view of their attack surface—normalized and ready for XSIAM's AI-driven analysis.

02. Continuous Enrichment and Correlation in Motion

- **XSIAM's** ML-powered analytics and Behavioral Indicators of Compromise (BIOCs) excel at correlating high-fidelity events once data is ingested.
- **Abstract** amplifies this by performing **in-stream enrichment and real-time detections**, flagging suspicious activity as it happens and forwarding those findings into XSIAM for deeper analysis.
- **Together,** teams detect and investigate faster with richer, earlier context before threats escalate into incidents.

03. Faster Onboarding, Smarter Operations

- Expanding XSIAM coverage often means writing custom integrations or managing ingestion pipelines across distributed environments.
- Abstract simplifies this with **no-code pipeline creation, automatic normalization, and adaptive routing**, letting teams onboard new data sources in minutes and scale coverage without extra engineering effort.
- **Together**, security teams modernize faster, turning complex, high-volume ingestion into a streamlined foundation for detection and response.

Building on Palo Alto with Abstract Security

Capability	Palo Alto Singularity™ AI SIEM	Abstract Security
Data Ingestion	Ingests security telemetry from Palo Alto products (Cortex XDR, Prisma Cloud, and Next-Gen Firewalls) and third-party sources into the Cortex Data Lake.	Adds SaaS-native, no-code connectors and streaming pipelines that normalize and enrich data in real time before routing to XSIAM.
Detection Speed	Uses machine learning and behavioral analytics to detect threats once data is indexed in XSIAM.	Performs streaming detections with sub-second latency before ingestion, surfacing early indicators and reducing mean time to detect.
Noise Reduction	Correlates and prioritizes alerts post-ingestion through AI-driven analytics and scoring.	Filters noise and deduplicates events upstream, ensuring only high-value data is sent to XSIAM for analysis.
Threat Detection	Provides autonomous AI-driven detection and correlation across Palo Alto telemetry and third-party data using Behavioral Indicators of Compromise (BIOCs).	Augments XSIAM detections with in-stream rules that identify early signals across SaaS, identity, and cloud data—feeding findings back into Palo Alto's BIOC-driven analytics for richer correlations.
Storage	Stores normalized security data in the Cortex Data Lake for scalable analytics and compliance retention.	Reduces volume and enables cost-efficient retention through real-time processing and selective routing before data enters the lake.

Ideal Use Case:

Palo Alto Networks Cortex XSIAM unifies data, analytics, and automation to deliver AI-driven detection and response across endpoints, cloud workloads, and network environments. Abstract Security enhances this foundation by filling critical visibility gaps, bringing SaaS and identity data directly into XSIAM through a streaming-first pipeline that simplifies ingestion, enriches telemetry in motion, and filters out noise before data lands in the Cortex Data Lake. The result is a more efficient, intelligent foundation for modern SOC operations.

01. More Visibility. Less Waste. A Smarter SOC.

- Cortex XSIAM ingests rich telemetry from Palo Alto products and select third-party sources, but scaling ingestion and enrichment post-collection can increase cost and complexity. Abstract optimizes this process upstream, applying normalization, enrichment, and filtering in real time so only clean, high-value events reach XSIAM. Security teams gain faster onboarding, lower overhead, and more predictable storage and compute usage.

02. Detect in Motion. Respond in Seconds.

- Cortex XSIAM delivers powerful, machine learning–driven detection and automated response. Abstract extends these capabilities with in-stream enrichment and detections that identify early signals from SaaS, identity, and multi-cloud sources, feeding results into XSIAM's BIOC-driven analytics. This combination accelerates detection and response while improving alert quality and reducing noise.

03. Modernize Without the Manual Work.

- Expanding XSIAM to cover new data sources often requires manual setup and engineering effort. Abstract streamlines this process with prebuilt connectors, automatic data normalization, and adaptive pipelines that integrate third-party telemetry in minutes. Security teams gain a unified, scalable architecture that evolves easily with new sources and emerging detection use cases.

04. Better Together: Palo Alto Networks Cortex XSIAM + Abstract Security

- Cortex XSIAM delivers AI-driven detection, analytics, and automated response across endpoints, networks, and cloud environments.

  Abstract Security expands that foundation with real-time streaming ingestion, SaaS and identity coverage, and in-motion enrichment that transforms raw telemetry into high-value insights before it reaches the lake.

  Together, they give security teams **earlier detections, broader visibility, and cleaner data—powering faster, more efficient SOC operations at scale.**