CARDINALOPS

5TH ANNUAL REPORT

State of SIEM Detection Risk

CardinalOps 5th Annual Report Examining Gaps in Enterprise SIEM Environments

2025 Edition

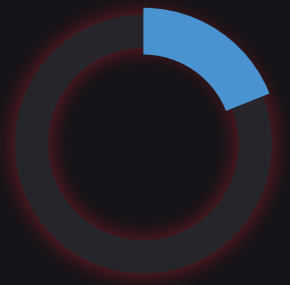
CARDINALOPS.COM

Based on aggregate analysis of all five years of our sample data:

Enterprise SIEMs only have detections for an average of

21%

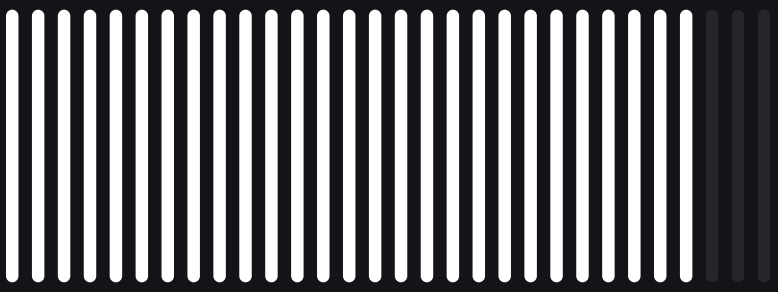
of the techniques in the MITRE ATT&CK framework



Organizations are ingesting enough data into their SIEMs to cover

90%

of all MITRE ATT&CK techniques, on average



SIEM data encompasses an average of **259 types of logs and nearly 24,000 unique log sources**

13%

of an org's SIEM rules are broken

Contents

04 Executive Summary

07 Methodology

08 The Evolving Roles of SIEM & MITRE ATT&CK for the Modern SOC

09 Threat Coverage, Log Volumes, and Sources

11 Rule Health, Quantity, and Quality

12 Detection for Threat Exposure Management

13 TTP-Level Threat Intelligence for Detection AND Exposure Management

14 Best Practices for Detection Posture Management

16 CardinalOps Platform Overview and Key Use Cases

01

Executive Summary

Every year, the pace of threat actors accelerates and the complexity of the average cyber attack increases. This raises the stakes for detection programs–and the expectations for Security Information and Event Management (SIEM) systems.

This is the fifth edition of the CardinalOps State of SIEM Detection Risk report where we analyze a range of production SIEM environments and evaluate the coverage, health, and overall performance of enterprise threat detection programs.

Over the years we've focused on establishing benchmarks for how enterprise SIEM detections provide threat coverage for Security Operation Centers (SOC), and where SOC teams can focus on improving detection posture. And despite years of technical evolution and significant investments, SIEMs are often not properly implemented or optimized, which results in underperformance in their key objective: identifying relevant threats and facilitating response and remediation.

> "Many organizations still struggle with the gap between the promise of SIEM technology and the reality of its deployment, often due to underestimating the ongoing effort required to tune and maintain detection rules."

ANTON CHUVAKIN
Security Advisor to Google's Office of the CISO
Practical Tips for SIEM Migration Success in 2024

This year's findings reinforce a theme across all five years of our analysis: **detection coverage is still far behind expectations when measured against MITRE ATT&CK techniques**. And despite organizations feeding their SIEMs more data than ever, they're not seeing a commensurate increase in coverage. Meanwhile, the persistence of broken rules in SIEM environments poses a huge risk where active threats can go unnoticed.

The confluence of these factors creates a perception vs reality disconnect for SOC teams that poses risks for their detection program and general security posture.

This year's data shows that, on average, enterprise SIEMs:

Only have detections for

22%

of all MITRE ATT&CK techniques

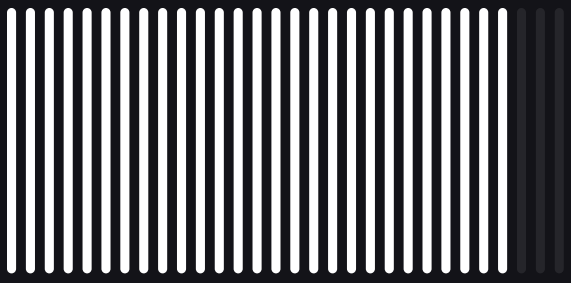
This means that organizations are lacking detection coverage for a staggering 78% of techniques across the ATT&CK framework.

Are ingesting enough data to potentially cover

90%

of ATT&CK techniques

This reflects a huge gap between theoretical and *actual* threat coverage, and a poor return on investments to operationalize SIEM data for detection programs.



Have

10%

of rules that are broken

This means that issues such as misconfigured data sources, missing fields, and parsing errors prevent an alert from firing when a legitimate threat is in the environment.

We acknowledge that full MITRE coverage of MITRE ATT&CK is not practical. The framework was never intended to encourage 100% coverage. Its purpose is to help organizations identify relevant attacker techniques seen in the wild and track progress toward covering those threats. **Looking at the data over time, that progress is moving much more slowly than most organizations would expect, hovering around 20% each year of our study.**

What are the reasons for the gap between actual and expected coverage?

Several factors are at play:

Adversaries' Increasing Sophistication

The average level of sophistication of today's adversaries has increased dramatically since we started publishing this report. Complex methods like multi-stage attacks, polymorphic malware, and nuanced deception and evasion techniques have become commonplace. The adoption of AI tools has also accelerated the pace at which adversaries can apply and iterate techniques to exploit their targets.

Growing IT and Security Complexity

The adoption of multi-cloud and hybrid architectures has tended to overwhelm SIEMs initially designed for more static environments. Sprawling infrastructure leads to fragmented data repositories and inconsistent log formats that can cause critical events to be missed. The proliferation of APIs and cloud workloads more generally has introduced novel log sources that put pressure on SIEM teams to create novel new rules. And attackers can weaponize this very complexity to overwhelm detection engineering processes.

Detection Engineering Bottlenecks

Detection engineering is a relatively new discipline that is still reliant on error-prone manual processes and individual heroics. We're leading the charge to streamline these processes. However, organizations still have a long way to go to evolve beyond "artisanal" approaches focused on individual craftsmanship in favor of more mature "industrial" approaches focused on consistent, scalable processes that create, test, and deploy high-fidelity rules.

Later in this report, we provide a series of best practice recommendations to help CISOs and detection engineering teams frame intentional solutions to challenges related to measuring detection coverage and tracking progress over time. These recommendations are based on the expertise of our in-house security team and SIEM experts like Dr. Anton Chuvakin, Office of the CISO at Google Cloud and former Gartner Research Vice President and Distinguished Analyst.

At the end of the day, this report's goal is to help the security community embrace automated, repeatable, and consistent processes for detection engineering, and to provide independent benchmarks that help CISOs and SOC leaders to answer the question "**How prepared are we to detect the highest priority threats?**"

02

Methodology

This report focuses on data from live production SIEM environments, aggregating and anonymizing SIEM configuration metadata across a wide array of deployments. This gives us a quantitative lens to examine the current state of detection coverage in modern SOCs for higher-fidelity conclusions compared to mere survey data analysis.

Dating back to our initial 2021 report, the full sample of our analysis over the past five years includes:

- A diverse range of enterprise SIEM platforms, spanning Splunk, Microsoft Sentinel, CrowdStrike LogScale, and Google SecOps (Chronicle), across a wide variety of deployment footprints
- Over **13,000 unique detection rules**
- Nearly **2.5 million total log sources**, across several hundred log source types
- Virtually every industry vertical in the global economy, including energy, utilities, financial services, manufacturing, professional and legal services, media and telecommunications, managed security services providers (MSSPs), and many more

The organizations in our sample data represent multinational enterprises with global operations and multiple billions of dollars in revenues. The addition of this year's sample data reinforces the depth and breadth of our dataset, **making it the largest recorded sample of real-world SIEM data ever analyzed**.

03

The Evolving Roles of SIEM and MITRE ATT&CK for the Modern SOC

> A great team with an average SIEM will run circles around the average team with a great SIEM.

ANTON CHUVAKIN
from "Detection Engineering and Scalability Challenges (Part 2)"

The quote above reinforces the core idea that a SOC boils down to people, process, and technology, with technology listed last intentionally. Technology merely enables the people in the SOC to implement the security processes to realize their strategy and achieve objectives. That said, the technology matters in how it enables best practices (processes) and supports the team (people) by streamlining or automating toilsome tasks to free up resources for higher-level strategic projects.

While far from perfect, SIEM technology has been around for nearly three decades for good reason. It remains the central operating system of the SOC. XDR had its moment a few years ago, but even the most advanced platforms lack the operational DNA to effectively detect complex attacks on targets like on-premise server infrastructure and legacy data architectures. The rise of cloud environments has stretched the traditional SIEM model, forcing a shift from monolithic to modular systems with flexibility to decouple components for cost optimization. Still, it's hard to imagine SOCs completely abandoning the underlying technical premise of SIEM technology.

The MITRE ATT&CK framework is also going strong. At the time of this report's publication, the latest version 17 encompasses 211 attacker techniques and 468 sub-techniques (though findings throughout this report focus on v16 as that was generally available during the analysis). Founded in 2013, the framework's underlying goal remains unchanged–to help defenders align their defenses and prepare to detect and prevent a wide range of tactics, techniques, and procedures (TTPs) observed in real-life attack scenarios.

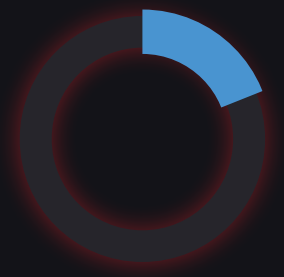
Great SOC teams continuously seek ways to refine and improve processes to achieve their objectives. Mapping SIEM detections to the MITRE ATT&CK framework gives SOC teams a structured, adversary-centric lens that enhances the identification and contextualization of attack techniques, enabling more precise detection and response.

Both this report and the CardinalOps platform use the MITRE ATT&CK framework to measure an organization's detection coverage. We define coverage as the presence of at least one SIEM detection rule mapped to a MITRE ATT&CK technique, and coverage score as the proportion of techniques with coverage relative to all ATT&CK techniques.

04

Threat Coverage, Log Volumes, and Sources

In our 2025 sample analysis, Enterprise SIEMs only have detections for



22%

of techniques in the MITRE ATT&CK framework

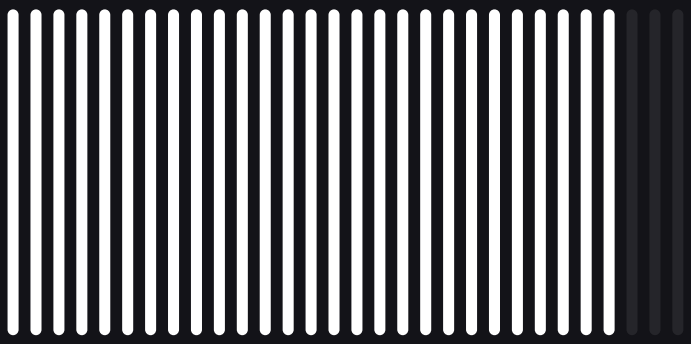
- In other words, organizations *don't* have detections for **78% of MITRE ATT&CK**, which represents nearly 160 techniques in the v16 framework.
- When narrowed down to most frequently used techniques in actual observed attacks, organizations still only have coverage for **4 of the top 10 techniques**.

Meanwhile, SOC teams are ingesting enough data to cover

90%

of all MITRE ATT&CK techniques

- This encompasses an average of **over 250 log source types** and nearly 24,000 unique log sources per organization.



While we fully acknowledge that **100% coverage is not a realistic goal for any SOC**, leading teams track their coverage to illuminate areas for improvement and monitor progress. And for those who say that the top 10 techniques account for the vast majority of observed attacks, our analysis shows that on average, SIEMs only have detection rules for 4 of the top 10 techniques.

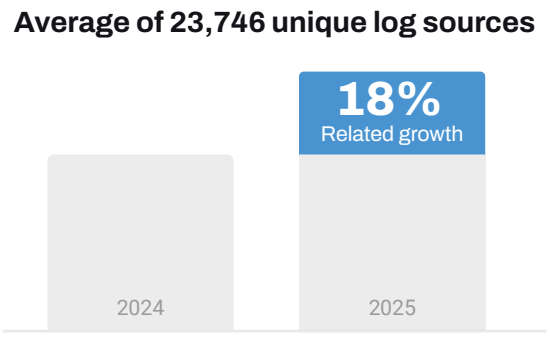
Some good news: **this year's 22% average coverage score is a slight improvement over last year's 19% coverage** score and the 20% benchmark across all historical data dating back to 2021.

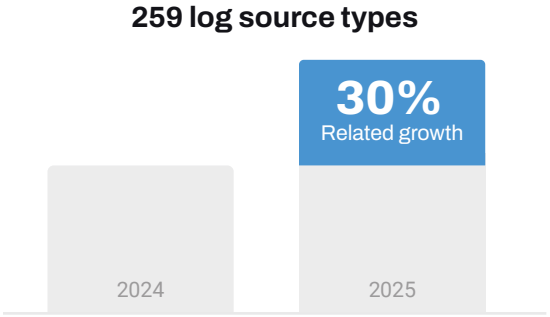
Still, this year's finding means that **the average production SIEM is missing rules for over three fourths of potential attacker techniques**. This year's minor increase is better than no progress at all, but organizations still have a long way to go in expanding coverage to fill the gaps. If you asked a random sample of SOC leaders what percentage of ATT&CK techniques their SIEM can't detect, only the most pessimistic (or brutally honest) would say anything above 50%, reinforcing the gap between perceived and actual threat coverage.

Meanwhile, this year's analysis reveals a more nuanced but critical gap between actual coverage and potential coverage score based on the telemetry teams are ingesting into their SIEM.

On average, the SIEMs we analyzed ingested an **average of 23,746 log sources across 259 unique log source types, representing 18% and 30% respective increases over last year**. This is not necessarily surprising: the growing complexity of IT infrastructure naturally expands both the telemetry from new infrastructure components and the security tools used to protect them. And it's logical for organizations to bring these logs into their SIEM to get more visibility.

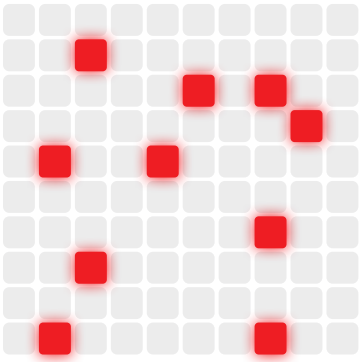
However, the fact that organizations haven't seen a commensurate increase in their coverage scores indicates that organizations are not getting significant returns on their investments in expanding their SIEM data ingestion.





05

Rule Health, Quantity, and Quality



This year we found that

10%

of an organization's SIEM rules are broken

Organizations had **163 rules in their SIEM on average**, so roughly 16 of those rules aren't functioning, risking undetected threats that persist until irrevocable damage is done.

Broken rules are a serious risk, especially when they go unnoticed. The SOC could be blissfully unaware of active threats lurking in their environment, biding their time. Valuable detection engineering resources were invested to create them in the first place, so when factoring in the risk of undetected threats, broken rules actually have a *negative* ROI.

The percentage of broken SIEM rules has fluctuated from year to year throughout our analysis. We saw steady improvements from 25% to 15% across the first few years of this report, followed by a slight regression back to 18% last year. This year's 10% finding is the lowest we've seen to date. While year to year variations could be attributed to sampling differences, the overarching positive trend reflects increased maturity of detection engineering processes.

Meanwhile, this year's data continues a trend of steady yearly declines in the quantity of production SIEM rules. This year they're down nearly a quarter compared to 2022. This is a curious finding. With increasing attacker sophistication and sprawling IT infrastructure expanding attack surfaces, a logical response would be to keep up by adding more detection rules. But more is not always better. This seems to represent a shift toward quality over quantity.

One of Anton's most viewed blogs states that the discipline of detection engineering "rewrites the classic SOC-building handbook by putting an emphasis on detection quality from the start." Similarly, leading-edge SOC teams are embracing detection philosophies rooted in "immutable artifacts" that prioritize intentional detection rules by identifying the underlying behaviors an attacker uses that persist even when their toolset evolves or their targets change. Over time, this approach would result in more durable detections that reduce the need for new rules.

The two trends in this section are connected: fewer rules allow the team to do more rule maintenance, decreasing the number of broken rules. But even with improvements in the percentage of broken SIEM rules, **it only takes one broken rule for an attack to go unnoticed and cause significant harm.**

06

Detection for Threat Exposure Management

A related topic not directly captured in the data is continuous threat exposure management (CTEM). Gartner introduced the CTEM framework around the time of our inaugural report. It's an integrated approach to scope business and security objectives, discover relevant assets and attack surfaces, prioritize high-impact remediation workflows, validate effectiveness of security controls, and mobilize cross-functional teams. Effectively managing exposures requires the orchestration of hardening, patching, security awareness, identity and access management (IAM) policies and governance, and much more.

So what does CTEM have to do with detection rules and SIEM health? Threat exposure management goes beyond vulnerability scanning and patching, especially when patches are too complex, resource-intensive, and risky to immediately implement for the remediation of a critical exposure. Gartner points out the inherent risks of patching disrupting the business:

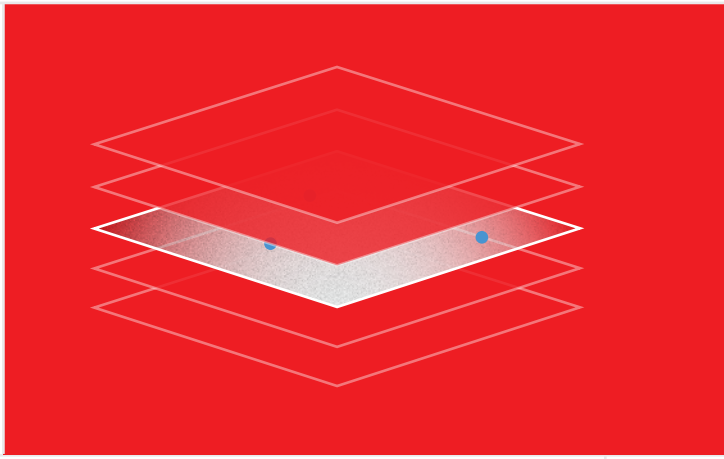
> Many organizations have experienced outages attributed to patches not working as intended. These outages are often high profile, generating reputational damage as well as lost revenue.

Gartner

GARTNER RESEARCH

We're Not Patching Our Way Out of Vulnerability Exposure

With this context, **SIEM detection rules become a crucial component to consider when evaluating potential remediation paths as part of a CTEM program.**



Detection for threat exposure management requires cross-functional coordination with adjacent IT and security teams. With the continuation of the trends outlined in the previous section–fewer broken SIEM rules, higher quality detections that require less manual tuning–SOC resources are freed up for more strategic projects in collaboration with teams responsible for proactive prevention controls. And the dividends for the SOC can be immense.

Challenges that have pained SOC teams for years can be solved outside of the SOC. For example, implementing enterprise-wide multi-factor authentication frees the SOC from endlessly toiling on rules to detect phishing. In other cases, detections are more cost-effective and logical to deploy than prevention controls. For example, securing automated infrastructure-as-code processes requires deep integrations with deployment pipelines and continuous updates to compliance policies. But detection rules can identify noncompliant resources in the environment, triggering alerts with runbooks instructing the response team to simply shut them down.

The two scenarios above are prime examples of compensating controls. When it's not practical, feasible, or cost-effective to implement a given security control, a *compensating control* provides comparable protections from a different layer of the security stack.

Managing exposures and prioritizing controls and assets requires ongoing risk assessments, mapping control coverage for potential attacker tactics and techniques to frameworks like MITRE ATT&CK. **Opportunities to prioritize high-impact, cost-effective remediations of risky exposures are only possible with a unified view of detection AND prevention controls.**

07

TTP-Level Threat Intelligence for Detection and Threat Exposure Management

Another trend not directly in the report data but worth mentioning is the growing interest and need for operationalizing threat intelligence (TI) feeds and reports into actionable security controls down to the specific attacker tactics, techniques, and procedures. Last year's report covered this from the detection engineering perspective, and the below quote captures the relevant pain point succinctly:

> Detection engineers often have to do the bulk of the threat research required to build detection backlog items… often even having to select intelligence sources themselves.

ANTON CHUVAKIN
from "Detection Engineering Is Painful (Part 1)"

Security teams rely on threat intelligence in its various forms for internal reporting, executive awareness, strategy and decision making, and some basic blocking actions. Gaps emerge, however, when it comes to operationalizing more advanced, in-depth intelligence on adversary procedures that can even be as specific as identifying command lines being used by threat actors during an attack.

To solve this challenge, detection engineers sought an automated way to extract TTP-level insights from lengthy TI reports and feeds and create targeted rules to detect those TTPs in their environment. CardinalOps delivered a solution with TI-Ops. By partnering with leading TI solutions like Crowdstrike's Falcon Adversary Intelligence, we convert adversary behaviors into actionable insights and tailored detection rules that protect against the top priority adversary groups and campaigns. Through AI and automation, the platform extracts atomic TTPs from reports to assess a threat's severity and relevance to the customer's environment, and delivers custom, production-ready detections to quickly address detection coverage gaps.

With the preceding section's broader concept of threat exposure management in mind, why not extend that capability from detections to proactive prevention controls? CardinalOps is offering a new solution to do just that, expanding our TI-Ops offering to also recommend proactive prevention controls that can remediate exposures related to TTPs that were identified in our analysis of the TI data.

08

Best Practices for Detection Posture Management

The insights throughout this report help frame approaches to improving detection processes. Below are several best practice recommendations for enhancing detection coverage and SIEM rule quality to maximize the impact your SOC has on the organization's overall security posture.

Refine Core Detection Engineering Processes

Like most continuous improvement efforts, reviewing foundational processes is a great starting point. For detection engineering, that boils down to how your team identifies gaps that require new detections, maintains existing detections, and measures progress toward key objectives.

Identifying Gaps for New Detections

Effective detection engineering starts with systematically identifying relevant threats from TI sources, frameworks like MITRE ATT&CK, and trends in adversary behavior relevant to your industry and attack surfaces. Asking these key questions will help prioritize and implement rules that address current and emerging risks:

- How do you identify emerging threats for building new detections?
- What framework(s) should you track coverage against?
- Are industry frameworks like MITRE ATT&CK sufficient, or is it worth framing a custom framework tailored to your unique threat models?
- How are detections developed today?
- How long does it take to develop, test, and deploy a new detection?

Maintaining Existing Detections

Maintaining existing detection rules is as important as developing new ones. Regular detection QA processes ensure positive returns on efforts to build and deploy rules–and your SIEM investments in general. Lax maintenance processes risk false positives that drown your team in noisy alerts, or false negatives that let actual threats go unnoticed. As you tune and refine your SIEM rules, consider:

- How do you tune rules to reduce false positives and ensure alerts are as high fidelity as possible?
- What processes are in place to identify broken rules and eliminate false negatives?
- How do you trace the impact of false negatives and mitigate previously hidden threats after a broken rule is fixed?
- How do you monitor impacts of changing infrastructure, log source formats, and SIEM data pipelines on whether detections work as intended?

Measuring Progress

To ensure continuous improvement, it's essential to establish metrics that track detection coverage and effectiveness. The specific KPIs to measure will vary from team to team, but reviewing these questions will point you in the right direction:

- How are you monitoring and managing false positives, true positives, and false negatives to maintain detection precision and reliability?
- How well do detections perform during simulated attacks?
- What is your average time to detect threats, and how can you improve it?
- How do these results influence rule refinement and prioritization processes?

Embed Detection Engineering into CTEM Programs

Detection engineering processes can be a critical component at every step of the CTEM program. Threat detection expertise helps the broader CTEM project team identify where detection can provide relevant controls, define what telemetry needs to be monitored, and ultimately prioritize and remediate real attack paths efficiently and effectively.

CTEM is still an emerging process, so embedding detection engineering teams into CTEM programs early on will set a tone of collaboration while proving the value of the threat detection function to the broader security team and leadership.

Below is a brief overview of the 5 stages of the CTEM process, with guidance on how threat detection teams can play a key role each step along the way:

01

Scoping

In the first stage of CTEM, cross-functional stakeholders discuss the organization's most significant risks for business reputational impact to establish key priorities. It is typically completed through a Governance, Risk, and Compliance (GRC) lens, but it's a perfect opportunity for threat detection leadership to get involved early, set a collaborative tone, and assert detection's role in the broader program.

02

Discovery

The second stage involves discovering relevant attack surfaces, assets and potential vulnerabilities, misconfigurations, and other exposure risks. During this step, the detection engineering team can give the broader project team visibility into how current SIEM rules can identify threats to exposed assets, and whether there are significant coverage gaps.

03

Prioritization

This stage involves prioritizing exposures by potential impact to the business and likelihood of exploitation. Collaboration between detection engineering, security architecture, vulnerability management, and leadership is crucial. Different functions own subsets of relevant security controls, with varying levels of complexity and effort to implement and maintain. As such, this step requires rigorous discussions of potential controls across security hygiene, hardening, patching, and detections, with an understanding of how compensating controls can deliver the most efficient, effective path forward. Once it's clear where detections will address key exposures, detection engineers can focus on refining and expanding relevant log sources and SIEM rules.

04

Validation

This stage focuses on validating whether security controls actually mitigate priority exposures. For detection engineering teams, it's an opportunity to collaborate with the broader CTEM project team to simulate adversary behaviors and test whether SIEM rules trigger expected alerts. The results from breach attack simulations help identify which detections require further tuning, and where new detection rules are needed to cover unexpected coverage gaps.

05

Mobilization

This stage focuses on mobilizing the cross-functional team to take action on the gaps identified in the validation stage. This involves a range of stakeholders implementing tactical improvements across IT and security to streamline processes, refine remediation workflows, and fix other issues to mitigate priority exposures. For detection engineering, this is where issues with existing rules and alert workflows are resolved, new detection rules are scoped and prioritized, and log ingestion processes are refined–effectively restarting the iterative CTEM lifecycle.

09

CardinalOps Platform Overview and Key Use Cases

Backed by security experts with nation-state expertise and a deep bench of threat researchers, **CardinalOps provides the only AI-powered platform that unifies visibility of SIEM rules with proactive prevention controls for a consolidated detection posture and threat exposure management platform.**

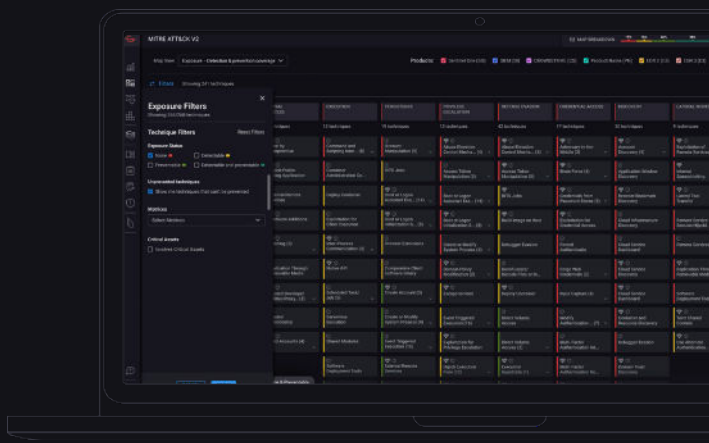
Using a range of LLMs and AI-driven automation processes, CardinalOps continuously maps your detection and prevention controls to MITRE ATT&CK for clear visibility into your threat coverage. By aggregating detection coverage with findings and context on assets and prevention controls, CardinalOps helps continuously assess and reduce exposure risk by showing what security controls you have, whether they will protect against relevant threats, and how to remediate the gaps.

Native API-driven integrations include major enterprise SIEMs like Splunk and Microsoft Sentinel, top EDR platforms like CrowdStrike and Tanium, and critical cloud security tools spanning Wiz, Microsoft Defender, Palo Alto Prisma, and many more. These integrations give CardinalOps a consolidated view of all the controls across your security stack to enable consistent and cost-effective remediation workflows that preemptively reduce risk and protect you from the threats that matter most.

This section includes an overview of the top use cases for the CardinalOps platform, with key features and their associated benefits for optimizing threat detection programs.

Map and Continuously Expand MITRE ATT&CK Coverage

Many organizations still use manual processes and tools like spreadsheets to evaluate their coverage for the techniques in the MITRE ATT&CK framework. This means your documented coverage is out of date almost as soon as the manual mapping is completed. More importantly, it means your detection engineering team is distracted from strategic, higher-impact projects and tasks.



CardinalOps automatically maps your SIEM data to MITRE ATT&CK tactics, techniques, and sub-techniques for an in-depth understanding of your detection posture. By integrating with the native API of your existing SIEM, the platform pulls in detailed metadata on your detection rules and log sources, while your sensitive data never leaves your SIEM.

The heatmap and metrics can be filtered toward specific APT groups, ATT&CK matrices, security layers (endpoint, network, cloud, IAM, etc.), and covered vs uncovered techniques. This gives you unparalleled clarity on your current SIEM coverage–and opportunities to expand strategically.

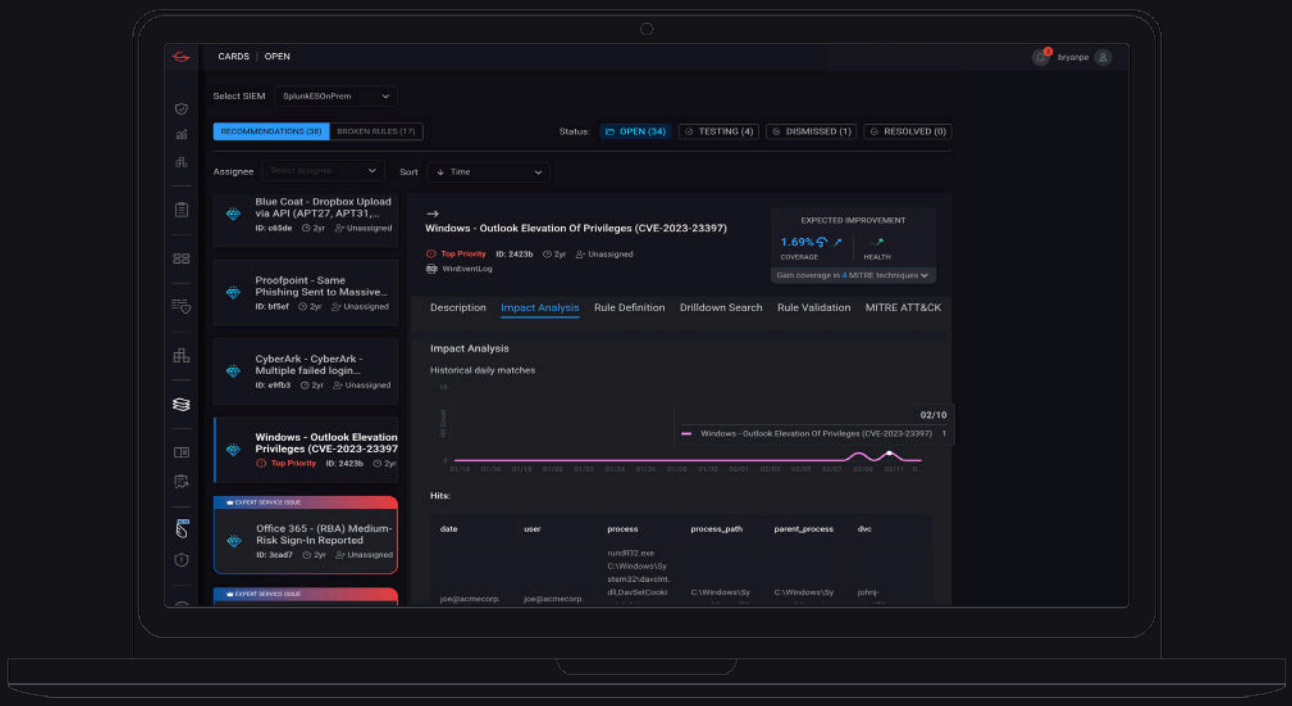
Close Detection Gaps and Fix Broken, Noisy Rules

After identifying key opportunities for expanding detection coverage, CardinalOps delivers curated, high-fidelity SIEM rules to proactively close the gaps. Rules are delivered in the native query language of your SIEM and already customized to your environment. Rules are ready to review, test, and push to your SIEM with a click of the button. This provides a steady stream of new detection rules that ensures you're proactively addressing critical detection coverage gaps.

Over time your environment changes in subtle ways beyond just adding new rules: your network boundary shifts, security tools upgrade to the latest versions, and monitoring workflows change. This drift can lead to broken rules that never fire, leading to a false sense of security. This report highlights the significant risks associated with false negatives, where active threats that penetrate your environment go unnoticed and lead to significant damage.

CardinalOps addresses this gap by proactively fixing broken rules. Specialized analytics processes continuously evaluate and diagnose issues with your SIEM rules. Those issues can stem from misconfigurations that prevent alerts from firing, OR improperly tuned rules that create alert floods that drown the SOC team in noise and hide the true signals.

By pinpointing misconfigured data sources, missing fields, parsing errors, and other common problems, **CardinalOps eliminates false negatives AND false positives, ensuring your team focuses only on high-fidelity alerts for efficient response workflows.**

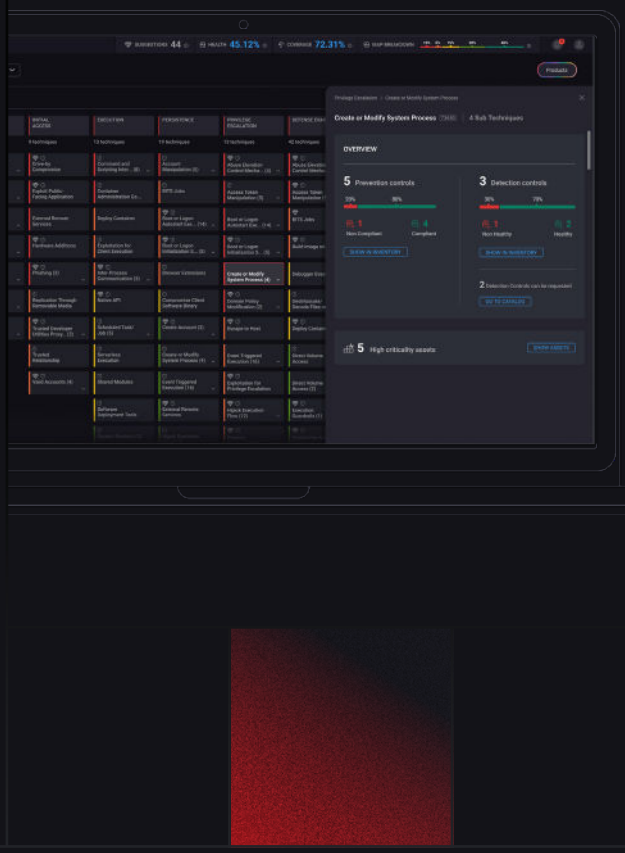


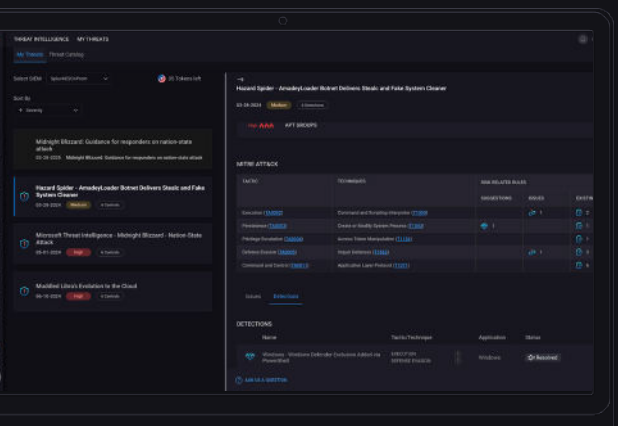
Cover Prevention Gaps with Detections

When it's impractical or too costly to implement prevention controls, detection rules can serve as compensating controls to mitigate exposure risk. For a defense-in-depth approach, having multiple layers of controls is preferable: security teams can proactively prevent a threat from entering the environment, or respond immediately in the event that a threat does get through the prevention layer. Unfortunately organizations lack the unified visibility across prevention and detection controls to identify these opportunities.

CardinalOps unlocks true defense-in-depth across prevention and detection by identifying areas where deploying detections can compensate for missing prevention controls. Our approach ensures that organizations maintain a robust security posture even when ideal prevention controls cannot be fully realized due to operational or budgetary constraints.

Starting with detections then unifying them with prevention controls gives CardinalOps a unique perspective to help teams continuously assess their exposure and cover prevention gaps with targeted detections. This strategy not only enhances visibility into gaps in coverage of relevant exposures but also supports a dynamic and adaptive defense posture that aligns with evolving threats and organizational priorities.





Operationalize Threat Intelligence

Security teams are increasingly burdened with building threat-informed cyber defenses that prioritize specific threats relevant to their industry, environment, and risk models. Innovations in threat intelligence offerings have been able to provide TTP-level insights on threat actors and their specific behaviors, but they typically come up short in enabling SOC teams to actually operationalize this intelligence for use in their detection rules.

CardinalOps maps the information from threat intelligence reports to the MITRE ATT&CK framework's techniques and subtechniques. After assessing initial coverage and detection posture, CardinalOps fills any gaps by delivering specific rules designed to detect relevant techniques in the report. The platform also recommends more proactive prevention controls to address exposures related to the TTPs included in TI reports and feeds, and facilitates automated remediation workflows.

The CardinalOps platform also leverages a catalog of open-source intelligence (OSINT) that aggregates public reports and articles with the latest threat intelligence, operationalizing the intelligence into detection insights and content for your unique environment.

With CardinalOps, you can build a proactive, threat-informed defense with actionable threat intelligence that keeps pace with attacker behavior and strengthens your organization's defense against the threats that matter most.

What Customers Are Saying About CardinalOps

REPSOL

“Security leaders are dealing with a growing volume and variety of security findings, creating massive complexity and difficulty around determining where to focus. The CardinalOps platform helps address the critical need for better processes around centralizing all of these security findings, assigning proper priorities, and then moving to mobilization in order to remediate critical exposures.”

JAVIER GARCIA QUINTELA
Global CISO, Repsol

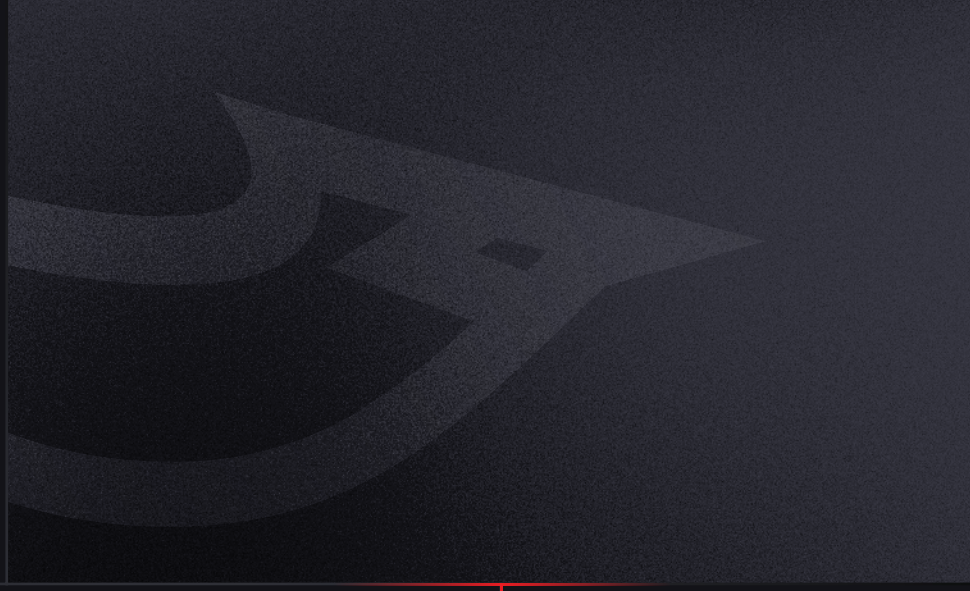
“CardinalOps delivers the strategic expertise and automation we need to ensure our SOC is operating at maximum effectiveness and efficiency.”

CISO
National Stock Exchange

“CardinalOps has been transformational for my team. Plus, time-to-value was extremely short. In our complex environment, it’s not easy for vendors to get their solutions into production – at scale – but they promised us quick API-level integration with Splunk, and they delivered.”

VP OF GLOBAL SECURITY ENGINEERING & ARCHITECTURE
Fortune 500 Food & Beverage, Manufacturing

CARDINALOPS



About CardinalOps

CardinalOps provides the only AI-powered threat exposure management platform that integrates both prevention and detection controls for unified visibility into exposure risks. By aggregating data from security tools across multiple domains, CardinalOps facilitates context-driven prioritization and automated, safe remediation. Actionable insights on compensating controls streamline consistent and cost-effective remediation workflows to proactively reduce risk and protect you from the threats that matter most.