nagomi

Global Media Giant Ramps Up a Modern Cybersecurity Practice with Nagomi

Overview

In 2021, a large transatlantic news media company hired a new Chief Information Security Officer (CISO) and tasked him with setting up a centralized information security practice. Upon taking the reins, he opted to fast-track progress by consolidating cybersecurity data and intelligence within the Nagomi Proactive Defense Platform.

The universal access, reliable data, and clear reporting enabled by Nagomi empowered the new security practice to build modern, highly automated operations rapidly. The centralized team led by the CISO now defines and validates policies for detecting threats and communicating risk and investment value to the company's five subsidiary news brands across Europe and the US.

THE CHALLENGE

Building a Modern Cybersecurity Practice in Short Order

The new CISO first created an Information Security Management System (ISMS) practice based on 150+ cybersecurity safeguards and setting up a formal compliance program. His expert central security team defines policies for threat detection, response, and GRC (governance, risk, and compliance) for the company's five subsidiaries in Europe and the US to follow.

The CISO knew centralizing and automating visibility, detection, tracking, and reporting intelligence would modernize operations and take the security program to the next level. Nagomi's Proactive Defense Platform fits the bill by consolidating access and normalizing data from the entire organization in one easy place.

"We didn't go through much of an evaluation process," the CISO recalls. "It was Nagomi or nothing. There's very little out there that compares to what Nagomi does."

A major draw was Nagomi's ability to simplify reporting — making it fast, efficient, and accurate. The CISO was able to showcase how the platform maps existing security tools against common threats and industry trends, highlighting its value across both technical and business stakeholders.

The proof of concept (POC) demonstration convinced management to move forward quickly. The effort to configure and plug security tools into the Nagomi platform went smoothly, thereby allowing their cybersecurity program to hit full stride.

THE NAGOMI SOLUTION

Automated Risk Assessment, Actionable Context and Ongoing Validation

Today, the media company's dynamic and agile Infosec team rely on Nagomi as its 'true North' for discovering, tracking, and communicating risk to the business. The platform ingests, correlates, and normalizes telemetry from security tools and renders an accurate, unified view of the company's attack landscape. Universal access and automated correlation of threat and control data give the team a powerful 'single source of truth' to model and mitigate threats:

Visibility illuminates exposure

Nagomi automates and accelerates the process of finding and evaluating threats that might cause serious problems for the company. Upon ingesting data from the company's security tools, the platform identified exposed assets in its attack surface, including servers with vulnerabilities the team thought had been patched and systems that should have been decommissioned years before.

Nagomi also uncovered coverage gaps — like devices that didn't have endpoint detection and response (EDR) up and running — and overlaps, inconsistencies, and redundancies within policies and workflows. The CISO recalls one instance in which the team was surprised to find they did not have multi-factor authentication (MFA) enabled for every account.

"When we launched the tool, we saw we only had 95% MFA coverage," the CISO says. "We were operating under a false assumption, thinking we had MFA covered because we didn't have access to the identity system to validate 100% coverage. We didn't have it covered, and we had been accepting that risk without knowing it."

According to him, automated in-depth analysis lets the team go beyond making educated guesses and generic statements about risk that management "doesn't want anyway" to provide sound recommendations backed by concrete data.

Context streamlines prioritization

Noting that plugging in and discovering gaps can be "a bit overwhelming," the CISO highlights that the intelligence provided by Nagomi helps defenders decide what to do first. The platform delivers a clear understanding of who might be targeting the company and how its controls stack up — a level of contextualization they did not have before.

"Without Nagomi, it would take days just to pull the data about a particular threat together and manually map it to the MITRE ATT&CK framework and build a narrative around it," the CISO explains, noting the data provided by manual efforts would have been "too technical" for the people asking questions.

"With Nagomi, the assessment only takes a few seconds,". "We can see which controls our individual security teams have activated and where in the kill chain we might intercept an attack. We can quickly take that information, make sense of it, and report out to others.""That was surprising to me," the CISO recalls. "Nagomi helped us identify simple ways to get the full effect out of our tools, things we were surprised we hadn't thought of before."

Modeling threats crystallizes mitigation

The company's security team also conducted a workshop with CrowdStrike that revealed 50+ adversaries that could potentially be targeting them. The visibility provided by the Nagomi platform showed how tools were orchestrated and the interplay between them, making it easier to model specific threats and convey requirements.

"I have a much easier time now explaining to people why certain configurations can cause problems and why certain tools and features need to be enabled," the CISO says. "With the live data in the system, I can pull up an actual ransomware campaign on the screen and show that a threat is in stage one, initial access, and only going to get worse. Seeing that there are multiple accounts that don't have MFA enabled makes the risk very tangible, very real."

Automated Assessments Validate Policies, Check Compliance, and Justify Investments

With corporate cybersecurity team currently using the Nagomi platform on a regular basis to validate deployed security controls, the CISO's vision is that the internal audit team will also begin using the data from the Nagomi platform as a foundational baseline to perform performance audits and optimize risk assessments. For starters, access to reliable data accelerates point-in-time assessments like ransomware readiness checks. "We can simply download and analyze data from Nagomi and either conduct a condensed audit or decide to do a deeper dive to understand the risks," the CISO explains.

The platform also automates the collection of data used to establish baselines and checks the efficacy of policies and safeguards over time. Last but not least, Nagomi helps validate individual subsidiaries' compliance with internal standards.

"For the first time we have that consistent visibility into the business units that participate and are in a position to provide ad hoc reporting very quickly," the CISO says, noting automated assessments significantly improve upon the ad hoc way of doing things. "You could potentially get similar results in terms of automated compliance checks with some GRC tools, but the effort to set those up is an absolute nightmare," he says. "I've done that a few times, and I'm not keen to do it ever again now that I've seen how you can do it with Nagomi; there's no need to go back."

Validation builds trust in an evolving security posture

Facing fewer data privacy regulations than most sectors, news media companies operate under a 'less is more' premise that favors freedom over rules and restrictions. The CISO finds having a tool like Nagomi helps him articulate the dangers of failing to manage risk and comply with internal policies.

Using Nagomi to map security capabilities to an attack kill chain also inspires confidence in the company's posture and individual tools. "Seeing everything laid out across the kill chain and how we have everything orchestrated lets me sleep a little easier." the CISO highlighted. "We'll never be security-driven like a bank, but we've definitely improved on basic hygiene and understanding the risks."

Best of all, Nagomi acts as a universal translator, equipping the CISO and his team to communicate effectively about security matters to practitioners and senior executives across the enterprise.

Nagomi Makes Board-level Reporting Fast and Easy

When the CISO first started running things, regular reporting to senior management about security mainly consisted of point-in-time snapshots produced by internal audits. Now, like many modern CISOs, he reports directly to the company's executive board about emerging risk and the evolution of the security posture multiple times a year.

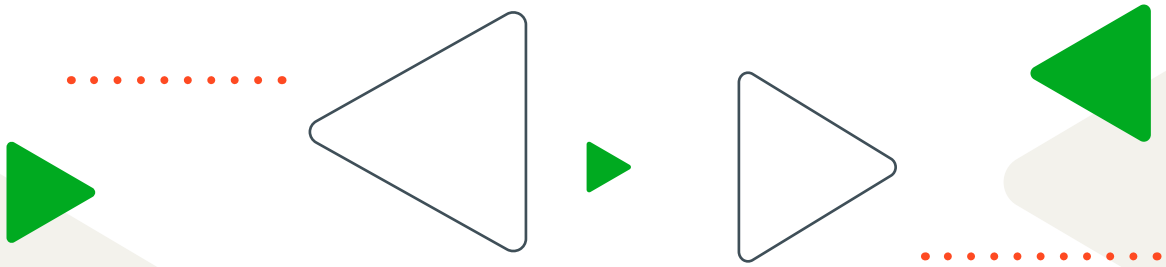
Nagomi provides the high-level explanations and drill-down detail he needs to communicate in language and terms his audience appreciates, as shown by a recent attack on another media company. "What the board really wanted to know was, 'Could this happen to us? Would this threat actor have been as successful in our environment as they were at a competitor?', the CISO recalls. "With Nagomi, it was very quick and easy to import data about that threat actor campaign, check our posture against it, and report back to the board. The findings supported my narrative about the importance of investing to protect our environment against ransomware."

Besides quantifying risk from individual threats, Nagomi helps the CISO and his team convey the effectiveness of security policies and controls and justify future investments. "Knowing that we're doing the right things for the right reasons helps to inspire confidence in the program we're building and justify the spend at a time when we're all being asked to do more with less," the CISO says.

Modern Intelligence Stacks the Odds in Defenders' Favor

In the grand scheme of things, the CISO feels next-level automation and actionability equip security leaders to "reverse the asymmetry" of needing to be right all the time while attackers only need to be right once.

"The intelligence we get from Nagomi puts us in a better position as defenders to understand the adversary and deploy safeguards that interrupt the kill chain based on the most likely path an attack will take," the CISO explains. "Now we're turning things upside down so that the attacker needs to be right in executing their kill chain from start to finish — and their tactics are surprisingly static — and we can disrupt their process multiple times to make their lives more difficult."



nagomi

Learn more at: nagomisecurity.com