Operationalizing Continuous Improvement in the Age of Advanced Threats

As a chief information security officer (CISO) or security operations center (SOC) leader, you're expected to do the impossible: ensure your organization is secure. It's a responsibility executives and board members place squarely on your shoulders, even though you know that complete security is never guaranteed.

It's an inconvenient reality that senior leadership teams struggle to accept—that irrespective of investment, sophistication, and expertise, the goalposts of security maturity will always be shifting, and the finish line will always be moving farther away.

Because, as you know better than most, the environment is constantly evolving—both internally as the security perimeter shifts and expands, and externally as new threats emerge. This means that your organization's security posture can weaken even as robust SOC processes and practices are strictly followed.

Consequently, there's always the potential for new detection coverage gaps to open; and in all likelihood, gaps already exist, even if no one has noticed them yet. So, while security leaders can never promise that the organization is fully secure, you can promise that you're enabling and ensuring the continuous improvement of security operations.

But these promises can't be empty, so how can you guarantee this is the case? How can you put systems and frameworks in place that will not only identify coverage gaps but also confirm that they have been successfully closed? And, just as significantly, how can you prove ongoing progress to executive and board stakeholders?

These are the questions you should be contemplating right now. And your ability to both deliver and demonstrate continuous improvement of the SOC should be a top priority.

Discovering Detection Gaps is a Challenge

Empowered and emboldened by advances in artificial intelligence (AI), threat actors have never been as tenacious or as numerous as they are now, launching identity-based and AI-augmented attacks on immense scales. If there's a gap in detection coverage, it's not a matter of whether it will be exploited, but when.

Gone are the days when security teams could wager that their potential vulnerabilities would be overlooked as long as another organization is weaker. Each year, SOCs effectively make bets on which gaps they need to prioritize with their finite resources, and which to deprioritize. And each year, some of them inevitably lose those bets. Those are the ones that end up in the headlines for all the wrong reasons, hurting everything from their company's market value and brand reputation to the trust and confidence of their customers.

That means that maintaining a comprehensive view of security coverage is crucial, as is spotting the coverage gaps before adversaries get the chance. But this is no simple task. Different products and vendors generate logs and alerts in different formats, with no coordination between them; amid the disparate noise of these fragmented environments, it's not only difficult to understand what to triage, it's also challenging to obtain an objective measure of what's working, what's not, and what might be missing.

A detection gap can occur due to a lack of software, but it could also occur because of a false sense of security when the SOC has the right tool, but analysts don't realize that it hasn't been configured or optimized in the way it needs to be.

What every security leader needs is an overview of the products and processes that logs are coming from, the detections associated with them, and the coverage that the current infrastructure provides. Then, this needs to be mapped against a framework such as MITRE ATT&CK® to see which attacker techniques they are most vulnerable to.

This can be a complex undertaking, but it's necessary to create an actionable strategic plan—one that can be communicated not only to the SOC team, but to stakeholders across the business.

Can Continuous Improvement Be Proven?

On the topic of communicating to stakeholders, another problem security leaders must navigate is providing meaningful metrics to show what is and isn't working. When security tools are doing their jobs, there isn't much to report, and the activity of the SOC goes unnoticed. But as soon as a serious incident takes place, the situation reverses, and you and your team find yourselves under scrutiny.

This is complicated by the fact that many traditional measures of TDIR effectiveness, such as mean time to detect (MTTD) and mean time to remediate (MTTR), are moving targets because as detection capabilities get better, the scores may worsen due to the ability to identify new issues.

Other typical metrics such as vulnerability counts are of questionable value, since they're really not much more than long, technical lists that only factor in known risks in the environment. So, to prove continuous improvement—and do so in a way that resonates with key decision makers at the executive and board level—you must think beyond these conventional indicators. That means taking a more informed, intentional approach to evolving your cybersecurity capabilities. Here are three important steps:

1. Conduct a What-If Analysis

You run your SOC on a robust architecture, purposefully pursuing well-defined objectives. But gaps can emerge anywhere, at any time: the dynamic business environment may alter log sources, modifying infrastructure may break compatibility and communication between tools, or the threat landscape may become more complex and adversaries will gain new capabilities.

Conducting what-if scenarios is essential for examining how changes to the environment can have cascading effects on security posture. But these are only helpful if the SOC has the means to model these scenarios accurately and comprehensively.

An advanced security information and event management (SIEM) solution is key here. A good SIEM tool should centrally collect, store, and enrich log data because having a coordinated, consolidated, and consistent understanding of the activity and events in the environment is fundamental. So, too, is having a full view of the products, processes, configurations, rules, and users that constitute it.

This forms a strong foundation for what-if simulations. You and your analysts can map the inputs collected by your SIEM to gain insight into where you have coverage—and, by extension, get a much clearer view of where gaps and vulnerabilities still exist. You can also model how new additions to your environment will affect your security posture.

2. Build Out the Strategic Plan

When security teams know what they're missing, they know what they need. So, after modeling their coverage with what-if scenarios, you can be intentional about how to specifically and impactfully improve your security infrastructure.

Too often, purchasing new products is a reactive process, whether due to pressure to follow market trends, persuasion by a particularly compelling vendor pitch, or repair and recovery after an incident. But really, it should be proactive; preemptive cybersecurity solutions will account for half of IT security spending in the next five years, up from under 5% in 2024 (Gartner). As such, new products and practices should be selectively incorporated to measurably strengthen areas of weakness.

When strategic planning is done proactively instead of reactively, and based on real rather than hypothetical needs, you can project costs, set budgets, assess potential ROI, and measure progress against tangible goals—such as closing a specific gap by a certain amount within a defined time.

3. Communicate It Impactfully

You know your security organization is often viewed as a cost center, which makes justifying expenses to senior stakeholders a constant challenge. Even though the contributions to the enterprise are vital—protecting employees, customers, data, business value, and reputation—investments in cybersecurity don't yield a quantifiable dollars-in, dollars-out return.

Thus, each time a new program or product is proposed, executives and directors ask the same question: "Will this make us secure?" And given that there's no such thing as complete, guaranteed security, it makes it more crucial than ever that you can demonstrate and communicate continuous improvement.

Instead of feeling pressure to say "yes, the organization is secure," or feeling like your position could be at risk by saying no, you need to be able to show your peers where the security posture was, where it is, and where it could go in future. To do that, you can reference the strategic plans you have created based on your data-informed what-if analyses.

Above all, it's essential for you to drive home the message that security is a journey, not a destination. Continuous improvement has no end, especially since adversaries are continuously improving as well.

Outcomes Navigator Is the CISO's Solution

The only cybersecurity product on the market that holistically supports CISOs and their teams with a built-in continuous improvement program is Outcomes Navigator from Exabeam. Being fully integrated within the New-Scale Security Operations Platform, it provides a comprehensive, interactive, and real-time coverage evaluation.

The New-Scale Platform is vendor agnostic, ingesting context and log data from cloud, on-premises, firewalls, endpoint tools, and other third-party sources. The built-in Threat Center workbench includes more than 9,500 parsers to standardize—and therefore analyze—data much more efficiently.

So, regardless of where data and rules originate, you have a single solution to help your security team understand their coverage, close visibility gaps, identify those hard-to-detect risks such as insider threats, and guard against a variety of other potential incidents.

With the New-Scale Platform unifying data sources, Outcomes Navigator constantly assesses the enterprise environment and provides a score of 0 to 100, holistically grading both data source coverage and detection logic. This lets you know whether the logs your security team collects are relevant and directly contribute to threat detection.

Teams also get granular insight into which detection rules are actively firing, versus which ones are deceptive because they're enabled but misaligned, underperforming, or unused. And analysts receive applicable guidance on everything from the parsing quality of their log sources to the types of sources that could be added to improve detection capabilities.

This vastly increases the SOC's ability to conduct what-if analyses as the team continuously strives to improve infrastructure; it also allows security leaders to devise and validate strategic investments and initiatives. The integration of the Exabeam Nova Advisor Agent takes this to the next level.

In the years since its inception, Outcomes Navigator has become one of the most popular Exabeam solutions for security professionals; but compiling, summarizing, and communicating all the insights that it provides can be a complex undertaking. The Advisor Agent enables it to generate a customized, thorough, and specific security coverage report, complete with strengths and weaknesses across detection categories, which use cases are trending positively and negatively, and recommendations for next steps.

While Exabeam Nova features other purpose-built AI agents to support the SOC across a range of workflows, the Advisor Agent focuses on translating data into leadership-ready reports to not only simplify the process of leveraging Outcomes Navigator for what-if scenarios and strategic planning, but proving progress to stakeholders who may not be fluent in the language of cybersecurity.

A Platform Built on a Powerful Foundation

Many vendors promise advanced SIEM capabilities, yet don't deliver; likewise, many vendors claim that their AI assistants can support decision-making even as they provide inaccurate information. It's all too easy for companies to build a convincing demo with predefined prompts and examples—but this approach to cybersecurity creates risk rather than reducing it.

The reason why Exabeam has long been a leader in providing today's next-generation cybersecurity technology is because it defined the previous generation by pioneering the application of AI to the SIEM through machine learning and deep learning. With enrichment and normalization, Exabeam invented a way to standardize the translation of abstract, disparate log files from any type of vendor into concrete, coherent events. This Common Information Model (CIM) remains best-in-class for modern SIEM—it's why security teams don't need dozens of rules for dozens of products.

This established history of research, development, innovation, and credibility has culminated in the New-Scale Platform, also known as Exabeam Fusion. This supports New-Scale Analytics, which builds on the behavioral baselining approach to TDIR pioneered by Exabeam to flag deviant activity, assign risk scores, automatically assemble actionable threat timelines, and detect events that evade traditional detection rules, such as credential misuse and lateral movement.

So, when you use a solution like Outcomes Navigator to map all log files to ATT&CK coverage, it may seem incredibly simple and elegant, yet it's doing something impossibly complicated; as dozens of products yield dozens of different types of log files across hundreds of fields, thousands of inputs are being neatly classified into 21 threat-focused subcategories and 236 different ATT&CK techniques. And all of this is made possible by a decade of refinement and innovation.

Also, it's no accident that Exabeam Nova and its agents far exceed competitors in quality and clarity; they also benefit from being built upon these years of groundbreaking research and development.

Continuous Improvement Can Be Achieved

For years, CISOs and SOC leaders have wanted a way to demonstrate the actual, factual needs, posture, and potential of their security operations. You've wanted to take the gut feel and guesswork out of detecting your coverage gaps, making decisions based on empirical reality rather than intuition and earning buy-in based on evidence instead of charisma.

Now, Outcomes Navigator gives you a way to do this. Decision makers can measurably and meaningfully understand the coverage of use cases in their environment, implement strategies for continuous improvement, produce better returns on investment, and validate their contributions to their peers. Ultimately, you can ensure cybersecurity leadership has a seat at the table and a voice in the conversation because security operations make an undeniable, invaluable contribution to the enterprise.

About Exabeam

Exabeam is a leader in intelligence and automation that powers security operations for the world's smartest companies. As a global cybersecurity innovator, Exabeam provides industry-proven, security-focused, and flexible solutions for faster, more accurate threat detection, investigation, and response (TDIR).

exabeam

Learn more at www.exabeam.com →