



A "BabelFish" for CISOs:

Take the Work Out of
Translating Security Data



▶ EXECUTIVE SUMMARY

In a Nutshell

The board looks to the CISO to interpret security data in terms of outcomes: Can we see where we're at risk and are we safer, stronger and better prepared than we were before? But with too many gaps in coverage, skills, and reporting, the value of data to drive decisions gets lost in translation.

Nagomi Security streamlines the process to help CISOs build trust and create alignment. In this guide you'll see how reliable reporting and clear communication help shift security from a technical cost center to an invaluable source of strategic insight.



Align around a single source of truth



Translate and interpret tool data



Take (or automate) the right actions faster



Why Cybersecurity Needs Its Own “BabelFish”

While cybersecurity protects the business, cybersecurity data empowers it. In fact, a recent survey by IANS Research found that half of all CISOs now meet with their executive boards at least four times a year.¹ It's clear: Boards aren't just looking for technology updates anymore—they want to understand how cybersecurity directly impacts business objectives and makes their companies safer.

When security captures board-level mindshare, it increasingly becomes “everyone's job,” from IT and development teams to business leaders and users themselves. However, it typically falls on CISOs to convey a baseline understanding by continuously answering two questions:

- “Are we *doing the right things* to protect the business?”
- “Are we *doing things right* to operate effectively and efficiently?”

This guide introduces the concept and value of a universal translator, like the “BabelFish” in *A Hitchhiker's Guide to the Galaxy*, that removes the complexities of translating security data into business decisions.

“

We see CISO satisfaction positively correlated with access and influence at the board level. CISOs with a strong rapport with their boards feel more valued and, generally, report they are ‘heard,’ even when there are disagreements on budgeting.”

—Steve Martano, IANS Research

¹ State of the CISO, 2023–2024

Without a “BabelFish,” Opportunity Gets Lost in Translation

The true value of cybersecurity data to drive business outcomes gets lost in translation. CISOs face the challenge of converting complex, technical data in ways that resonate with non-technical stakeholders, but for many, assessing security effectiveness still relies heavily on manual, subjective methods to compile, normalize, and interpret data.

Nagomi Security streamlines this process with results-driven insights to help CISOs foster trust and create alignment. With reliable reporting and clear communication, cybersecurity shifts from being seen as a technical cost center to a strategic business enabler. Without a platform that translates data into accessible insights for both CEOs and SecOps teams, organizations miss vital opportunities to advance key business objectives at the board level.

Reducing risk

Teams are overwhelmed by an avalanche of alerts, vulnerabilities, and backlogs, making it difficult to prioritize the most critical threats. Misaligned priorities and gaps in communication hinder quick action, leaving organizations vulnerable. This not only complicates risk management, but also makes it harder to justify spending, attract top-tier talent, and assure customers, partners, and investors that their data and investments are safe.



Lowering cost

Security investments produce obvious (yet, hard to quantify) savings by preventing data breaches and recovery efforts, brand reputation damage, and fines for non-compliance—but that's just the beginning. Extrapolating insights from security data leads to practical, quantifiable savings, such as reducing security operation costs, retaining skilled analysts, and securing lower cyber insurance premiums.

Better data and more efficient processes also reduce companies' reliance on expensive point-in-time (PIT) tools. For example, annual penetration testing of BAS tools provide snapshots of risk in the moment, but this risk will likely change before you can implement any recommended remediations.

Reducing workload

Every security team's most precious resource is time. Reducing workload reduces burnout, improves retention, and avoids dangerous gaps in coverage.

A clear and unified view of security workflows shows where you can eliminate redundant tools and efforts—for example, patching a vulnerability in one system instead of ten. Automating recurring efforts, like domain maturity assessments, means analysts spend less time compiling and interpreting data for the stakeholders and more time acting on the results.

“

This tool could have helped me plan my budget for next year by showing different threats and risks by focus areas and what projects I should have prioritized.”

—CISO, Global Retailer

“What else could you be doing?” Savings as a Function of Time



Straightforward cost-savings calculations start with determining how many hours full-time employees (FTEs) spend performing specific functions and the time it takes to achieve a point-in-time view of results.

Add in the cost and time it takes to interpret data, prepare and consume reports to get the true cost of manual processes and disparate workflows.

Companies Pay a High 'Reporting Tax'

The more time everyone spends buried in Excel files, the less time they have available to focus on securing and growing your business. In this paper we'll show you how an instantaneous understanding of data translates into faster, more efficient security stacks that net security teams the credit they deserve. And, how Nagomi's Proactive Defense Platform prevents value from getting lost in translation.

Security Leaders Say It Best . . .

“

Nagomi will bring down my time spent to make configuration changes to my security stack from **2-3 months to 2-3 days.**”

“

We spend 5-8 hours a week, or **350 hours per year**, meeting with vendors to understand new features and values. Nagomi automates this process, freeing up our security engineers and aligning with our existing tool roadmap.”

“

When we look at how much of my time as the CISO and your time as the CRO is spent answering the question, "What is our control effectiveness'? **the cost of that time is crazy.**”

The Communication Breakdown: Stakeholders Speak Different Languages

Universal access to a single set of security data won't automatically equip everyone to leverage its full potential. Security practitioners need clarification on what to do first, while CIOs and board-level executives just want to know how well things worked. In both cases, it falls to CISOs and other security leaders to translate complex data into crystal-clear recommendations.

Practitioners: What Should We Do First?

SOC analysts, SecOps, incident responders (IR), and CTI teams all use telemetry from multiple security tools (often 15+) to understand and mitigate risk, and to respond to C-level requests about a particular threat appearing in the news. Since the alerts have practitioners outnumbered, the process starts with choosing where to focus first.

This decision requires consistent threat intelligence, full visibility, and correlation of data about threats, assets, policies, and controls. Aggregating data manually could take multiple security analysts days or weeks to understand risk from a single known threat. Other work gets delayed and, in the meantime, the threat landscape continues to change.

Prioritization also requires analysts to 'slice and dice,' and drill down to evaluate risk from business leaders' and adversaries' perspectives:

- What is the company's risk level against a particular threat?
- Which specific assets are being targeted by a particular threat group or technique?
- Which of our assets and business groups face the greatest risk and why?
- What controls do we have in place—and available—to deflect this threat?
- What, if any, steps should we take next?

Security Simplified with a BabelFish

To help the team prioritize threats and report progress to CISOs, teams need a unified picture (without going tool-by-tool) that shows:

- Which tools have visibility to which assets
- What controls and policies currently protect each asset
- What steps need to be taken to mitigate risk
- What steps need to be taken to accept certain risk
- Whether the steps taken helped mitigate risk

CISOs: What Do We Need to Do Next?

Where practitioners need details, CISOs and other security leaders need context to understand and communicate what matters. CISOs face the greatest communication challenge in that they sit between practitioners and board-level executives translating the same data into two very different perspectives. Striking ideal balance means communicating:

To practitioners: "Where to focus":

- Changing priorities
- How to allocate or redirect resources

To the board: "How well, and why, it's working"

- Risk posture against a particular threat
- Overall security posture and trends
- Where gaps still exist and additional investments might be required to mitigate risk

“

The visibility and posture of our whole estate is a huge challenge for us. We are still simply taking feeds from different tools and using Excel spreadsheets and PowerPoints and prioritizing by a 'gut feel.' It's extremely inaccurate."

—CISO, Fortune 500 Consumer Goods Company

“

If you can help me show 'here's how we rate ourselves,' I can confidently present that to the board. The goal is to provide context that proves the security team's credibility, whether it's highlighting weaknesses or showing the overall security status."

—CISO, Fortune 500 U.S. Bank



Security Simplified with a BabelFish

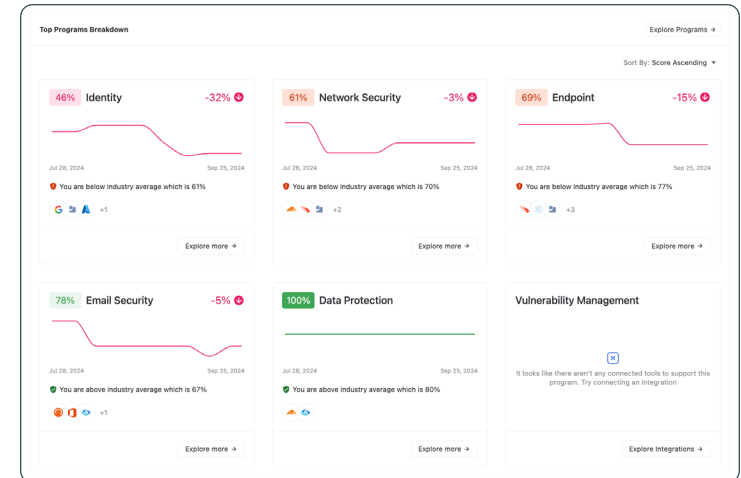
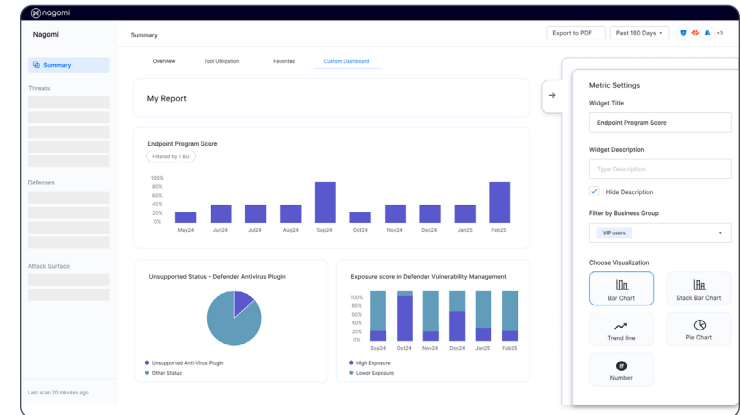
Here again, a security translator saves CISOs from having to go spreadsheet-by-spreadsheet, or dashboard-by-dashboard to interpret data. It provides:

A consolidated, normalized view of your attack surface that shows how well your company is—or could be—mitigating risk from a particular threat with the tools you already own. The dashboard combines data about threats and vulnerabilities targeting your industry (or a particular asset), with data about security controls, available protections, and applicable policies. This alone saves weeks.

Drill-down context and control that maps threats to assets and business groups, interpreting risk in context. For example, if you have accounts not yet protected by multifactor authentication (MFA), you need to know whether they're privileged or admin accounts.

Risk interpretation to ensure relevance and credibility, then translating numbers into next steps. The data should help CISOs present and translate known risks and why business or IT leaders may have chosen to accept the risk.

Fast, easy ticket and report creation to direct the staff and deliver board-level reports in hours instead of weeks.



Board / Business Leaders: Are We (More) Secure?

Senior executives and board members need assurance that their investments are safe, sound, and generating the expected returns. This group does not typically have direct access to security platforms, however they are briefed quarterly on the state of the company's security. Timely reports tailored to their level of technical knowledge (or lack thereof) should explain your company's security posture in layman's terms in order to instill confidence, secure funding and customer loyalty, and satisfy due diligence during mergers and acquisitions.

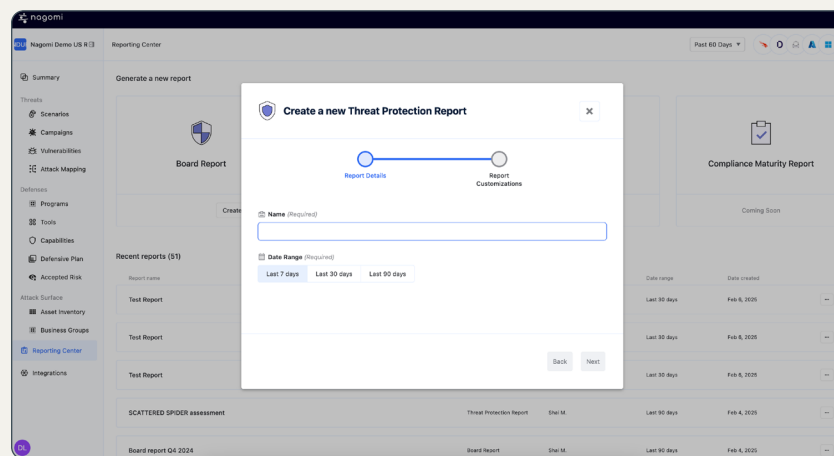
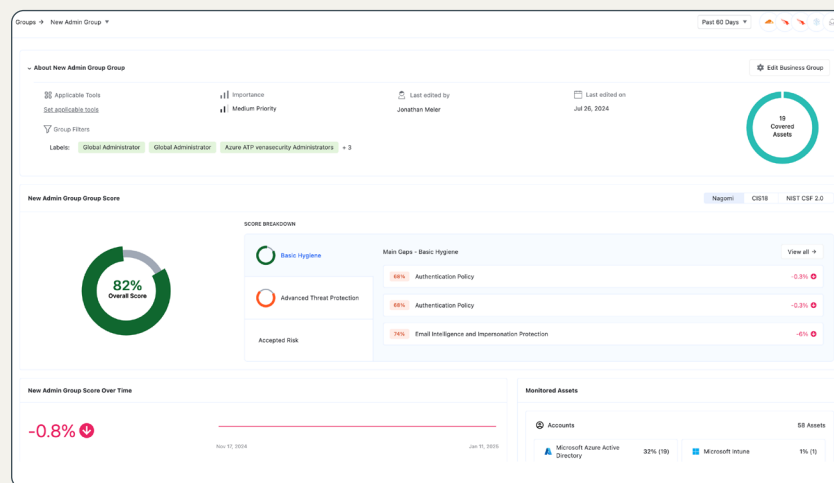
"Are We Moving the Needle?": Security's Common Denominator

At the end of the day, effectiveness is the metric that matters, and the one CISOs struggle most to measure and defend. A security BabelFish needs to help everyone answer the same three questions:

- How can we maximize the value of our existing tools and resources?
- Where should we focus resources and budget for the greatest impact?
- How can we simplify reporting and governance?

Now, let's take a look at how that works in practice.

Nagomi Custom Board Reporting



▶ PART II

The Role of A Universal Translator

It happens every day: a major cybersecurity threat hits the news, and this time it targets your industry. Your CEO immediately pings the CISO: "Are we protected from this . . . Scattered Spider?"

To pull together an answer, the CISO reaches out to the Threat Intelligence team for details about the attack, and then to the SecOps team about how the company's current security measures stack up against the attacker's techniques. Pulling this information together takes lots of work — work that gets done manually and delays or preempts other work from getting done.

The CISO then attempts to map data about the company's assets, exposure, and defensive controls against the threat actor and attack techniques by working in spreadsheets and PowerPoints. This also takes time — and often fails to render a complete picture. By the time the CISO creates a 'so-so' answer, the CEO is asking about the next threat.

That's the "Before": the day-to-day reality that costs companies millions of dollars and cycles per year.

"Thanks for the quick turnaround"

Nagomi's Reporting Center and "Threats in the News" feature make it easy to track cybersecurity news and craft compelling narratives for executives quickly while also equipping practitioners with contextual insights to take the right action.



- Unique threat profiles
- Real-time context
- Actionable intelligence
- Automated mapping
- Prioritized response

The “After”

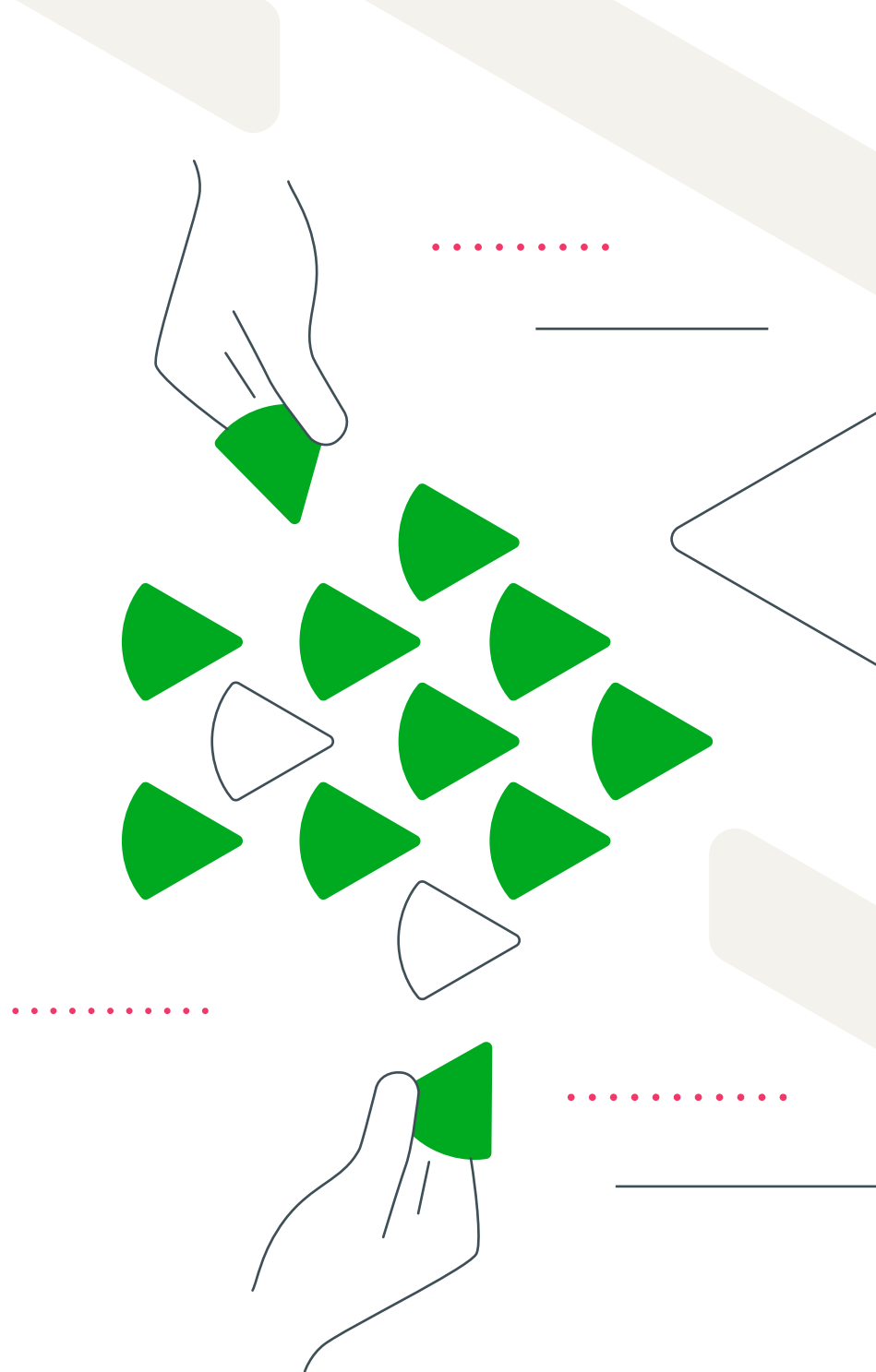
With a security “BabelFish” to translate data into clarity, everything changes. The CISO logs into Nagomi’s Proactive Defense Platform and sees all the disparate pieces of the puzzle assembled perfectly in one place.

Any user can view a campaign page for Scattered Spider and get an overview or detailed analysis of your organization’s resilience against it — all without bothering or derailing individual teams.

A complete view includes:

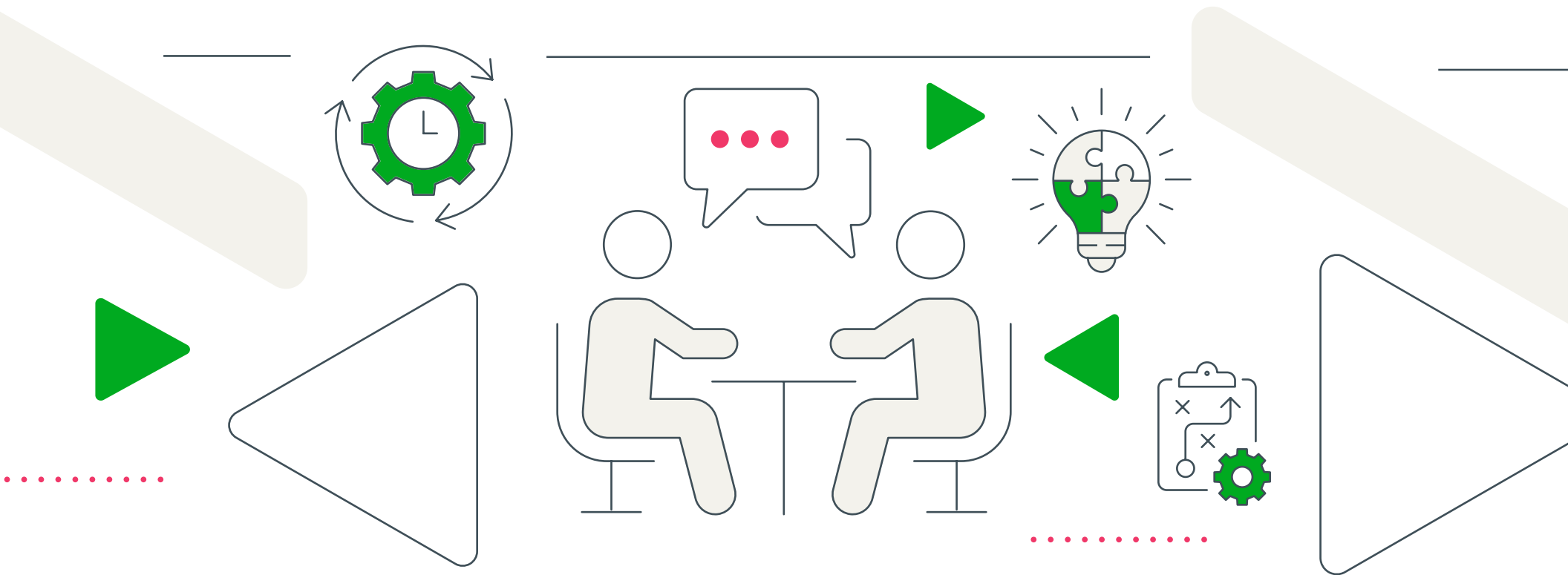
- A clear description of the attack
- Corresponding news articles for additional context
- Technical details
- A MITRE ATT&CK map showing techniques used in the attack
- Prioritized recommendations for mitigation based on your unique threat profile

In the next section, we’ll cover the seven essential questions every CISO should ask and how a universal security translator can answer them in clear, jargon-free terms and speak to key stakeholders in metrics that matter.



The 7-point Security BabelFish Checklist: The Human Element

Even though platforms and portals can automate the heavy lifting of report generation, it's still up to people to present, explain, and defend the findings. Incomplete or inconclusive data only delays critical decisions, making it harder to drive action, justify investments, and plan ahead. Modern security teams continue to drown in tools, overwhelmed by data and stuck in reactive cycles.



1 To Build Confidence

Questions to Ask: Do we know if we're affected or targeted by this threat? Are we protected, and if so, how well?

What to Do: If the answer is unclear, how do we confirm the facts?

Why It Matters: Confidence comes from clarity—knowing exactly where we stand.

2 To Take Action

Questions to Ask: What actions have we taken? What's still pending, and why? Who's responsible, and when will it be done?

What to Do: Make sure every step is clear and accounted for.

Why It Matters: Action is about accountability—keeping things on track and transparent.

3 To Make the Right Investments

Questions to Ask: Do we have the right tools and people to address this? Are the tools set up correctly and being used to their full potential?

What to Do: Calculate the cost of addressing this threat—how many cycles will it take to prevent, investigate, or mitigate it?

Why It Matters: Efficiency means cutting down on wasted resources and making sure we're getting the most out of what we have.

4 To Recruit and Retain People

Questions to Ask: Are we relying solely on automated data, or is there a smart human validating it? Is this issue contributing to analyst burnout?

What to Do: Understand the human side of security—balance automation with the expertise needed to make decisions.

Why It Matters: Keeping your team fresh and engaged is key to long-term success.

5 To Make the Most of Time

Questions to Ask: How up-to-date is the data we're working with? Will it still be relevant when we take action?

What to Do: Ensure data is timely and relevant by the time decisions are made.

Why It Matters: Speed matters, but so does accuracy. You need data that moves as quickly as your team does.

6 To Eliminate Fire Drills

Questions to Ask: Are we able to communicate insights without scrambling? Are we diverting resources unnecessarily or leaving gaps in our response?

What to Do: Eliminate chaos by ensuring the right people get the right information, without unnecessary distractions.

Why It Matters: Efficiency is everything. A well-organized response reduces stress and improves results.

7 To Make a Real Difference

Questions to Ask: Are we effectively moving the needle on our security goals? Does our communication make the impact clear, without leaving people to figure it out for themselves?

What to Do: Focus on measurable outcomes and clear communication of progress.

Why It Matters: Progress is defined by results. Make sure everyone sees the real impact of your work.

★ Bonus: To Sustainably Grow

Questions to Ask: Is our security program scalable? Can it adapt as our company grows?

What to Do: Build for the long term by creating a flexible and scalable security framework.

Why It Matters: Sustainability is about future-proofing—ensuring security keeps pace with the business.

The Right Solution . . .

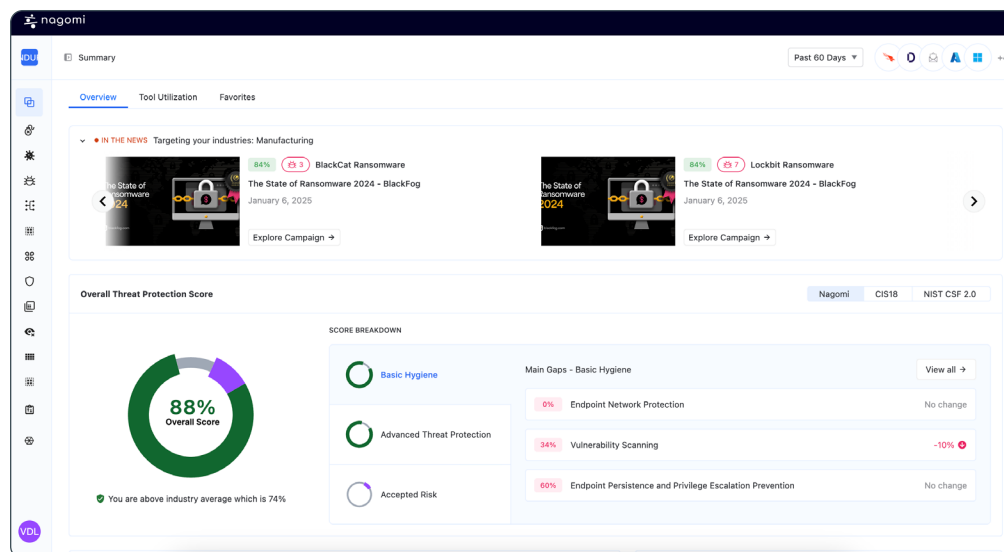
A security BabelFish coalesces the vantage points of multiple tools and categories to correlate assets, defenses and business context—all in one place. Drill-down analyses and roll-up reporting equip defenders to evaluate how well assets are configured against a particular threat and communicate what happens next.

Unify. Operationalize. Enable.

Effective reporting starts with easy access to a single set of unified security data that allows professionals to collaborate and prioritize effectively, and provide leadership with data-driven updates. These collaborations ensures organizations can track and measure complex outcomes with greater confidence.

The result is threefold:

1. **Alignment.** An assessment of your current coverage, effectiveness, and alignment to policies.
2. **Action.** A prioritized, data-driven plan to remediate the gaps and exposures in your defenses.
3. **Automation.** Your own customizable dashboards and reports to unify your organization around common security benchmarks and goals.



Translate Your Own Data into Decisions – with Tools You Already Own

Reliable, automated reporting must replace manual efforts that drain resources and compromise your team's ability to act and stay agile. A clear understanding equips organizations to unify data across their controls, operationalize threat intelligence, and turn reporting into a strategic asset.

Nagomi Turns Reporting into Board-level Rapport

Nagomi redefines how CISOs approach security program effectiveness with a command center that simplifies data. The Nagomi Proactive Defense Platform pioneers a new era of effective, relatively effortless translation of security data to maximize controls, minimize exposure, and empower teams.

The only proactive defense platform to bridge the gap between tactical execution and strategic planning, Nagomi allows everyone to work with the same unified dataset so they can collaborate, prioritize, and communicate effectively. With Nagomi, create a unified threat-centric view of your security posture to measure and enhance the efficacy of your security program.

Experts Interpret the Value of Nagomi



Analysts say:

Nagomi leverages the value of, and takes the work out of reporting.



Security leaders say:

"When I first saw the platform, I knew it was perfect for me as the CISO. While it's great for my endpoint engineers, the real value is having all the information I need in one place. That holistic view is essential for security professionals."

—CISO, Insurance Company



Practitioners say:

"I have no way to prove what I say I do and with your tool I can."

— SOC Analyst, Global Bank

See What Your Data Has to Say

Interested in learning more? Request a demo today to see how Nagomi's Proactive Defense Platform translates your security data into action, alignment, and acknowledgement of its value from the top down.

LEARN MORE



ABOUT NAGOMI SECURITY

Nagomi automates the process of proving your security is actually working. Our platform unifies data across your assets, defenses, and threats to clearly illustrate your security program is both efficient and effective to key stakeholders. By maximizing existing investments, reducing threat exposure, and improving alignment, Nagomi is the only Proactive Defense Platform to turn cybersecurity from a technical cost center into a strategic business enabler.