ServiceNow and Anomali: Streamline threat intelligence and response

Identifying and prioritizing threats faster is key to effective incident response

Challenge

Today's cybersecurity landscape is dominated by several common challenges–collaboration between IT and security analysts, massive volumes of data, and increasingly deceptive cyberattacks. With more people and devices connected than ever before, these attacks continue to grow at a rate that is impossible for manual intervention alone.

Current security infrastructures offer many tools to managing this information, but incomplete integration between those tools persists even today. This results in a frustrating amount of engineering effort to manage systems while analysts spend time on threats that are irrelevant to their organization. Key indicators of risk to an organization are difficult to identify when the organization's adversaries, including their thoughts, capabilities, and actions are unknown. Due to these challenges, 70% of SOCs say their top challenge is detection of hidden, unknown, and emerging threats.[1]

Today's SOC analysts must be able to identify, prioritize, and respond to threats faster than ever. Knowing your adversary helps your organization stay one step ahead with a proactive security posture.

Solution

Every day new threats are discovered, adding to the list of millions of known Indicators of Compromise (IOCs). This presents organizations with two challenges:

1. Evaluating newly-identified threats to uncover an existing breach

2. Checking millions of IOCs daily to detect newly launched attacks

Securing your organization from unknown threats means taking a proactive security approach. By working with ServiceNow Security Operations, Anomali Threat Intelligence empowers security analysts with an end-to-end security orchestration, automation, and response engine covering monitoring, visibility, and remediation. With Anomali and ServiceNow, analysts can:

- Consolidate security intelligence, visibility, and resolution with the Anomali + ServiceNow solution
- Automate manual lookups tasks using ServiceNow workflows and orchestration for faster, more efficient response
- Improve prioritization decisions by combining Anomali Threat Intelligence with business context from the ServiceNow Configuration Management Database (CMDB)
- Accelerate analyst time to resolution with highly curated Anomali Threat Intelligence
- Gain additional insight into the scope and type of incidents for better classification and assignment to playbooks

ANOMALI™

Benefits

Shrink Resolution Window

By supplying incident context within a single platform for security response, Anomali and ServiceNow work together to streamline the investigation process, thereby reducing the mean time to resolution.

Reduce Alert Fatigue

With an integrated approach towards threat intelligence and management, analysts can use ThreatStream confidence and severity metrics to help prioritize incidents by criticality in ServiceNow Security Operations. This greatly simplifies the remediation process while avoiding overwhelming SOC teams with security alerts.

Understand Your Security Posture

Spend time analyzing what's important with customizable dashboarding, and more.

[1] Source: 2017 Threat Hunting Report, Crowd Research Partners

Using Anomali with ServiceNow

The Anomali and ServiceNow integration leverages a bi-directional workflow that works hand-in-hand to consolidate incident intelligence and remediation processes.

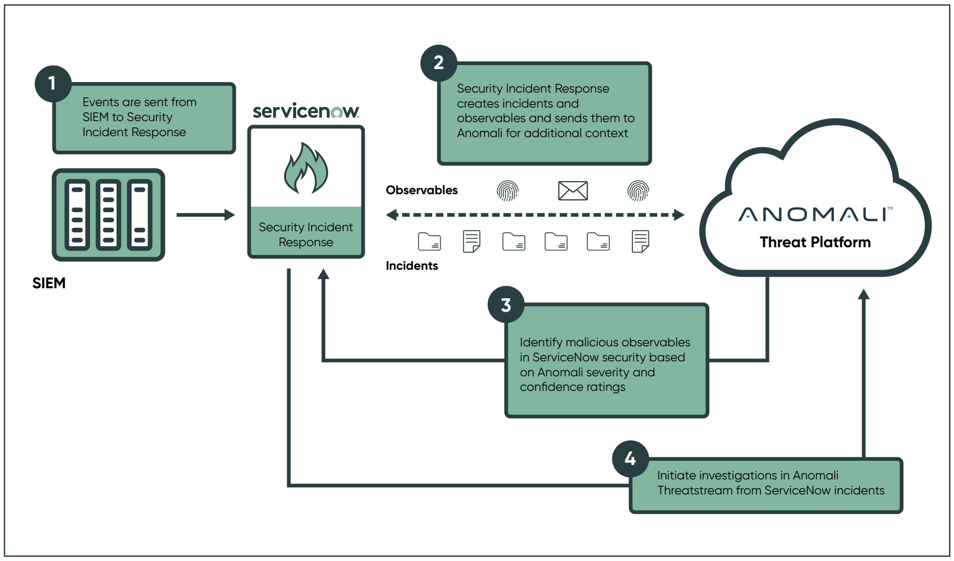
Automatically associate Anomali Threat Intelligence with observables in ServiceNow

Anomali Threat Platform and ServiceNow Security Operations work together to accelerate the investigation and remediation of security incidents. This is accomplished by associating intelligence about indicators of compromise in ServiceNow Security incidents with context from Anomali ThreatStream including threat score, confidence level, source and severity.

To provide analysts additional information within the ServiceNow console, Anomali Threat Intelligence is automatically appended to indicators in the Security Incident table saving valuable time. Analysts can drill down for additional details or link back to Anomali to perform additional investigation.

Submit New Observables to Anomali Investigation from ServiceNow

In certain cases, observables from ServiceNow incidents might not exist already within Anomali. The ServiceNow analyst can select these newly discovered observables to send directly to Anomali so that as more intelligence is collected, they may be associated with future incidents.


1
Events are sent from SIEM to Security Incident Response
SIEM
servicenow
Security Incident Response
2
Security Incident Response creates incidents and observables and sends them to Anomali for additional context
Observables
Incidents
ANOMALI
Threat Platform
3
Identify malicious observables in ServiceNow security based on Anomali severity and confidence ratings
4
Initiate investigations in Anomali Threatstream from ServiceNow incidents

Create Anomali Investigations with a single-click within ServiceNow

ServiceNow Security Incidents can serve as the basis for creating Investigations in Anomali. This allows an analyst to pivot to find new threats that are associated with the same indicators in Anomali. If additional indicators are appended to the originating ServiceNow incident, updates can be sent to Anomali with the click of a button.

Summary

With Anomali and ServiceNow, your SOC team is better enabled to protect your organization's IT assets. The combined solution offers a sturdy foundation for incident response procedures and effective security management.