PALO ALTO NETWORKS AND SYNCURITY

Reduce Enterprise Risk at Machine Speed with SOAR Platform Integration

HIGHLIGHTS

Palo Alto Networks and Syncurity IR-Flow accelerate an organization's ability to identify, contain, and remediate complex threats as part of its automation and orchestration playbooks. With Syncurity's unique mix of process and automation, the integration provides:

- Real-time search of logs in Panorama or PAN-OS to verify network or user activity and identify potential victims of attacks.
- Rapid containment and remediation of threats through the use of blocks to modify Panorama or PAN-OS.

The Challenge

Most organizations recognize that to keep pace with rapidly evolving threats, changing IT landscapes like multi-cloud deployments, and increases in the attack surface—such as those introduced by the internet of things—they must quickly identify, validate, escalate, and contain risk. Attackers penetrate and exfiltrate data at machine speed, and security operations teams must match them. Together, Palo Alto Networks and Syncurity enable organizations to use tightly integrated, dynamic workflows or playbooks to rapidly triage, escalate, contain, and remediate risks automatically.

Syncurity IR-Flow SOAR Platform

Syncurity IR-Flow® delivers an agile security orchestration, automation, and response (SOAR) platform that reduces cyber risk. Syncurity helps make security operations centers (SOCs) more efficient and effective through the automation and orchestration of tightly integrated alert and incident response workflows. IR-Flow is built by analysts, for analysts, to deploy within hours and calibrate easily to every customer's unique environment for immediate value. IR-Flow uniquely incorporates human analysts into the decision-making loop instead of deploying "lights-out" automation. It also generates a detailed, immutable "security system of record" that enables reporting and measurement, process improvement, and compliance demonstration.

Palo Alto Networks Security Operating Platform

The Palo Alto Networks Security Operating Platform prevents successful cyberattacks through intelligent automation. It combines network and endpoint security with threat intelligence and accurate analytics to help streamline routine tasks, automate protection, and prevent cyber breaches. Tight integrations across the platform and with ecosystem partners deliver consistent security across clouds, networks, and mobile devices, natively providing the right capabilities at the right place across all stages of an attack lifecycle. Because the platform was built from the ground up with breach prevention in mind—with important threat information shared across security functions system-wide—and architected to operate in modern networks with new technology initiatives like cloud and mobility, customers benefit from better security than legacy or point products provide and realize better total cost of ownership.

Palo Alto Networks and Syncurity IR-Flow SOAR Platform

To meet the challenges organizations face, security tools must interact in the context of their business processes, which can differ across individual organizations, industries, and technologies. By adapting the industry's most advanced threat intelligence and prevention into the security operations workflows of Palo Alto Networks and Syncurity, we enable joint customers to move at machine speed, with humans at the wheel.

Use Case No. 1: Threat Identification

Challenge: Security analysts need to automatically validate potential threat indicators without manually logging in, cutting and pasting the fact from an alert, and cutting and pasting the result into a SOAR or security incident and event management (SIEM) case record.

Answer: Palo Alto Networks and Syncurity IR-Flow integration accomplishes this with Log Search, which can be fired automatically, semi-automatically, or by an analyst to enrich an alert with results about an indicator, such as a URL or IP address, including categories like Malicious Score, Confidence, and others. An analyst can query the URL log in Panorama or PAN-OS to determine if one or more users visited a given URL. The Log Search integration can be used to query any next-generation firewall or Panorama log sources, such as traffic, URL, and threat, with minimal configuration.

Benefit: Analysts can quickly determine the level of risk associated with an alert and decide if it should be escalated to an incident.

Use Case No. 2: Threat Containment and Remediation

Challenge: Overwhelmed security teams need the ability to rapidly, automatically contain a confirmed risk by blocking an indicator, such as an IP address, URL, or file hash, at the network and endpoint levels without sending emails, creating IT management system tickets, or logging into multiple system consoles to apply policy changes.

Answer: Palo Alto Networks and Syncurity IR-Flow integration uses the Block Action, which can be fired automatically, semi-automatically, or by an analyst when pivoting response activities to update enterprise protection. The Block Action works by adding an IP address to an address list object associated with a security policy. IR-Flow workflows can optionally require analyst approval before remediation. IR-Flow supports multiple block lists, enabling different block lists for various use cases to be associated with distinct security policies.

Benefit: Seamlessly and rapidly respond to validated threats by systematically containing indicators of compromise across network and endpoint vectors.

Figure 1: Palo Alto Networks and Syncurity integration

About Syncurity

Syncurity® optimizes and integrates people, process and technology to realize better cybersecurity outcomes and accelerate security operations teams by delivering an agile incident response platform. Syncurity's IR-Flow® platform uniquely allows "on the fly" customization to speed deployment, separates alert handling from incident management processes to increase efficiency, incorporates human analysts for more accuracy, and generates a detailed security "System of Record" that enables reporting and measurement, process improvement and compliance demonstration. With pre-built integrations that enable context enrichment and automated action across the security stack, IR-Flow empowers security teams to reduce alert triage and escalation time by over 80 percent and implement consistent, repeatable, and auditable processes for incident handling. For more information, visit https://www.syncurity.net.

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 emboldens their digital transformation with continuous innovation that seizes the latest breakthroughs in security, automation, and analytics. By delivering a true platform and empowering a growing ecosystem of change-makers like us, we provide highly effective and innovative cybersecurity across clouds, networks, and mobile devices. 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