

Nagomi and CrowdStrike: Proactive Threat Defense

Operationalize threat intelligence to provide better visibility into your organization's security posture

Challenges

Modern security teams face a barrage of alerts and fragmented data from a multitude of security tools. Evaluating whether their environment is protected from specific threats becomes a complex, time-consuming process—often delayed by manual correlation, normalization, and analysis. The result: delayed response, misaligned controls, and an inability to answer, "Are we secure?"

Solution

Nagomi and CrowdStrike jointly deliver a proactive, intelligence-driven approach to operationalizing threat data. By correlating CrowdStrike threat intelligence with real-time visibility into an organization's environment, Nagomi maps TTPs to existing security controls and policies. The result: prioritized recommendations, policy optimization, and actionable remediation steps that close exposure gaps and strengthen defenses.

Key Benefits

- **Manage Risk Proactively**
Continuously assess threats and defenses to uncover coverage gaps and prioritize remediation.
- **Strengthen Defensive Plans**
Maximize protection by fine-tuning configurations and activating unused capabilities in your existing tools.
- **Improve ROI**
Drive better outcomes by optimizing your current security stack and freeing up teams to focus on high-impact tasks.
- **Communicate Progress Clearly**
Share risk posture and tool effectiveness with stakeholders using evidence-based insights and actionable plans.



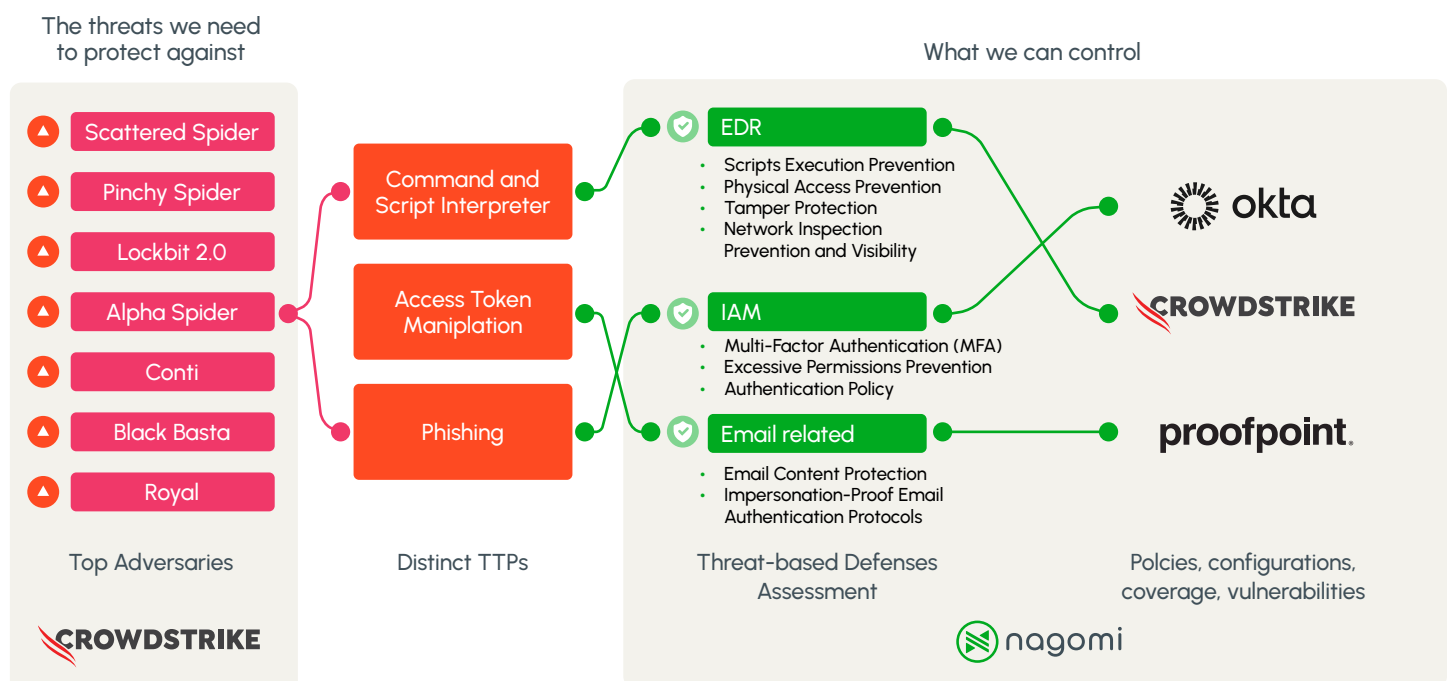
Business Value

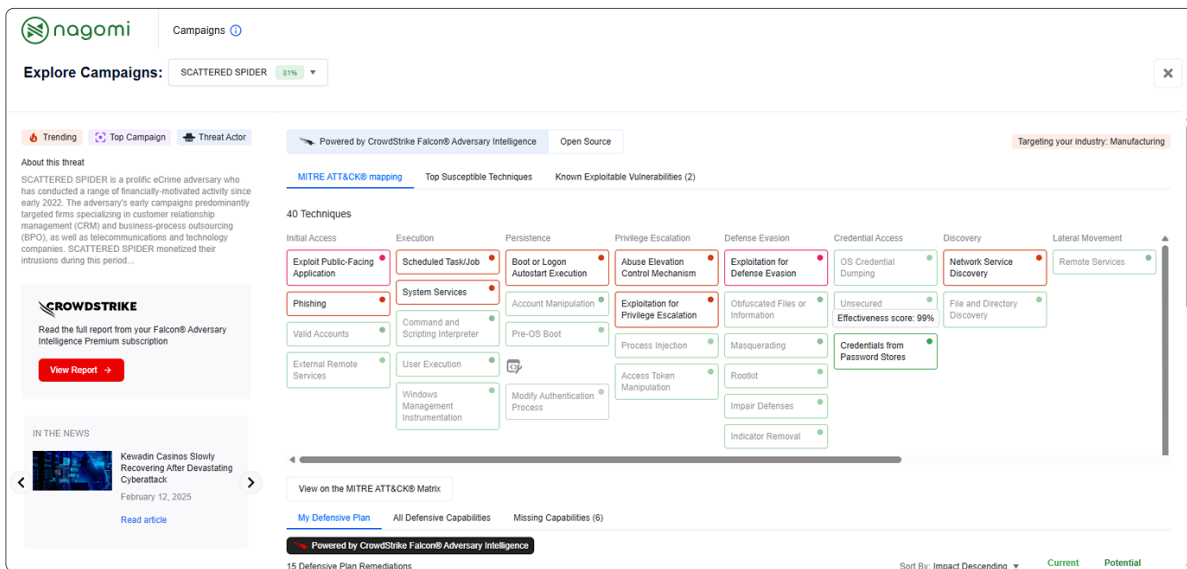
Use Case/Challenge	Solution	Benefits
Assess Exposure to Targeted Threat Campaigns	Nagomi ingests CrowdStrike threat intelligence and maps TTPs to your organization's current security controls, misconfigurations, and vulnerabilities—enabling fast, tailored visibility into specific threat exposures.	<ul style="list-style-type: none"> Quickly determine exposure to relevant threat actors and campaigns Identify and prioritize mitigation of high-risk misconfigurations and control gaps Communicate campaign-specific risk posture to stakeholders with confidence
Optimize Existing Tools for Maximum Protection	Nagomi analyzes current security tool configurations and maps them to threat actor TTPs from CrowdStrike intelligence, providing prescriptive, prioritized recommendations to fine-tune defenses using what you already have.	<ul style="list-style-type: none"> Maximize ROI from existing security investments Reduce manual analysis by automating configuration assessments Improve detection and prevention efficacy across the environment
Demonstrate Security Posture and Progress Over Time	Nagomi translates threat intelligence and configuration insights into visual, evidence-based reports that illustrate current coverage, risk areas, and remediation progress over time.	<ul style="list-style-type: none"> Get clear, actionable insights for security leadership and peers Track posture improvements and remediation outcomes against known threats Align operational efforts with strategic security objectives

Technical Solution

The Nagomi platform integrates with CrowdStrike Falcon® Adversary Intelligence to continuously assess the effectiveness of existing security tools and configurations. It correlates threat actor TTPs with control gaps, misconfigurations, and attack paths, providing MITRE ATT&CK®-mapped insights and customized threat profiles. These insights are translated into prioritized defensive plans, enabling security teams to preemptively act against evolving threats using the tools they already own.

Operationalize threat intelligence by proactively maximizing existing tools utilization to reduce risk surface





CrowdStrike-enriched MITRE Mapping

Key Capabilities

- **Threat-Informed Defense:** Maps adversary TTPs directly to deployed tools to evaluate existing protection and highlight misconfigurations.
- **Prescriptive Remediation Plans:** Provides step-by-step recommendations for optimizing existing policies and configurations to harden defenses.
- **Real-Time Risk Visibility:** Aligns CrowdStrike's threat intelligence with real-world organizational exposures to identify high-priority risks.
- **Campaign-Specific Threat Profiling:** Tailors analysis to industry, geography, and threat actors targeting your organization.
- **Automated Ticketing and Workflow Support:** Pushes recommendations to ticketing systems to accelerate and manage resolution processes.

About Nagomi Security

Nagomi Security helps security teams proactively manage their defenses with a platform that translates threat intelligence into action. By analyzing your existing environment and aligning it with real-world threats, Nagomi delivers clear, prioritized steps to reduce risk and optimize your current security investments. Learn more at nagomisecurity.com

About CrowdStrike

CrowdStrike has redefined security with the world's most advanced cloud-native platform for protecting critical areas of risk — endpoints and cloud workloads, identity, and data.

The Falcon® platform harnesses real-time threat intelligence and enterprise telemetry to automate threat prevention, detection, remediation, hunting, and vulnerability observability through a single, intelligent, lightweight agent. Start a [free trial](#) today.



Learn more at: nagomisecurity.com