# Cortex XSOAR Automation I Orchestration SOC-as-a-Service I LinearStack

PaloAlto Networks' security orchestration, automation, and response solutions [(XSOAR)](https://register.paloaltonetworks.com/introducingcortexxsoar) have several capabilities for workflow automation to help clients with increased protection and faster response to security incidents, external threats, and other security challenges.

LinearStack, a global cybersecurity partner of Palo Alto Networks based in New Zealand, developed an XSOAR Security-as-a-Service (SOC) based on Palo's tool sets. How a client will maximize the investment in the XSOAR response platform to meet enterprise security challenges is the value of LinearStack's professional services and managed SOC and SOAR automation service.

## Automating Security Functions

Attack surface management with automated processes starts with a solid foundation of integration points, playbooks, incident pages, and other system features that allow for resource orchestration, process automation, case management, and analysts' workflows. Security Operations (SecOps), Development Operations (DevOps), Network Security Operations (NetSecOps), and Application Development Operations (APPDev) all rely heavily on automated functions for their daily operations. Palo Alto Networks XSOAR capabilities provide several tools needed to automate these functions as a service.

### SecOps Teams Enabling Greater Usage of Extended Security Orchestration

A significant requirement for SecOps is to leverage automation and orchestration. Organisations do not have a full complement of qualified SecOps engineers with experience with scripting.

Automation and orchestration allow the organisation to meet its SecOps protection requirements with fewer resources. Timeline

Description automatically generatedXSOAR's playbooks include responses for malware and ransomware outbreaks, account takeover, and brute force attacks.

 These playbooks provide a unified step-by-step process for everyone within the organisation can leverage when dealing with a security outbreak. Each playbook offers the ability to allocate tasks to individuals or groups within the organisation to help execute adaptive security controls to help stop the security breach from propagating. The playbooks are customizable to fit into the organisation's current SecOps work streams.

Along with playbooks, XSOAR has several process automation capabilities connecting to various third-party products. A core component of XSOAR is the ability to remotely connect to a firewall, IDS, or an endpoint security agent and apply a just-in-time security control to block zero-day attacks through automated response PowerShell or Python scripts. Palo's XSOAR has an ecosystem of partners with proven automation response scripts.

### LinearStack XSOAR and Security-as-a-Service (SOC) offering

LinearStack developed their XSOAR and SOC managed service based on the Palo Alto Cortex XSOAR solution. By leveraging existing and proven XSOAR automation capabilities, LinearStack works with clients to develop automation and orchestration workflow, including customizing XSOAR playbooks, automated scripts, and secure API connections to the various Palo Alto ecosystem partner. Even with a consistent set of tools, the client's automation workflows will vary based on resources and network topology. Organisations with nearly 100% of their workloads in a cloud environment may have limited options for automation and orchestration. Clients with a DevOps culture leveraging containers will very likely have more automation and customization needs.A picture containing graphical user interface

Description automatically generated

LinearStack's experts in XSOAR have years of experience working with clients to help customize and tune their XSOAR.

### Leveraging LinearStack for Managed Services - A Partner of Choice

Clients needing extensive automation and orchestration often lack qualified resources to help with the day-to-day operations and upkeep of the various scripts and playbooks. LinearStack's managed XSOAR combined with the market-leading SOC-as-a-Service provides a comprehensive engagement model for all clients to offer a 24 x 7 x 365 daily SOC service combined with a wholly managed XSOAR offering.

## Why Palo Alto Networks partnered with LinearStack

LinearStack is an Auckland, New Zealand-based cyber security service provider with the vision of making enterprise-grade cyber security services accessible to more organisations in the APAC region. Graphical user interface, application, website

Description automatically generated

The growing team of 26 delivers round-the-clock SOC-as-a-Service out of two geo-redundant facilities for its customers.

Our security experts who monitor client networks enabled this 24/7; a dedicated threat research unit to observe and analyze thousands of malware families; dedicated cyber security alignment managers for all clients; and regular context-based threat hunts.

Our XSOAR service, powered by the Cortex platform from Palo Alto Networks, picks up the heavy load of 24x7 cyber vigilance and incident response for you so you can focus on your core business.

According to MITRE ATT&CK's technology evaluations, Cortex XSOAR is a top performer in orchestration and automation. By combining the power of Cortex with our cyber defence expertise and 24x7 monitoring, we deliver a world-class service to protect businesses from advanced cyber-attacks.

**For more information,** [**Contact**](https://www.linearstack.co.nz/contact) **LinearStack:**

Graphical user interface, application

Description automatically generated

## 

## For more information, Contact LinearStack: