

Accelerate Your Cybersecurity Incident Management with Vectra® and ServiceNow

Consolidate and streamline processes to deliver effective and efficient security operations.

A siloed approach to cyber threat detection and response will create unnecessary complexity, slow down the identification of real threats and result in inefficient security operations that ultimately prove to be ineffective against modern attacks. Most importantly, security leaders, management and practitioners will struggle to succeed in stopping a compromise from becoming a costly breach.

By integrating the Vectra Threat Detection and Response platform with the ServiceNow Platform, organizations can streamline incident response processes to manage risk and resilience in real time, detect real threats, automatically prioritize what is urgent and speed up incident response.

- Best of breed cyber threat detection, security incident response and service management solution.
- Erase known and unknown threats across hybrid cloud threat surfaces.
- Rapidly detect, investigate and respond to threats.
- Focus on the most urgent threats.
- Improve incident response efficiency.
- Enhance security incident reporting to senior management.

Key Security Challenges

- Unintegrated security solutions create unnecessary complexity.
- Isolated and inefficient threat management workflows slow down response time.
- Misalignment of security and incident response teams create incident response gaps.
- Poor communication of threat response actions to senior management can hinder the threat resolutions.

IT solutions for cyber resilience

Vectra erases unknown threats with the best AI-driven threat detection and response platform for hybrid and multi-cloud enterprises, delivering unmatched attack surface coverage, threat signal clarity and intelligent control so security teams can get ahead and stay ahead of modern cyberattacks.

- **Attack Coverage** to erase unknown threats across 4 of your 5 attack surfaces – cloud, saaS, identity and networks.
- **Signal Clarity** with Security AI-driven Attack Signal Intelligence™ to automatically detect, triage and prioritize unknown threats.
- **Intelligent Control** to arm human intelligence to effectively hunt, investigate and respond to unknown threats.

The Now Platform from ServiceNow helps organizations optimize processes, connect data and organizational silos to accelerate innovation at scale.

- Automate and optimize security operations work across the enterprise.
- Connect siloes to create seamless experiences for employees and customers.
- Create new value by enabling innovation at scale and speed.

The Vectra platform harnessing Attack Signal Intelligence is delivered via an API to the ServiceNow SaaS tenant through a MID Server.

Entities are prioritized using certainty and threat scores by the Vectra platform and automatically sync with the ServiceNow Platform. There are two Vectra modules available for ServiceNow:

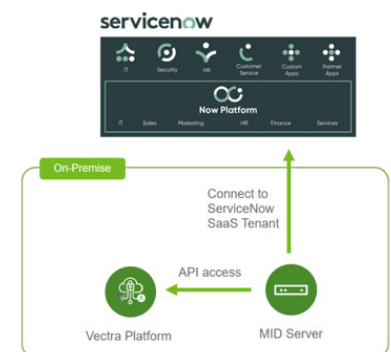
Vectra Threat Detection for ITSM

The ITSM module allows ServiceNow users to manage Vectra events and incidents like other 'helpdesk' events.

Vectra Threat Detection for Security Operation

If this module is used, the ITSM module is not required. It provides the functionality of the ITSM module, but extends it to end-to-end security incident management including case management, runbooks and orchestration.

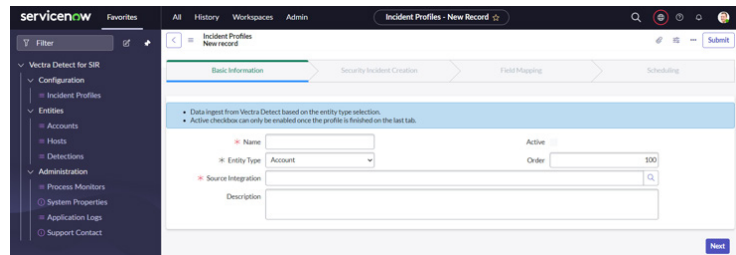
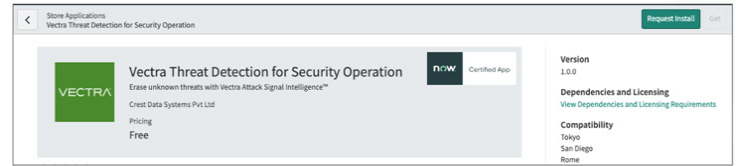
Installation of the selected module is simple and can be accessed and deployed from the [ServiceNow Store](#).



Vectra Threat Detection for Security Operation – Images

Key integration features integration include:

- Create “security incidents” from accounts and hosts.
- Automatically create “security incidents” in ServiceNow based on the specified criteria.
- Fetch detections based on accounts and hosts.
- Download a PCAP file attached to a detection.
- Mark the detection(s) as fixed from ServiceNow to Vectra.
- Manage tags of hosts, accounts and detections from ServiceNow to Vectra.
- Enrich the observables based on IP(s).



What it means for your OT environment

By integrating the Vectra Threat Detection and Response platform with the ServiceNow Platform, organizations can streamline security incident response processes to manage risk and resilience in real time. You’ll enable:

- Consolidated and simplified security operations that are effective, efficient and resilient.
- Removed silos to improve your threat detection, investigation and incident response processes.
- Alignment of your security operations and incident management teams to improve productivity and enhance reporting and communication.

To learn more visit...

[Vectra and ServiceNow Integration Webpage](#)

[Vectra and ServiceNow Integration Blogpost](#)

[Vectra Threat Detection for ITSM – Demo](#)

[Vectra Threat Detection for Security Operation – Demo](#)

[ServiceNow Store for Vectra Apps](#)

About Vectra AI

Vectra AI is the leader in hybrid cloud threat detection and response. Vectra’s patented Attack Signal Intelligence detects and prioritizes threats across public cloud, SaaS, identity, and networks in a single platform. Vectra’s Attack Signal Intelligence goes beyond simple anomaly detection to analyze and understand attacker behavior. The resulting high-fidelity signal and deep context enables security operations teams to prioritize, investigate and respond to cyber-attacks in progress sooner and faster. Organizations worldwide rely on the Vectra platform and MDR services to stay ahead of modern cyber-attacks. Visit www.vectra.ai.