



**CARDINALOPS**  
Detection Posture Management

**4TH ANNUAL REPORT**

# STATE OF SIEM DETECTION RISK 2024 EDITION

Quantifying the MITRE ATT&CK  
gaps that lead to undetected  
attacks in production SIEMs



**Enterprise SIEMs only have detections for**

**19%**

of all 201 techniques in the MITRE ATT&CK v14 framework



**Enterprise SIEMs already ingest sufficient data to cover**

**87%**

of all MITRE ATT&CK techniques

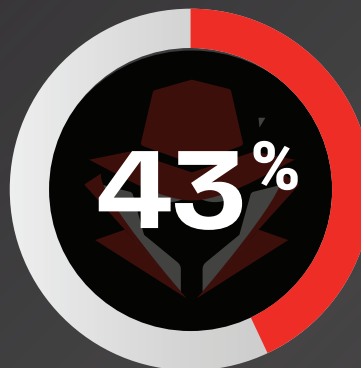
In other words, we don't need to collect more data, but rather scale our detection engineering processes to develop more detections faster.

**18%**

of all SIEM rules are broken and will never fire due to common issues such as misconfigured data sources and missing fields.

**Multiple SIEM environments are on the rise**

**Organizations reporting two or more SIEMs in production**



# Table of Contents

<b>1</b>	Executive Summary .....	3
<b>2</b>	Methodology.....	6
<b>3</b>	Continuing Importance of the SIEM.....	7
<b>4</b>	Why MITRE ATT&CK Matters.....	8
<b>5</b>	Coverage for MITRE ATT&CK Techniques.....	10
<b>6</b>	Health Metrics .....	11
<b>7</b>	Trends in SIEM Detection and Security Operations .....	12
	7.1 Multi-SIEM Environments are on the Rise.....	12
	7.2 Increased Demand for Operationalizing TTP-Level Threat Intelligence.....	13
<b>8</b>	Best Practices for Detection Posture Management .....	14
	8.1 Review current SIEM processes .....	14
	8.2 Become more intentional about how you develop and manage detection content.....	15
	8.3 Build or refresh your use case management processes .....	14
	8.4 Measure and continuously improve.....	14
<b>9</b>	CardinalOps Platform Overview & Top Use Cases.....	16
	9.1 Map all your detections to MITRE ATT&CK.....	17
	9.2 Gain new detections to address critical gaps faster.....	18
	9.3 Continuously identify and fix broken rules.....	19
	9.4 Automatically analyze and tune noisy rules .....	20
	9.5 Operationalize TTP-level threat intelligence into actionable detection rules.....	21
	9.6 Automate to reduce need for additional personnel and eliminate mundane tasks.....	23
<b>10</b>	What Customers Are Saying About CardinalOps .....	25
<b>11</b>	About CardinalOps.....	26

## 1 Executive Summary

**“Is this a good detection rule? Do I have good ATT&CK coverage in this area? Do my SIEM rules work well here? Does my EDR cover the holes of my SIEM detection posture?”**



**Dr. Anton Chuvakin**  
Office of the CISO, Google Cloud  
[Medium Blog Post](#)

Understanding SIEM detection coverage and quality can be difficult, as Anton wrote in his blog post on Medium, but looking at overall trends from a range of production SIEM environments can provide us with data and measurement to better understand how organizations and security teams as a whole are doing.

In this 4th installment of our annual data-driven report, CardinalOps set out to gain visibility into the current state of use case development and threat detection coverage in enterprise SOCs.

What did we find? Using the [201 adversary techniques in MITRE ATT&CK as the baseline](#), we found that actual detection coverage remains far below what most organizations expect and what SOCs are expected to provide.

Worse, organizations are often unaware of the gap between the theoretical security they assume they have and the actual security they have in practice, creating a false impression of their detection posture.



In particular, we found that, on average, enterprise SIEMs:



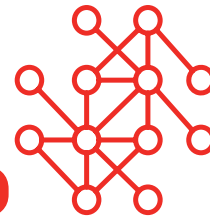
Are missing detections for

**81%**

of all MITRE ATT&CK techniques.

Can potentially cover

**87%**



of ATT&CK with existing data sources they're already ingesting – but are currently only covering less than 19%. This suggests that we don't need to collect more data, we need to scale our detection engineering processes to develop more detections faster.

Have more than

**18%**



of their rules that are broken and will never fire an alert due to common issues such as misconfigured data sources, missing fields, and parsing errors. That means that, on average, more than 1 out of every 6 rules is not working properly.

While both the numbers for overall coverage and rule health metrics worsened by a few percentage points since 2023, we attribute this primarily to differences in sampling, and also because we had a larger, more diverse set of organizations in this year's dataset.

## What are the reasons for this disparity between actual and expected coverage?



**Complexity:** The **average enterprise has more than 130 distinct security tools** (endpoint, network, cloud, email, IAM, etc.). Each of these tools has its own log format, event types, and/or alert types, with each requiring unique detections to be developed based on a detailed understanding of how they function.

As a result, according to Ponemon, more than **80% of security professionals rate the complexity of their SOC as very high**, and **less than 40% assess their SOC as highly effective**.



**Constant change** in infrastructures, security tools, attack surfaces, adversary techniques, and business priorities (e.g., cloud). In fact, over the next 5 years, Gartner Research projects that over 60% of security incidents will be traced to misconfigured security controls.<sup>1</sup>



**No "one-size-fits-all"** — every enterprise is unique, making it impractical to copy-and-paste generic content from SIEM vendors, MSSPs, open source communities, and marketplaces.



**Manual and error-prone processes** that are highly dependent on individual "ninjas" with specialized expertise, making it difficult to effectively scale and maintain high-quality detections.



**Challenges in hiring and retaining skilled personnel** who can develop detections across diverse scenarios and log source types.

In section 2 of the report, we provide a series of best practice recommendations to help CISOs and detection engineering teams address these challenges and be more intentional about how detection coverage is measured and continuously improved over time. These recommendations are based on the experience 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.

It is our goal with this report to help the security community move forward in recognizing the importance of bringing automated, repeatable, and consistent processes to detection engineering, and to provide independent benchmarks enabling CISOs and SOC leaders to answer the question **"How prepared are we to detect the highest priority threats?"**

## 2 Methodology

Rather than rely on subjective survey-based data, CardinalOps analyzed configuration meta-data from real-world production SIEM instances to gain visibility into the current state of detection coverage in modern SOCs.

In the 4 years of analyzing data for these reports we have examined, aggregated, and anonymized data across:

**Diverse SIEM solutions** including









**More than 10,000** detection rules – with the largest SIEM we analyzed having more than 600 rules!

Over **1.2 million** log sources.

**Hundreds** of unique log source types.

**Diverse verticals** including banking and financial services, insurance, automotive, manufacturing, energy, media & telecommunications, professional & legal services, and MSSP/MDRs.

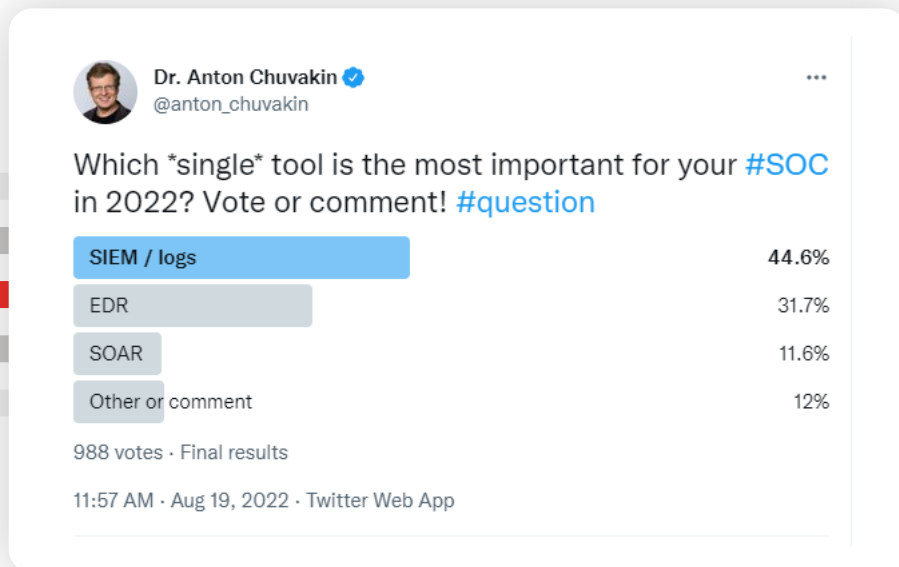
Many of these organizations represent multibillion dollar, multinational corporations – making this the largest recorded sample of real-world SIEM data analyzed to date.

### 3 Continuing Importance of the SIEM

According to Forrester Research, despite the hype around XDR, SIEMs continue to be the central “operating system of the Security Operations Center.”

In fact, according to the [SANS 2023 SOC Survey](#), SIEMs and EDR are the top two technologies considered critical to having an effective SOC.

This view is also supported in a Twitter poll that Anton conducted:



As one security leader recently explained to us, even if you’re using EDR to detect and block malicious activity at the endpoint layer, you still need a SIEM with custom detections that act as a critical “backstop” to catch attacks that EDR solutions miss.

This can occur for several reasons including that sophisticated adversaries have figured out a way to disable or bypass EDR controls; relevant EDR alerts have been disabled due to excessive noise; or adversaries have devised a way to “hide in the noise” of untuned alerts.

So how do we measure and continuously improve our coverage for the threats most important to our organizations? [The MITRE ATT&CK](#) framework can help (see next section).

## 4 Why MITRE ATT&CK Matters

**“Since its creation in 2013, the MITRE ATT&CK framework has been of interest to security operations professionals. Based on ESG research, MITRE ATT&CK usage has now reached an inflection point. After nine years, MITRE ATT&CK and its use cases have evolved well beyond a reference architecture. In many ways, MITRE ATT&CK has become a “lingua franca” of security operations.”**



**Jon Oltsik**  
ESG Distinguished Analyst,  
CSO Online

As the standard framework for understanding adversary playbooks and behavior, MITRE ATT&CK now describes more than 500 techniques and sub-techniques used by threat groups such as APT28, the Lazarus Group, Cozy Bear, and Scattered Spider.

According to ESG research, 89% of organizations currently use MITRE ATT&CK to reduce risk for security operations use cases such as determining priorities for detection engineering, applying threat intelligence to alert triage, and gaining a better understanding of adversary tactics, techniques, and procedures (TTPs).

The biggest innovation introduced by MITRE ATT&CK is that it extends the traditional intrusion kill chain model to go beyond static IOCs (like IP addresses, which attackers can change constantly) to catalog all known adversary playbooks and behaviors (TTPs).

These are grouped into both Tactics (“why” an adversary is performing an activity, such as Initial Access or Privilege Escalation) and Techniques (“how” they are executing that activity, such as by exploiting a public-facing application or modifying a domain policy).

MITRE ATT&CK has also standardized our taxonomy vocabulary for both offensive and defensive teams. As Rick Howard, former CISO for Palo Alto Networks and now Chief Analyst at The CyberWire says in a [recent CyberWire podcast](#):

**“Where the Lockheed Martin kill chain model is conceptual, the MITRE ATT&CK framework is operational. [Before the framework], we were all looking at the same activity and couldn’t talk about it collectively in any way that made sense because each vendor and government organization had their own language and any intelligence coming out of those organizations couldn’t be shared with anybody else without a lot of manual conversion grunt work. Talk about the Tower of Babel!”**

**It’s also become the standard way to communicate to executive leadership about defensive posture and how it relates to recent attacks and vulnerabilities they heard about in the news (like [Microsoft Outlook](#), [MOVEit](#), and [Ivanti](#) vulnerabilities) — as well as answer the classic question “How prepared are we to detect the highest-priority threats?”**

There are still some drawbacks and challenges when using MITRE ATT&CK. Some of the main deficiencies is that the framework is often not granular enough and that techniques can span multiple source types, thus making them difficult to detect in a singular binary fashion. This is precisely why CardinalOps developed [MITRE ATT&CK Security Layers](#). Security Layers extends the concept of ATT&CK coverage by measuring the “depth” of detection coverage for the first time. It does this by mapping each detection to a specific security layer – such as endpoint, network, email, cloud, containers, and IAM – and then enumerating the number of distinct layers covered for a given technique.

In this report – and in the [CardinalOps platform](#) – we use the MITRE ATT&CK framework to [measure an organization’s coverage](#) across all these TTPs. The platform also helps organizations prioritize new detections to address gaps for the techniques that matter most to them, and [delivers deployment-ready detections](#) for their existing SIEMs, among other [use cases](#).

## 5 Coverage for MITRE ATT&CK Techniques

Our data shows that enterprise SIEMs, on average:



Are missing detections for

**81%**

of all 201 techniques in the MITRE ATT&CK v14 framework

This implies that adversaries can execute more than **160 different techniques** that will be undetected by the SOC. Or stated another way, SOCs are only covering around **38 techniques** or **19% of all techniques that can potentially be used by adversaries.**



Are already ingesting sufficient data to potentially cover almost all ATT&CK techniques.

**87%**

This suggests that *we don't need to collect more data, we need to scale our detection engineering processes to develop more detections faster.*

## 6 Health Metrics

**Our data shows that enterprise SIEMs, on average:**

- **Have 18% of their rules that are broken and will never fire an alert due to common issues such as misconfigured data sources, missing fields, and parsing errors.**

This commonly occurs due to ongoing changes in the IT infrastructure, vendor log format changes, and logical or accidental errors in writing a rule.

**Here are some specific examples (for Splunk SPL) of some of the ways a rule can break:**

- **Sourcetype does not exist**, e.g. because a source has stopped sending data
- **Index does not exist**, e.g. because the data is now going into a different index
- **Lookup does not exist**
- **Scheduling has time gaps** leading to missed alerts
- **Sourcetype <-> Index** are mismatched
- **Logical operators are not in uppercase**
- **Parsing is incorrect**
- **Fields have been renamed**

---

**Data quality issues:**

- **Process Command Line is not being logged in Windows**
- **Key Vault changes are not being logged in Azure**

## 7 Trends in SIEM Detection and Security Operations

### 7.1 Multi-SIEM Environments are on the Rise

This year saw an increase in the number of organizations that have multiple SIEM platforms in production – with more than 43% of organizations reporting multiple SIEMs in their environments. Although this data was not shared in previous years’ reports, this marked a notable increase from 2023 and the years prior.

There are a range of reasons for why organizations choose to run two or more SIEMs, including:



**Cost-savings** derived from a combination of cloud-native SIEMs (Microsoft Sentinel, Google Chronicle, etc.) and traditional SIEMs (Splunk, IBM QRadar, etc.).



**Multiple business** units adopting their own SIEMs, either by choice or resulting from M&A activity.



**Regulatory requirements** mandating local storage of sensitive data (e.g. EU data protection laws).

Along with the additional complexity of managing multiple platforms, CISOs and security leaders can often struggle to gain a federated or aggregated view while lacking consistent detections and log sources across multiple SIEMs in order to have an accurate understanding of their overall detection posture.



**Read our Security Research Summary on Addressing the Complexity Challenge of Multiple SIEMs**

## 7.2 Increased Demand for Operationalizing TTP-level Threat Intelligence

Another trend that is not directly captured in the report's data is the growing interest and need for organizations to be able to operationalize TTP-level threat intelligence for SIEM detection content. This was paired with a demand to find an automated way of achieving this and drastically shortening the detection engineering lifecycle in order to take action on such intelligence – with many organizations citing that manual processes were too slow and burdensome to do this effectively.

Various forms of threat intelligence are currently being leveraged by security teams for internal reporting, executive awareness, strategy and decision making, and some basic blocking actions. There is a gap, however, when it comes to being able to take action on 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.

Being able to operationalize this level of TTP intelligence enables security teams to operate and develop detection and response capabilities based on adversary behaviors. Contact the CardinalOps team to learn how you can transform threat and adversary intelligence (TTPs) into a stronger detection posture within your SIEM.



**Contact the CardinalOps team to learn how you can transform threat and adversary intelligence (TTPs) into a stronger detection posture within your SIEM.**

## 8 Best Practices for Detection Posture Management

**“Organizations need to become more intentional about detection in their SOCs. What should we detect? Do we have use cases for those scenarios? Do they actually work? Do they help my SOC analysts effectively triage and respond?”**



**Dr. Anton Chuvakin**

Office of the CISO, Google Cloud  
[SANS webinar on “The Future of SIEM”](#)

Here are a series of best practice recommendations for enhancing detection coverage and detection quality in your SOC.

### 8.1 Review current SIEM processes

- **What is the approach for finding false negatives – and what adversary techniques, behaviors, and threats are currently being missed?**
- **How are use cases managed and prioritized? Typically, we find they’re added to the backlog via an ad-hoc process driven by a combination of:**
  - + Threat analysts & threat intelligence
  - + Red teaming
  - + Breach and attack simulation (BAS) tools
  - + Manual pen testing
  - + News about the latest high-profile attacks or vulnerabilities
- **How are detections developed today and **what is the process for turning threat knowledge into detections?****
- **How long does it typically take to develop new detections?**
- **Is there a systematic process to periodically identify detections that are no longer functional due to infrastructure changes, changes in vendor log source formats, etc.?**

## 8.2 Become more intentional about how you develop and manage detection content

### What

- + do I need to detect based on our business priorities, crown jewel assets, industry sector, etc.?
- + do I detect today?
- + is our current coverage compared to adversary techniques most relevant to our organization?

### Do I

- + really detect it?
- + detect it well?
- + triage and respond correctly?

### Are we

- + missing data sources that would improve our coverage in high-priority areas?

## 8.3 Build or refresh your use case management processes

- Choose 3-5 enhancements to address the questions from the last section, with an agreed-upon timeline.

## 8.4 Measure and continuously improve

- Detection engineering processes are no different than other security and IT management processes. As IT modernizes and uses DevOps and SRE approaches, so should the SOC.
- You can't improve what you can't measure. Many SOC metrics - focused on people, process, and technology - are needed for consistent improvement
- Set organizational goals around how to increase detection coverage and reduce the time to detect non-functioning rules.

## 9 CardinalOps Platform Overview & Top Use Cases

**“Security operations teams are at a crossroad. Organizations need unprecedented security operations scale and efficiency but continue to be dragged down by manual processes, skills shortages, and suboptimal technology usage. The MITRE ATT&CK framework can help, as it introduces an adversary view and structure for security operations. Organizations seeking to operationalize MITRE ATT&CK as a framework for identifying and remediating control gaps may want to consider detection posture management with CardinalOps.”**



**Jon Oltsik**

Senior Principal Analyst and Fellow, Enterprise Strategy Group  
Operationalizing MITRE ATT&CK with Detection Posture Management

Backed by security experts with nation-state expertise, the [CardinalOps platform](#) uses automation and MITRE ATT&CK to continuously assess your detection posture and eliminate coverage gaps in your existing SIEM – so you can easily implement a threat-informed defense.

What’s more, it improves detection engineering productivity by 10x and drives cost savings by recommending new ways to tune noisy and inefficient queries, reduce logging volume, and eliminate underused tools in your stack.

Native API-driven integrations include Splunk, Microsoft Sentinel, IBM QRadar, Google Chronicle, CrowdStrike LogScale / Next-Gen SIEM, and Sumo Logic.

Here are the top use cases for the platform, with a description of all use cases shown [here](#).

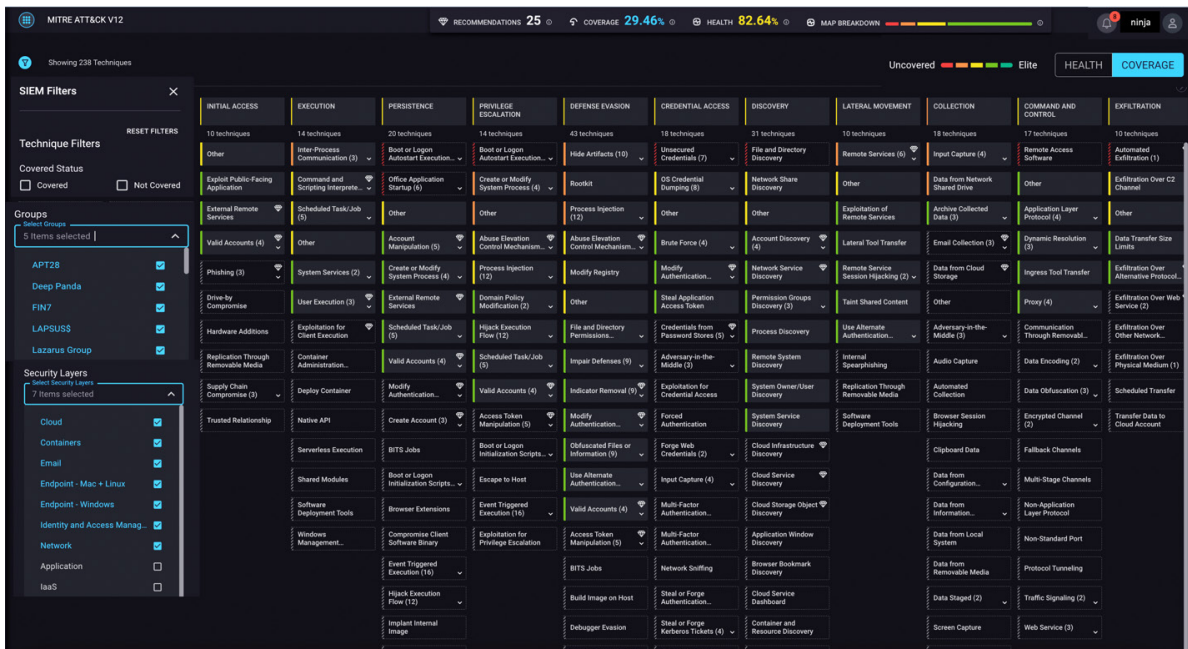
## 9.1 Map all your detections to MITRE ATT&CK

Most organizations are still using spreadsheets or other manual tools to understand their ATT&CK coverage. This is a mundane and time-consuming activity that takes your engineers and analysts away from more strategic activities – plus your visibility into your actual MITRE ATT&CK coverage is always out of date.

In order to map your ATT&CK coverage, our platform starts by connecting via the native API of your existing SIEM. It then ingests all your rules as well as metadata about your log sources (your sensitive log data never leaves the SIEM).

The platform then uses specialized, ML-based analytics and feature extraction to map your detections to the most appropriate ATT&CK technique and sub-technique, producing a heatmap and coverage score that’s continuously updated whenever you add detections or the ATT&CK framework gets updated.

The heatmap and metrics can easily be filtered based on selected variables including APT groups, ATT&CK matrices, security layers (endpoint, network, IAM, cloud, etc.), and whether you want to examine covered or uncovered techniques.



MITRE ATT&CK coverage showing coverage and health metrics at top, and selected filters at bottom left.

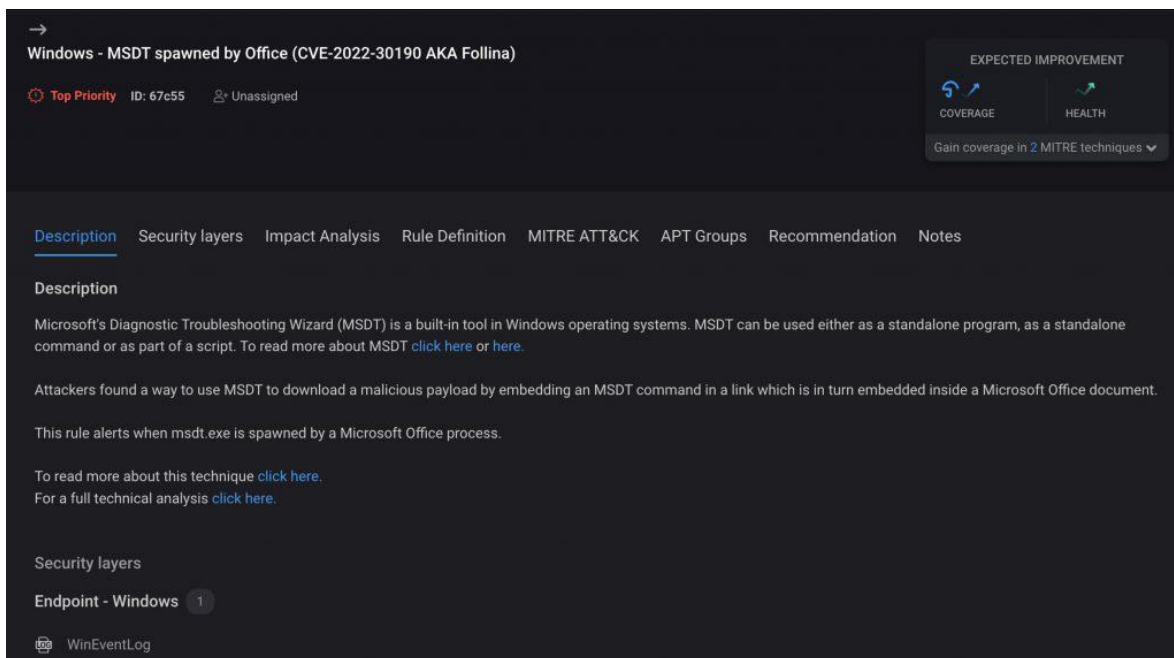
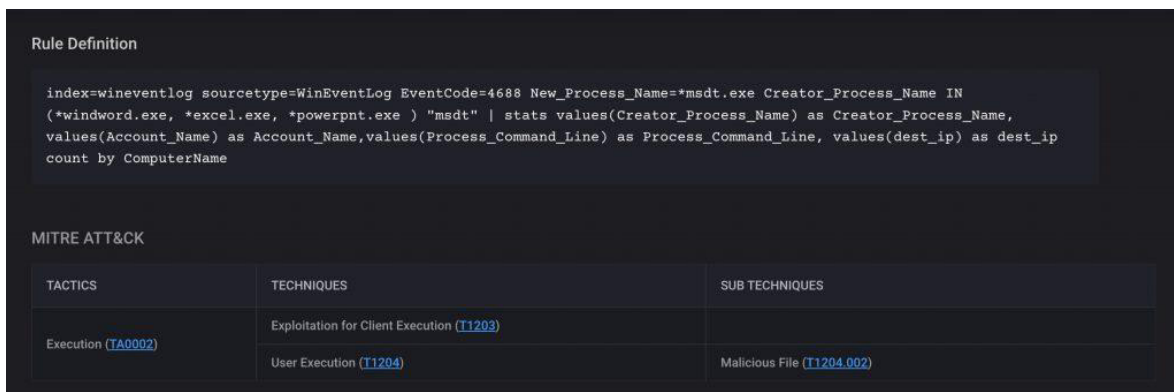
## 9.2 Gain new detections to address critical gaps faster

Once you’ve identified your top priorities for eliminating coverage gaps – such as specific APT groups, Tactics and Techniques, or log source types – the platform delivers curated, high-fidelity detections to close the gaps.

Rules are delivered deployment-ready, meaning they’re in the native query language of your SIEM and have been pre-validated and auto-customized for your environment, including your data sources, naming conventions, and indexes.

The platform makes it easy to quickly review, test, and push new rules into your SIEM with the click of a button (via its native API).

Plus, you gain access to a searchable rule catalog containing thousands of rules – covering hundreds of diverse data sources – including for the latest high-profile threats and vulnerabilities.

TACTICS	TECHNIQUES	SUB TECHNIQUES
Execution (TA0002)	Exploitation for Client Execution (T1203)	
	User Execution (T1204)	Malicious File (T1204.002)

APT Groups		
TECHNIQUES	SUB TECHNIQUES	APT GROUPS
Exploitation for Client Execution (T1203)		admin@338 (G0018), Andariel (G0138), Aocin Dragon (G1007), APT12 (G0005), APT28 (G0007), APT29 (G0016), APT3 (G0022), APT32 (G0050), APT33 (G0064), APT37 (G0067), APT41 (G0096), Axiom (G0001), BITTER (G1002), BlackTech (G0098), BRONZE BUTLER (G0060), Cobalt Group (G0080), Confucius (G0142), Darkhotel (G0012), Dragonfly (G0035), Elderwood (G0066), Ember Bear (G1003), EXOTIC LILY (G1011), Higaisa (G0126), Inception (G0100), Lazarus Group (G0032), Leviathan (G0065), MuddyWater (G0069), Mustang Panda (G0129), Patchwork (G0040), Sandworm Team (G0034), Sidewinder (G0121), TA459 (G0062), The White Company (G0089), Threat Group-3390 (G0027), Tonto Team (G0131), Transparent Tribe (G0134), Tropic Trooper (G0081), FIN11, APT9  admin@338 (G0018), Ajax Security Team (G0130), <small>Andariel (G0138), Aocin Dragon (G1007), APT12 (G0005), APT28 (G0007),</small>

Example of a new detection showing a description of the attack that is being detected by this rule; the full rule in the native syntax of your SIEM; and which Techniques and APT groups are covered by this detection. Once the rule has been manually reviewed and automatically tested using the past 90 days of historical log data, it can be pushed directly into the SIEM via the SIEM’s API.

### 9.3 Continuously identify and fix broken rules

If you’re like most detection engineering teams, you’re continuously adding new detection rules to your SIEM. But over time, your environment has changed in different ways.

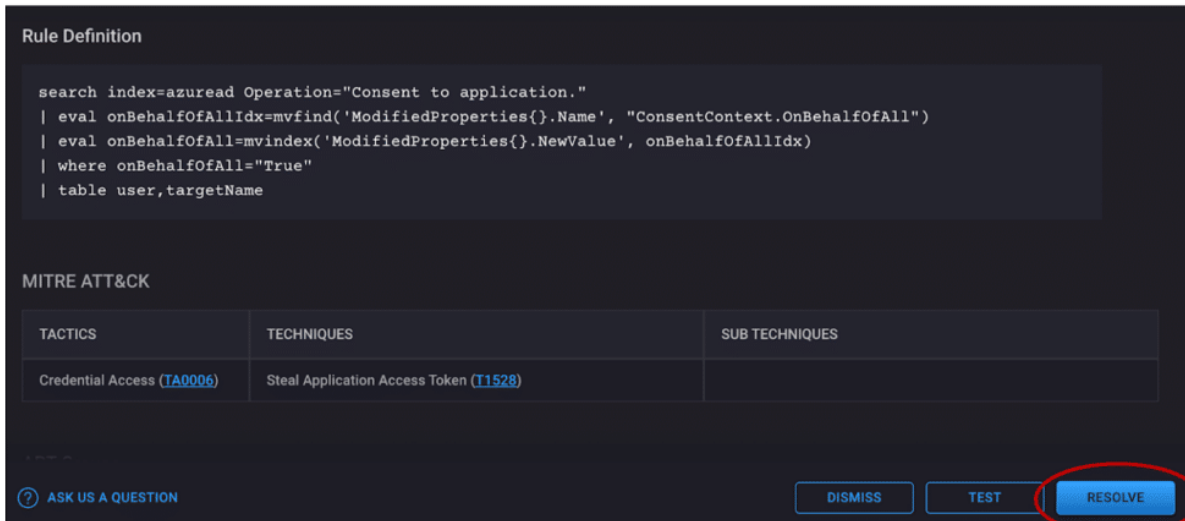
Your network has changed, your security tools have been upgraded to newer versions and log formats, older log sources have been retired, and your monitoring targets have changed.

And you may even have added generic rules that were copied and pasted from open sources or by an MSSP (and might contain RegEx errors that prevent proper parsing).

The result? Broken rules that will never fire due to misconfigured data sources, missing fields, parsing errors, and other data quality issues – creating additional gaps in your coverage.

This leads to a false sense of security because your CISO and SecOps team think they’re protected – but then are surprised when your Red Team (or worse, an adversary) finds a hidden gap in your defenses and exploits it.

The CardinalOps platform uses specialized analytics to continuously analyze all your rules to ensure they have all required prerequisites to fire (log data, field values, etc.). But it doesn’t just identify issues with broken rules, it delivers remediated rules that you can review, test and instantly deploy into your SIEM.



*New and remediated rules can be pushed directly into the SIEM after manual review and automated testing.*

And if remediation requires actions outside your SIEM – such as enabling event logging options on endpoints that were previously turned off – it delivers detailed recommendations on how to fix it, with links to technical documentation you can share with your IT team.

## 9.4 Automatically analyze and tune noisy rules

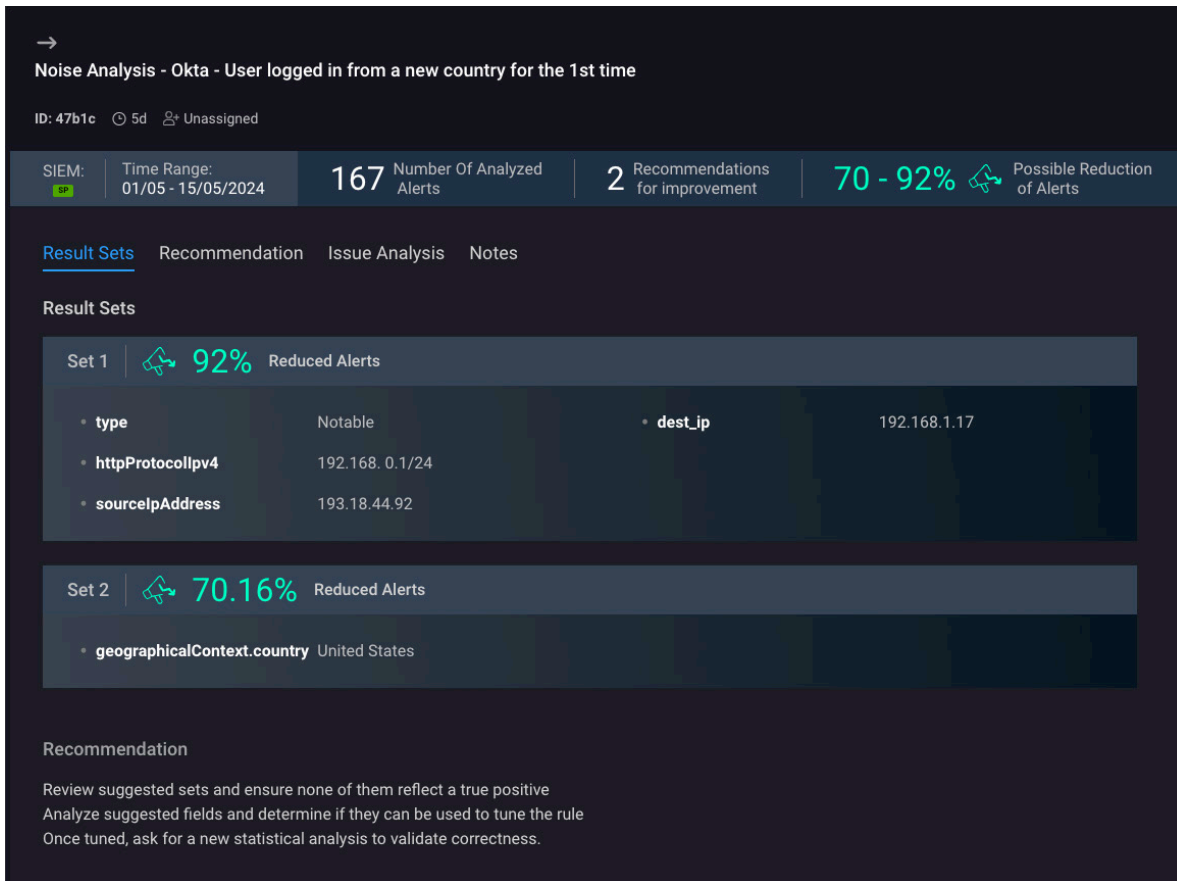
The only thing as bad as a rule that doesn't fire when it should, is a rule that fires when it shouldn't. It's like the boy who cried 'wolf' – noisy detections lead to alert fatigue which, according to a report conducted by International Data Corporation (IDC), results in complacency on the SOC team.

In fact, researchers found that 20-30% of all alerts are simply ignored or not investigated in a timely manner. It results in high burnout, high turnover, and low job retention of security professionals.

Noisy rules also give adversaries an easy path to exploit weaknesses in your defenses. According to SANS, an overwhelming majority of ethical hackers (more than 58%) can exploit and break into an environment in five hours or less – often by "hiding" their attacks in a cacophony of noisy detections that the SOC team regularly ignores.

Of course you can also deploy SOAR, alert triage, and other post-processing solutions to address this issue, but why not go after the source of noisy alerts – the "offending" rules themselves?

CardinalOps addresses the challenge of alert fatigue by analyzing all incidents created by the noisiest rules in your SIEM. To isolate the likely root cause of the problem, it looks for patterns and pinpoints specific field/value pairs that are responsible for triggering most of the alerts. It then provides recommendations on how to tune the rules using exclusions derived from the statistical analysis.



→  
Noise Analysis - Okta - User logged in from a new country for the 1st time

ID: 47b1c 5d Unassigned

SIEM: SP Time Range: 01/05 - 15/05/2024 **167** Number Of Analyzed Alerts **2** Recommendations for improvement **70 - 92%** Possible Reduction of Alerts

[Result Sets](#) Recommendation Issue Analysis Notes

Result Sets

Set 1 92% Reduced Alerts

• type	Notable	• dest_ip	192.168.1.17
• httpProtocolIpv4	192.168.0.1/24		
• sourceIpAddress	193.18.44.92		

Set 2 70.16% Reduced Alerts

• geographicalContext.country	United States		
-------------------------------	---------------	--	--

Recommendation

Review suggested sets and ensure none of them reflect a true positive  
Analyze suggested fields and determine if they can be used to tune the rule  
Once tuned, ask for a new statistical analysis to validate correctness.

*The CardinalOps platform performs a statistical analysis to pinpoint the root cause of noisy rules and provides recommendations for tuning.*

The end result? A meaningful reduction in alert volume and alert fatigue – without eliminating alerts that are most likely to be true positives.

## 9.5 Operationalize TTP-level threat intelligence into actionable detection rules

Organizations are struggling to keep up with an evolving threat landscape and security teams are increasingly burdened with the pressure to build an effective cyber defense against sophisticated threats.

Recent advancements in threat intelligence have been able to provide TTP-level intelligence on threat actor procedures and behavior – even going as deep as showing specific command line scripts being used in the wild.

Despite this being valuable intel, security teams have had challenges with effectively being able to operationalize the intelligence. Some of the main hurdles include a lack of expertise amongst their team to be able to accurately interpret and apply the threat data, an inability to analyze and prioritize the

vast amount of intelligence in a timely manner, and the complexity of trying to adapt the intelligence into actionable security controls with their processes and tools.

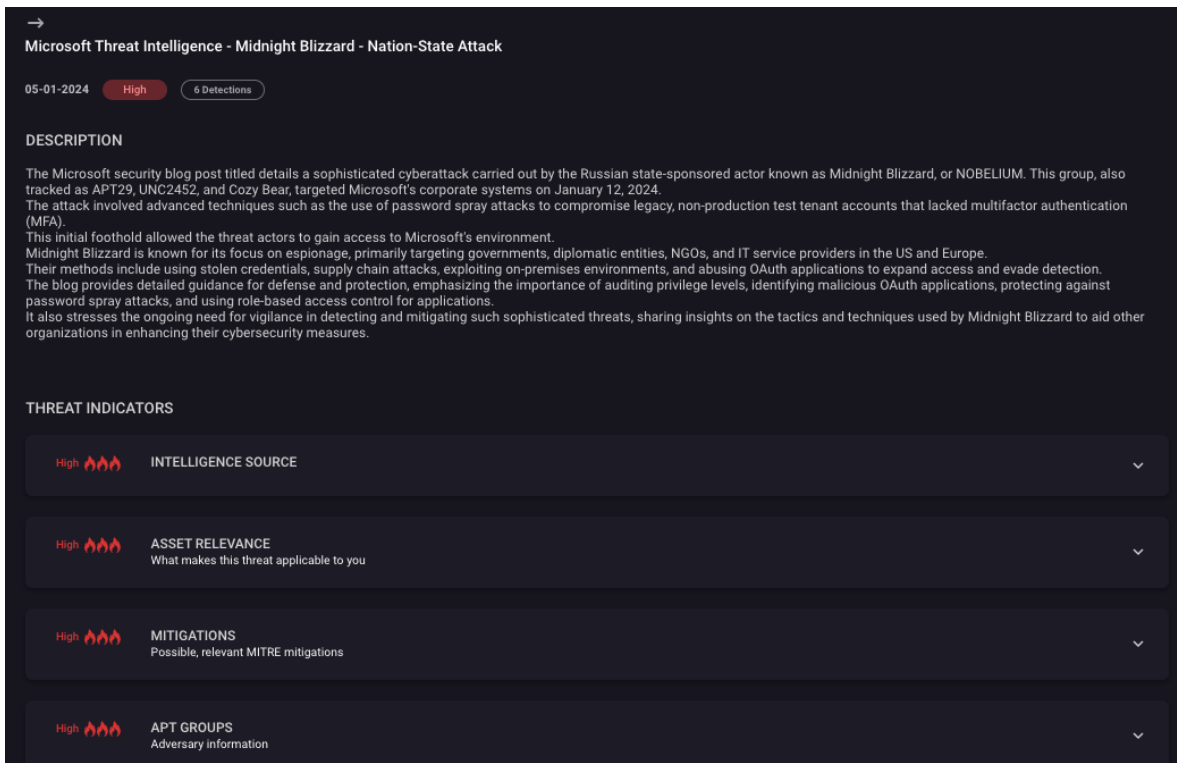
These challenges create a bottleneck in cybersecurity operations, impacting the speed and efficacy of the organization’s defensive measures.

With CardinalOps, security teams are able to translate TTP-level threat intelligence reports into actionable detection rules to proactively strengthen their cyber defense with near real-time adversary intelligence.

Leverage your organization’s access to commercial threat intelligence, such as TTP-based reports from CrowdStrike, Google/Mandiant Threat Intelligence, and Microsoft Defender Threat Intelligence, to understand where current threat coverage stands and also receive recommendations of deployment-ready rules to mitigate areas where gaps exist.

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

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.



*Upload threat intelligence reports to extract atomic TTPs and understand a threat’s severity and relevance.*

→ Microsoft Threat Intelligence - Midnight Blizzard - Nation-State Attack

05-01-2024 High 6 Detections

MITRE ATT&CK

TACTIC	TECHNIQUES	RISK RELATED RULES		
		SUGGESTIONS	ISSUES	EXISTING RULES
Persistence (TA0003)	Account Manipulation (T1098)			
Defense Evasion (TA0005)	Use Alternate Authentication Material (T1550)			
Credential Access (TA0006)	Brute Force (T1110)			
Credential Access (TA0006)	Steal Application Access Token (T1528)			

Tactics and Techniques are mapped to MITRE ATT&CK with visibility into current rule coverage and health. Suggestions are also provided for new rules to increase coverage.

DETECTIONS

Name	Tactic/Technique	Application	Status
Office 365 - User Granted the Application Impersonation Role (APT 28, APT 29)	PERSISTENCE ①	Office 365	
Office 365 - Full Access as Application Permission Granted (MuddyWaters, APT29)	DEFENSE EVASION ① LATERAL MOVEMENT ①	Office 365	
Azure - User Added to Global Administrator Role	PERSISTENCE ①	Azure	
Azure - End User Consent to Application	CREDENTIAL ACCESS ①	Azure	
Azure - Application Credential Modification	DEFENSE EVASION ①	Azure	
Office 365 - Distributed Password Spray (APT 28)	CREDENTIAL ACCESS ①	Office 365	

Customized, applicable set of detections are provided and ready for deployment

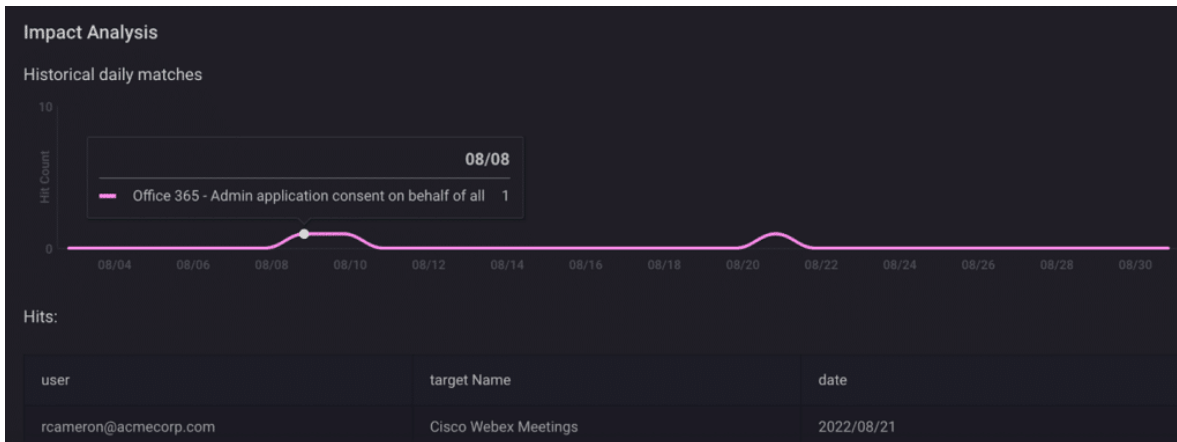
## 9.6 Automate to reduce need for additional personnel and eliminate mundane tasks

While automation has delivered significant benefits to multiple areas of the SOC – such as anomaly detection and incident response – the detection engineering function remains stubbornly manual and typically dependent on “ninjas” with specialized expertise.

With CardinalOps, you can now apply automation and analytics to level-up your team and streamline the end-to-end process of researching, testing, and delivering new detections. Address the latest vulnerabilities. Onboard new log sources. And respond to ongoing requests from your Red Teams and threat intelligence teams.

You can also leverage automation to address more mundane tasks such as mapping your rules to ATT&CK, identifying and fixing broken detection and data sources, and tuning noisy detections.

The benefits? Higher productivity, greater agility, and cost avoidance from a reduced need to hire additional personnel. Plus happier staff members that are less likely to leave because they can now spend their time on more interesting activities such as threat hunting and researching new and novel attack techniques.



*Impact Analysis shows an automated test workflow typically executed before deploying any new rules. The test shows if and when the new rule would have fired, had it been in place for the past 90 days, as a way to ensure the rule is not too noisy and/or to determine appropriate exclusions.*

## 9 What Customers Are Saying About CardinalOps



**CISO, National  
Stock Exchange**

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



**VP of Global Security  
Engineering & Architecture,  
Fortune 50 Food & Beverage,  
Manufacturing**

**“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.”**



**Director of Information  
Security, \$3B Global  
Corporate Law Firm**

**“Splunk is the backstop we rely on to catch attacks our other security tools (like EDR) miss. CardinalOps ensures all our custom detections are working as intended and we aren’t missing detections for the MITRE techniques and APTs most relevant to our organization. Plus the platform saves us a ton of time on MITRE mapping, and their team has been incredibly responsive.”**

## About CardinalOps

Backed by security experts with nation-state expertise, the CardinalOps platform uses automation and MITRE ATT&CK to continuously ensure you will always detect the threats most relevant to your organization.

What's more, it improves detection engineering productivity by more than 10x and drives cost savings by recommending new ways to tune noisy and inefficient queries, reduce logging volume, and eliminate underused tools in your stack.

Native API-driven integrations include Splunk, Microsoft Sentinel, IBM QRadar, Google Chronicle SIEM, CrowdStrike LogScale / Next-Gen SIEM, and Sumo Logic.

Learn more at [cardinalops.com](https://cardinalops.com).

