PALO ALTO NETWORKS AND RESPOND SOFTWARE

Technology Segment: Autonomous Security Operations

HIGHLIGHTS

- Automate some of the most important parts of security operations: monitoring, analyzing and escalating the right network threat events to incident response.
- Increase your security team's capacity to apply comprehensive analysis to Palo Alto Networks threat alerts, including low- and medium-severity events.

The problem the Respond® Analyst for Network Intrusion Analysis addresses is nothing new – it's the gap created by exponential growth in security-related data and the shortage of personnel to analyze that data, leaving companies at risk. Up to now, efforts to address this problem have focused on filtering or reducing the event volume to be analyzed. As more and more data keeps pouring in, resources remain tight, the gap widens, and the shortage of skilled personnel continues to appear on nearly every CSO survey as a top concern. Why hasn't this problem been solved?

Respond Analyst

The Respond Analyst is an artificial intelligence-based, streaming analytics expert system that uses mathematics to determine the likelihood and priority of Palo Alto Networks® threat alerts using evidence specific to each organization. The Respond Analyst autonomously performs the security monitoring, analysis, case building and escalation tasks of a skilled network intrusion security analyst. Specifically, it:

- Investigates threats:
  - Evaluates every event with machine consistency and scale.
  - Uses a knowledge base of internal company context, threat intelligence and historical patterns.
- Scopes and builds cases:
  - Groups related events and systems into common security incidents.
  - Builds actionable, detailed cases that explain why incidents were escalated.
- Prioritizes and escalates to incident response:
  - Applies triage procedures, incorporating attack stage, likelihood and asset scope.
  - Notifies incident response teams of the escalation.
  - Integrates with existing workflow and case management processes.
- Improves with feedback:
  - Receives feedback to continuously improve foundational knowledge.
  - Builds and maintains tribal knowledge for future investigation application.

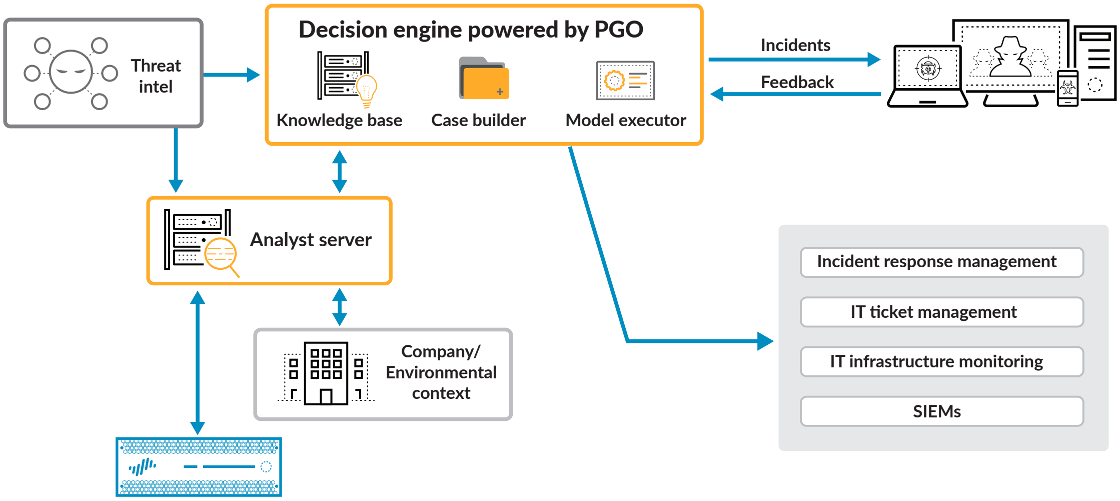

Figure 1: Respond Analyst in a network ecosystem

Palo Alto Networks Security Operating Platform

The Palo Alto Networks Security Operating Platform prevents successful cyberattacks by harnessing analytics to automate routine tasks and enforcement. Tight integration across the platform and with partners simplifies security so you can secure users, applications and data.

The platform empowers you to confidently automate threat identification and enforcement across cloud, network and endpoints using a data-driven approach and precise analytics. It blocks exploits, ransomware, malware and fileless attacks to minimize infections of endpoints and servers. The platform also lets you easily adopt best practices and take a Zero Trust approach to reducing opportunities for attack.

Palo Alto Networks and Respond Software

The integration between Palo Alto Networks and Respond Software allows security teams to monitor, prioritize and analyze alerts generated by Palo Alto Networks next-generation firewalls. Organizations will no longer have to manually analyze threat alerts to determine if events are true positives that require actionable responses.

Like a frontline security analyst, the Respond Analyst escalates triaged and scoped incidents based on Palo Alto Networks threat alerts, including but not limited to alerts on malware beaconing, malware outbreaks, lateral movement through exploitation, and unauthorized scanning and reconnaissance.

Empowering the Respond Analyst to monitor Palo Alto Networks threats within your organization can reduce the total cost of ownership for network intrusion monitoring by removing the human analyst's task of reviewing and analyzing IDS alarms in addition to automating analyst decision-making.

Additionally, the Respond Analyst is skilled at monitoring for endpoint malware based on antivirus telemetries and works with the network intrusion model to gain in-depth understanding as well as mutual confirmation of malicious activity.

Use Case #1

Challenge: Because security teams do not have enough skilled security analysts or engineers to match the alert volume security and network devices generate, they often evaluate less than 0.001 percent of alerts.

Answer: Automate security monitoring of your network intrusion prevention system with the Respond Analyst to achieve 24/7 coverage.

Benefit: Add unlimited, expert-level capacity to your team and elevate your existing analysts to more enjoyable, engaging work than security monitoring. You'll no longer need to turn off signatures from your IPS devices – the Respond Analyst can meet the scale of your enterprise.

Use Case #2

Challenge: The priority of an incident and its scope within an organization can change over time as more related alerts or context are introduced. However, analysts struggle to rationalize new information with existing situations, especially if those incidents involve multiple systems over long periods.

Answer: As a part of the Respond Analyst's decision-making process, it evaluates each network threat alert and any relevant context to determine if the alert relates to a new incident or an ongoing situation. The latter may need to be scoped and reprioritized in light of the new information.

Benefit: Good scoping is important for time to resolution. The Respond Analyst can identify all affected destinations and malicious IP addresses involved in a given incident to facilitate a quick response. Prioritization based on IPS signatures alone doesn't include context. The Respond Analyst factors in asset criticality when deciding priority, which is key to accurate incident prioritization.

About Respond Software

Respond Software redefines Security Operations with the first security expert system, the Respond Analyst. Driven by its patent-pending Probabilistic Graphics Optimization (PGO) technology, Respond Analyst emulates the decision-making of an expert security analyst, effectively becoming a SOC team member that specializes in high-volume, low signal use cases while it applies, adapts and maintains an organization's tribal knowledge 7x24x365. Respond Software was founded by security operations veterans and world class product technologists to serve its customers across multiple industries.

About Palo Alto Networks

We are the global cybersecurity leader, known for always challenging the security status quo. Our mission is to protect our way of life in the digital age by preventing successful cyberattacks. This has given us the privilege of safely enabling tens of thousands of organizations and their customers. Our pioneering Security Operating Platform safeguards your digital transformation with continuous innovation that combines the latest breakthroughs in security, automation, and analytics. By delivering you a true platform and empowering a growing ecosystem of change-makers like us, we provide you highly effective and innovative cybersecurity across clouds, networks, and mobile devices.

Across the world, customers love our security and consistently award us the highest loyalty ratings and net promoter scores in the industry.

Find out more at www.paloaltonetworks.com.

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