Identify and respond to security threats faster with Palo Alto Networks and ServiceNow

The challenge

Security teams today commonly use a combination of email, spreadsheets, and phone calls to manage their incident response processes. This leads to slow detection and containment times that are measured in days and weeks, and can result in costly breaches.

Security incidents also require business context for prioritization and better decision making. Incidents that affect critical services could end up buried on a long to-do list because analysts were unaware of the business impact.

The key to reducing detection and response times lies in automating basic tasks, such as intelligence gathering. This combined with knowledge of the affected asset's importance to the organization allows you to better identify critical threats quickly. Additionally, security response can be improved via orchestration, allowing actions to be initiated from a single platform, instead of dealing with multiple consoles or teams.

The solution

Palo Alto Networks has partnered with ServiceNow to help organizations better respond to security incidents by creating two distinct integrations to connect their respective solutions. The first integration links Palo Alto Networks Next-Generation Firewall and ServiceNow® IT Service Management for basic incident creation. This allows an organization to have a streamlined process for responding to incidents with ServiceNow workflows, routing, and communication tools.

The second integration joins Palo Alto Networks Next-Generation Firewall, Palo Alto Networks WildFire™ cloud-based analysis service, and Palo Alto Networks AutoFocus™ threat intelligence service with ServiceNow® Security Operations for security orchestration, automation, and response. With ServiceNow Security Operations, security teams leverage workflows and automation to cut out manual tasks, thereby accelerating threat identification and remediation.

Use case with Palo Alto Networks Next-Generation Firewall and ServiceNow IT Service Management

A structured process for threat remediation can be created with automated incident creation from Palo Alto Networks to ServiceNow IT Service Management.

When suspicious activity is detected by Palo Alto Networks Next-Generation Firewall, a new incident is created in ServiceNow. This incident triggers custom pre-defined workflows, automatically routing the incident to the correct responders. Service Level Agreement tracking automatically escalates the incident as needed. Knowledge base articles and built-in collaboration tools also help reduce the time to incident resolution. Interactive dashboards keep track of the incident backlog.

Use case with Palo Alto Networks and ServiceNow Security Operations

Threat research can be automated using Palo Alto Networks and ServiceNow Security Operations.

In partnership with

Key benefits of Palo Alto Networks Next-Generation Firewall and ServiceNow IT Service Management

- Create structured processes for threat remediation with automated incident creation from Palo Alto Networks to ServiceNow

Key benefits of Palo Alto Networks and ServiceNow Security Operations

- Accelerate threat identification with automated enrichment from Palo Alto Networks WildFire and AutoFocus
- Speed up decision making with business context for security incidents
- Reduce time to eradicate by initiating Palo Alto Networks Next-Generation Firewall changes from within ServiceNow Security Operations

For example, a threat protection product detects a suspicious file on a server, and a security incident is created in ServiceNow Security Operations. To learn more about this potential threat, Security Operations sends observable data to AutoFocus to search for relevant threat intelligence. A report is attached to the security incident for review.

In parallel, the suspicious file is automatically sent to WildFire for analysis. Using static and dynamic analysis over multiple operating systems and application versions, this cloud-based analysis can identify never-before-seen threats. The resulting report includes a verdict as well as detailed analysis of the file, including behavior, network activity, and processes. This is automatically attached to the security incident in Security Operations for the analyst to review. This search puts the entire wealth of Palo Alto Networks threat intelligence at your fingertips, cutting the time it takes to conduct analysis, forensics, or hunting efforts.

1 File Information

File Type	PE
File Signer	None
SHA-256	9ac69101daee24a43f98f5895415abb1b4b5905020ad93c51254e51e2169e0fe
SHA-1	b7b8a00b772fe99c5d010e77ba1e2849a2c40016
MD5	8b3bcafaa464216b7eeebfbfd869e0d7
File Size	20480bytes
First Seen Timestamp	2016-05-11 23:36:37 UTC
Verdict	Malware
Antivirus Coverage	VirusTotal Information

Figure 1 - This report from Palo Alto Networks WildFire shows the suspicious file is malware

With Security Operations, research was initiated automatically and completed in seconds, meaning the security analyst can review both the incident and valuable context in one place. Security Operations can also automatically retrieve running processes and active network connections from the server in question as well as correlate Indicators of Compromise (IoCs) against threat intelligence feeds.

Using the data from AutoFocus, WildFire, and the IoC lookup, the analyst can determine that the suspicious file is indeed malicious and has also attempted to contact an unknown IP address. The analyst also sees that ServiceNow has identified this incident as business-critical because of the importance of the affected server and the services that depend upon it.

From here, the analyst can follow a security playbook within Security Operations to prevent further infection and remediate the malware. The playbook was customized to the organization's security runbook and built using ServiceNow's workflow tools. The first step is to update the Palo Alto Networks Next-Generation Firewall to block communication with the unknown IP address. This can be done from within ServiceNow Security Operations by creating a new firewall block request. The request can be sent for approval or straight to the firewall. The IP has now been quickly blocked without requiring the analyst to move to a different console.

Now, the analyst can follow the remaining tasks in the response workflow. All tasks and approvals are tracked within ServiceNow, and service level agreement thresholds ensure they are completed on-time. Once the incident is closed, a time-stamped, post-incident review is automatically generated. The post-incident review includes all actions and decisions related to the incident, as well as results from any participant assessments—and it can be used to refine response processes or for future audits.

Take action with Palo Alto Networks Next-Generation Firewall directly from ServiceNow.

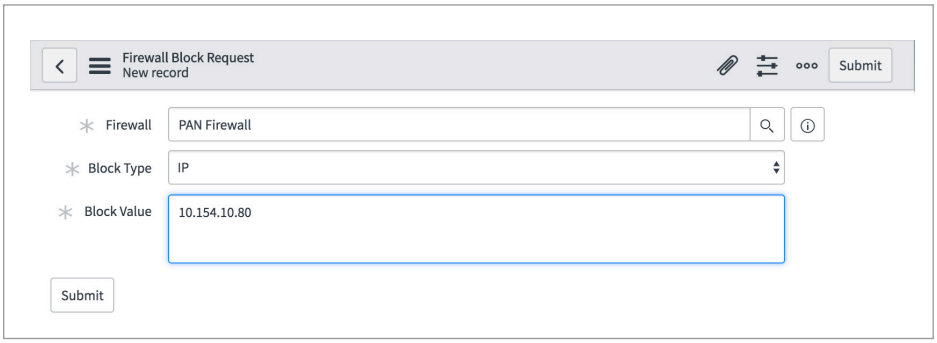

Figure 2 - Firewall block requests can be initiated and approved from within ServiceNow Security Operations.

Summary

By integrating Palo Alto Networks products with ServiceNow Security Operations, analysts can quickly identify and eradicate threats. Automating intelligence gathering with AutoFocus and WildFire reduces investigation time to seconds. Business context tells analysts threats are critical and should be addressed immediately. By using Security Operations with Palo Alto Networks Next-Generation Firewall, analysts can act quickly without logging into a different system. Together, security response is faster and more efficient.

About Palo Alto Networks

Palo Alto Networks is the next-generation security company, leading a new era in cybersecurity by safely enabling applications and preventing cyber breaches for tens of thousands of organizations worldwide. Built with an innovative approach and highly differentiated cyberthreat prevention capabilities, our game-changing security platform delivers security far superior to legacy or point products, safely enables daily business operations, and protects an organization's most valuable assets.

Find out more at **www.paloaltonetworks.com**.

About ServiceNow

ServiceNow was started in 2004 with the belief that getting simple stuff done at work can be easy, and getting complex multistep tasks completed can be painless. From the beginning, ServiceNow envisioned a world where anyone could create powerful workflows to get enterprise work done. Today, ServiceNow's cloud-based platform simplifies the way we work through a structured security response engine. ServiceNow Security Operations automates, digitizes, and optimizes security and vulnerability response to resolve threats quickly based on business impact. Reduce manual processes and increase efficiency across security and IT teams. ServiceNow is how work gets done. For more information, visit **servicenow.com**.

servicenow