SECURONIX™ | servicenow®

SOLUTION BRIEF

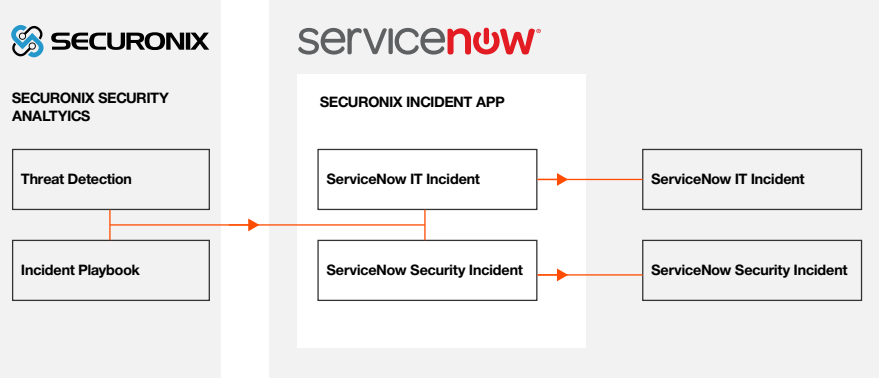
Accelerate Automated Incident Response

Securonix enables you to detect, investigate, and respond to threats in real time. It seamlessly integrates with your ServiceNow Service Management solution to help you smoothly track and manage your incidents, problems, changes, and service requests.

The Challenge

Cyber threats are a top concern for organizations. It is not a matter of if, but when an organization will be attacked. An effective incident response plan needs a solution that can to identify threats in real time, prioritize based on threat level, and respond rapidly to minimize the damage.

Integrating Securonix with your ServiceNow solution provides you with actionable intelligence on your highest risk threats in real time, so you have the contextual information you need to take action. Securonix also consolidates all events associated with a threat into a single incident, reducing the noise so you can focus on the threat.



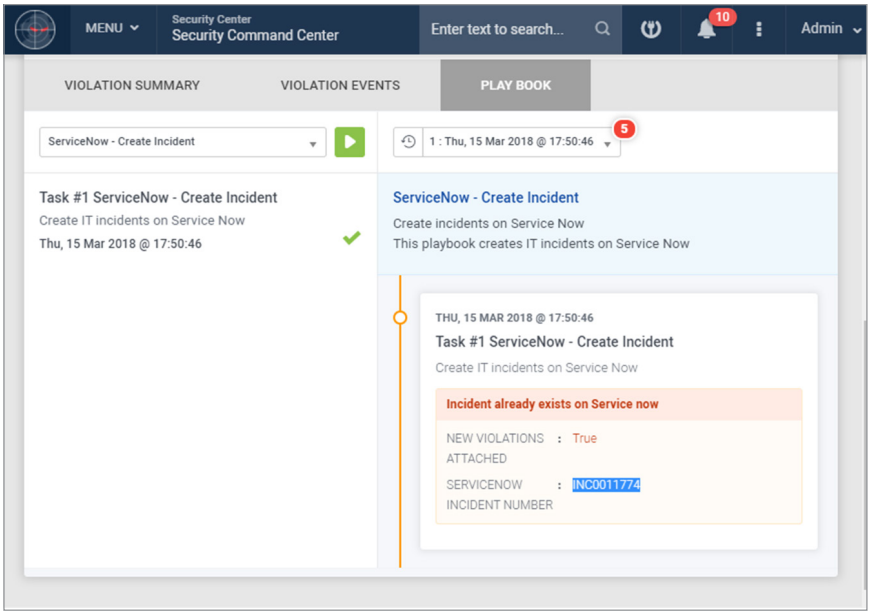
A threat is detected by Securonix and triggers a playbook. As part of that playbook, either an IT or a security ticket is created in the ServiceNow platform.

In addition to creating the tickets, Securonix is also able to pull ServiceNow Configuration Management Database (CMDB) data, which is used to enrich security events in the Securonix platform. Securonix pulls common identifying fields such as MAC addresses and hostnames and correlates those assets with a user. This means that, if a MAC address or hostname is connected to a violation, malware attack, or other incident, the security analyst knows first-hand which user that endpoint belongs to because of the ServiceNow CMDB data. This saves your analysts time and resources trying to track down an otherwise unknown device.

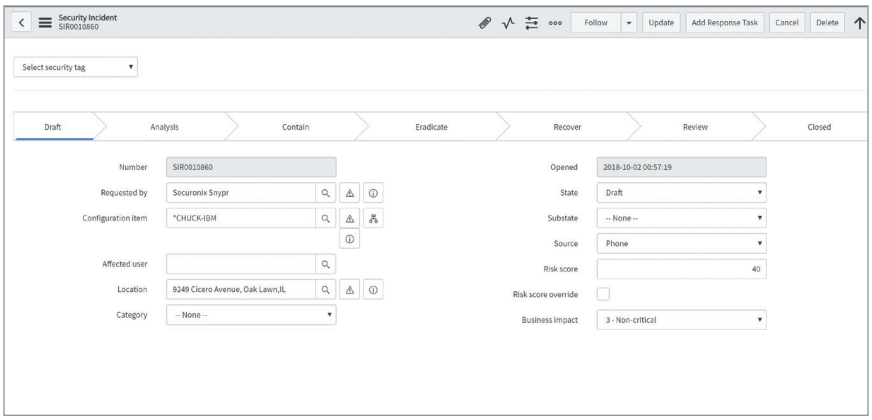
Integration Benefits

- Automated incident creation lets you see threats quicker so you can take action faster.
- Reduce incident noise when related events are aggregated into one incident.
- Reduce mean time to respond when you have access to real-time actionable intelligence.
- Using ServiceNow CDMA asset data, Securonix is able to enrich otherwise anomalous behaviors on endpoints and saves you time and resources trying to track down an otherwise unknown device or event.

Example Use Case



Securonix detects data exfiltration attempts by a terminated user.



Key fields from security incidents are stored within the ServiceNow tables and are displayed directly within the ServiceNow Security Incident UI. Fields include source MAC address, source hostname, destination MAC address and destination hostname. Subsequent data exfiltration events for the same user are attached to the same incident in ServiceNow.

How it Works

- Securonix pulls ServiceNow CMDB data, which is used to enrich security events in the Securonix platform.
- Securonix behavior analytics identifies actionable threats using out of the box threat models that trigger automated playbooks.
- Securonix uses its REST-API based integration with ServiceNow to open an incident ticket and capture the incident number.
- The incident ticket in ServiceNow has an attachment with the complete event details from Securonix.
- If a MAC address or hostname is connected to an incident, the security analyst knows firsthand which user that endpoint belongs to because of the ServiceNow CMDB data.
- Any subsequent violations are added to the same incident ticket in ServiceNow.

About Securonix

The Securonix platform delivers positive security outcomes with zero infrastructure to manage. It provides analytics-driven next-generation SIEM, UEBA, and security data lake capabilities as a pure cloud solution, without needing to compromise. For more information visit www.securonix.com.

About ServiceNow

ServiceNow makes work better. Our applications automate, predict, digitize and optimize business processes across IT, Customer Service, Security Operations, HR and more, for a better enterprise experience. For more information visit www.servicenow.com.

SECURONIX™

LEARN MORE
www.securonix.com

LET'S TALK
+1 (310) 641-1000