Palo Alto Networks and Elastic

Cost-Effective, Open, and Scalable SIEM Integration

Benefits of the Integration

With Elastic, the leading open source tool for data analysis, users can:

- Store, search, and analyze large amounts of information from Palo Alto Networks Next-Generation Firewalls.
- Take advantage of a cost-effective, scalable, and open alternative to legacy SIEM vendors.
- Create alerts that trigger actions or playbooks in Cortex XSOAR for SOAR use cases.

The Challenge

Relying on traditional security information and event management (SIEM) platforms is no longer a cost-effective strategy for managing the growing volume of data and telemetry necessary to protect your organization from today's rapidly shifting threats.

Elastic

Search. Observe. Protect. From finding documents to monitoring infrastructure to hunting for threats, Elastic™ makes data usable in real time and at scale. This is made possible through the Elastic Stack, the next evolution of the ELK Stack. "ELK" is the acronym for three open source projects: Elasticsearch®, Logstash®, and Kibana®. It's all available both as a service in the cloud and for download. Capabilities of the Elastic Stack provide extra help when users want solutions for enterprise search, observability, or security, such as Elastic's SIEM offering.

Palo Alto Networks

Palo Alto Networks Next-Generation Firewalls offer a prevention-focused solution and architecture that is easy to deploy and operate. Replacing disconnected tools with automated analytics lets your security teams focus on what matters and enforce consistent protection everywhere. Next-Generation Firewalls inspect all network traffic including application data and tie it to associated users regardless of their locations or device types. As a result, you can easily align your business policies to your security rules.

Palo Alto Networks and Elastic

Together, Palo Alto Networks and Elastic developed an integrated solution to help security teams reduce the overhead of maintaining a traditional SIEM by providing a flexible alternative, proven to work in large-scale installations worldwide, for managing your Next-Generation Firewall data.

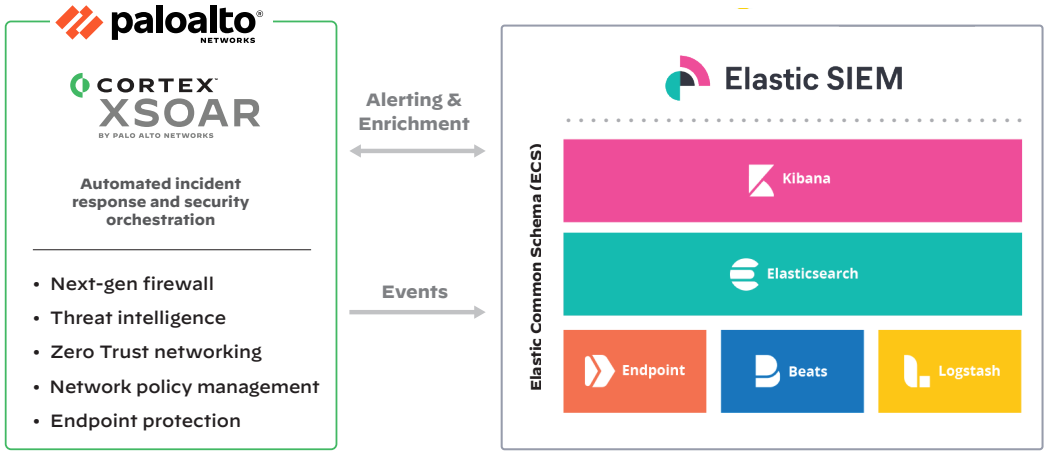

Figure 1: Integration between Palo Alto Networks and Elastic

This integration is made even better with the addition of Cortex™ XSOAR, the industry's leading orchestration, automation, and extended threat intelligence management platform for security response.

Use Case No. 1: Effective SIEM That Scales

Challenge

With traditional SIEM, as your security requirements and data volume increase, addressing advanced use cases and monitoring all the valuable data collected from your Palo Alto Networks Next-Generation Firewalls and other sources becomes cost-prohibitive.

Solution Benefits

Elastic SIEM scales to serve the expanding use case requirements of protecting your organization without sacrificing any of your critical data. Now you can easily ingest and normalize your PAN-OS® firewall logs into Elastic SIEM using the Filebeat Palo Alto Networks module, which leverages Elastic Beats data shipper technology and Elastic Common Schema format. Visualize, search, and correlate Palo Alto Networks logs in Elastic SIEM with flexible Kibana dashboards for real-time threat hunting and automated detection.

Use Case No. 2: Automation for Cortex XSOAR Playbooks

Challenge

Security teams also need to effectively scale their operations to address complex security investigations and response use cases by standardizing processes and minimizing manual tasks across every type of threat.

Solution Benefits

Cortex XSOAR integrates[1] with Elastic SIEM alerting to instantly recognize known threats and trigger automated playbooks so your team can efficiently cut through alerts, qualify advanced attacks, and respond quickly.

About Elastic

Elastic is a search company that powers enterprise search, observability, and security solutions built on one technology stack that can be deployed anywhere. From finding documents to monitoring infrastructure to hunting for threats, Elastic makes data usable in real time and at scale. Founded in 2012, Elastic is a distributed company with Elasticians around the globe. Learn more at elastic.co or contact us at **partners@elastic.co**.

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

1. Cortex XSOAR was formerly known as Demisto, https://go.demisto.com/hubfs/Resources/Solution_Briefs/Elasticsearch/Elasticsearch%20Solution%20Brief.pdf.

paloalto NETWORKS

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