CARDINALOPS

2022 REPORT

THE STATE OF SIEM DETECTION RISK

Quantifying the gaps in MITRE ATT&CK coverage for production SIEMs

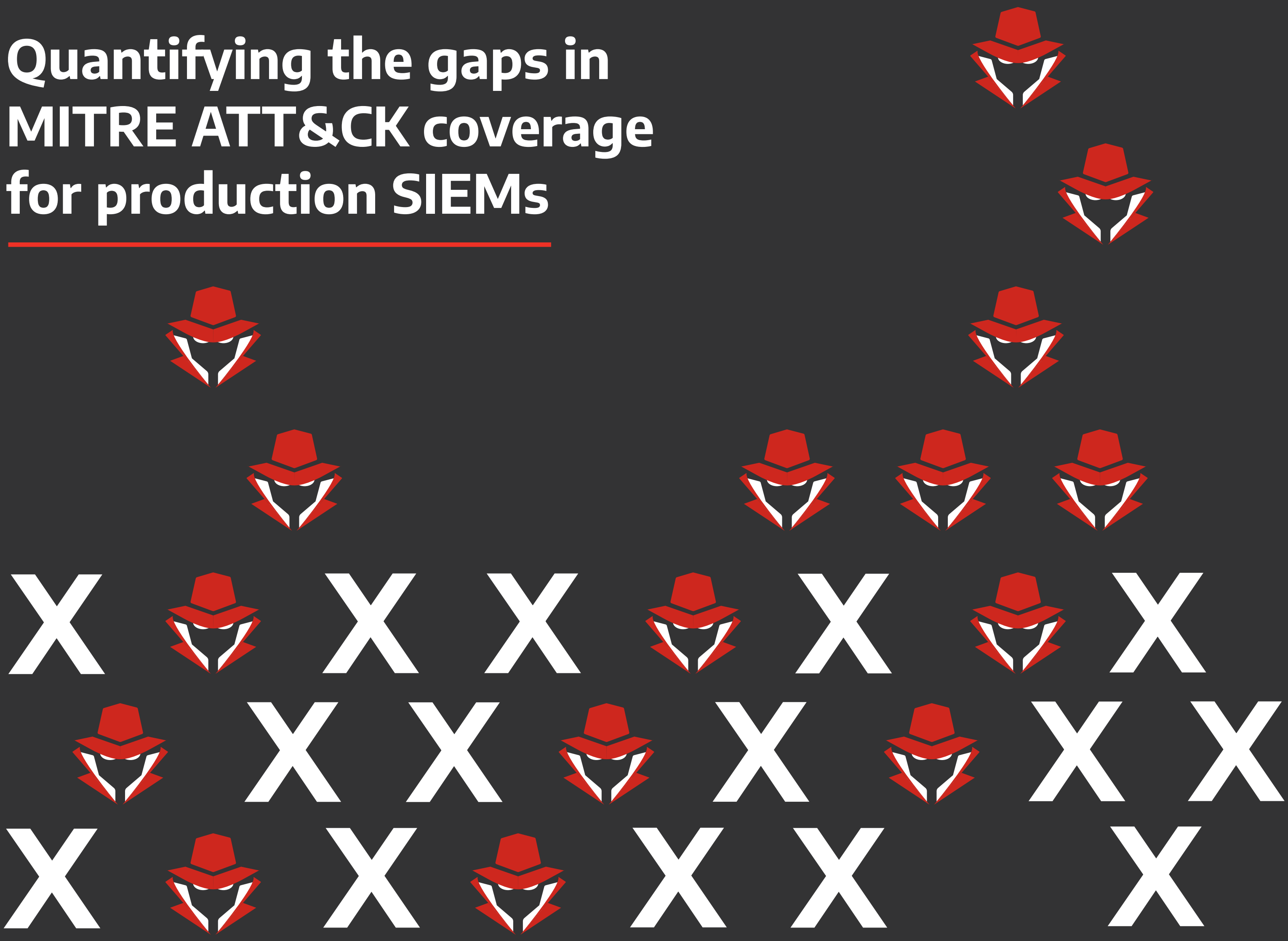


Table of Contents

1.0

2.0 3.0 4.0 5.0 6.0 7.0 8.0

EXECUTIVE SUMMARY

> “**Use cases are the core of security monitoring activities.** A structured process to identify, prioritize, implement, and maintain use cases allows organizations to align monitoring efforts to security strategy, choose the best solutions and maximize the value obtained from security monitoring tools.”
>
> **- Dr. Anton Chuvakin**
> Blog post

SIEMs are foundational to the modern SOC, providing the essential role of helping security teams rapidly detect and respond to cyberattacks before they can have a material impact on the business of the organization.

In order to be effective, SIEMs now aggregate log and event data from an exponentially-growing number of data sources across the infrastructure (applications, network and endpoint security tools, cloud monitoring tools, identity providers, etc.). This data is then analyzed using predefined threat detection rules and queries to identify suspicious or unauthorized behavior.

In this 2nd annual data-driven report, CardinalOps set out to gain visibility into the current state of threat detection coverage in enterprise SOCs.

Using the 190+ 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. In particular, we found that on average:

Enterprise SIEMs **only address**

5 of the top 14

ATT&CK techniques used by adversaries in the wild.

Enterprise SIEMs are **MISSING DETECTIONS** for

80%

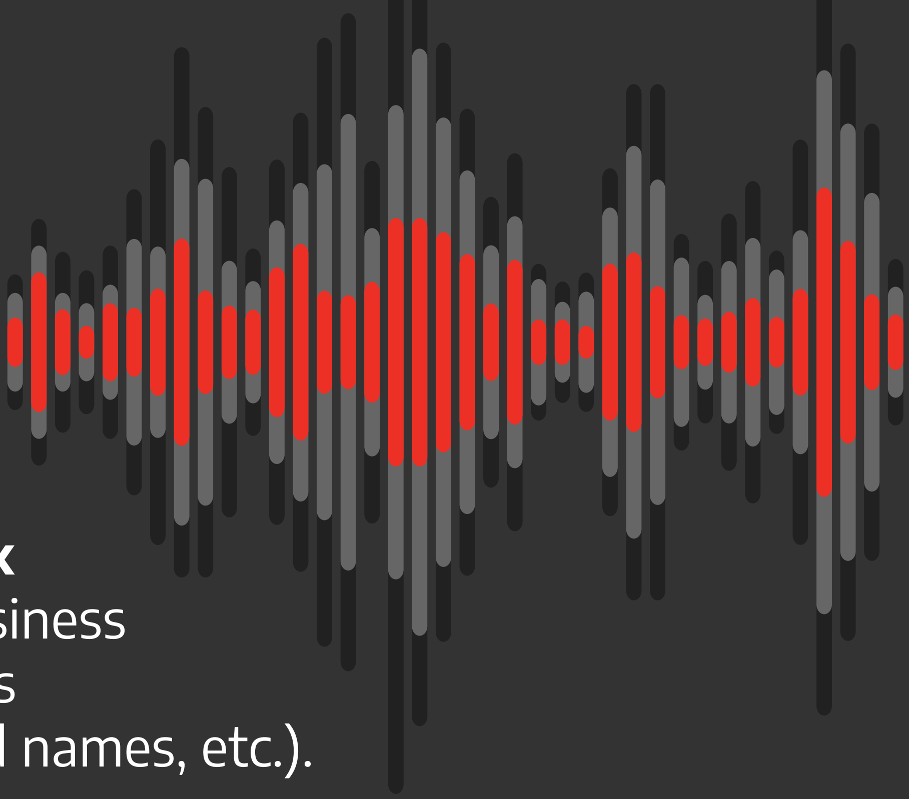
of all MITRE ATT&CK techniques.

15% of SIEM rules are **broken and will never fire** due to common issues such as misconfigured data sources and missing fields.

Organizations **disable**

75%

of generic **out-of-the-box** vendor content due to noisiness & customization challenges (e.g., log source types, field names, etc.).



Only

25%

of organizations that forward identity logs such as Active Directory and Okta to their SIEM, actually use them in their detection rules.

(Zero trust, anyone?)

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

What are the reasons for this disparity?

Complexity from a constantly increasing number of data sources, attack vectors, and correlation rules. In fact, 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).

No “one-size-fits-all” — every enterprise is unique, making it impractical to copy-and-paste generic content.

Manual and error-prone processes make it difficult to effectively scale and maintain high-quality detections.

Lack of skilled personnel to understand and develop use cases 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, Head of Security Solution Strategy at Google Cloud and former Gartner Research Vice President and Distinguished Analyst.

It is our goal 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?”

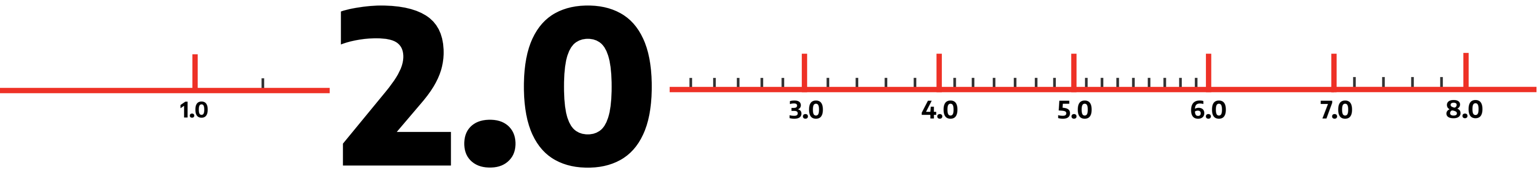
METHODOLOGY

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

We examined aggregated and anonymized data across:

- **Diverse verticals** including financial services, manufacturing, media, pharmaceuticals, freight logistics, and MSSP/MDR services
- **Diverse SIEM** solutions including Splunk, Microsoft Sentinel, IBM QRadar, and Sumo Logic
- **14,000+** log sources
- **Thousands** of detection rules
- **Hundreds** of log source types

These organizations represent multibillion dollar, multinational corporations – making this one of the largest recorded samples of actual SIEM data analyzed to date.



STATE OF DETECTION COVERAGE AS MEASURED BY MITRE ATT&CK

> “**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**
>
> Head of Security Solution Strategy, Google Cloud
>
> SANS webinar on “The Future of SIEM”

Here are the insights we developed after analyzing a broad cross-section of real-world SIEM production instances.

2.1 Coverage across all ATT&CK techniques

On average, SIEMs only cover 20% of the 190+ adversary techniques described in MITRE ATT&CK v10.[1]

2.2 Coverage for top ATT&CK techniques used by adversaries in the wild

On average, SIEMs cover fewer than 5 of the top 14 techniques used by adversaries in the wild, based on 2021 threat intelligence data from Recorded Future, Red Canary, and Picus Security.

These consist of:[2]

- T1059 Command and Scripting Interpreter
- T1218 Signed Binary Proxy Execution
- T1543 Create and Modify System Process
- T1053 Scheduled Task / Job
- T1027 Obfuscated Files or Information
- T1105 Ingress Tool Transfer
- T1569 System Services
- T1036 Masquerading
- T1486 Data Encrypted for Impact
- T1082 System Information Discovery
- T1497 Virtualization/Sandbox Evasion
- T1098 Account Manipulation
- T1219 Remote Access Tools
- T1018 Remote System Discovery

2.3 % of broken/nonfunctioning SIEM rules

15% of SIEM rules are broken and will never fire, primarily due to fields that are not extracted correctly or log sources that are not sending the required data.

[1] V11 was released after this analysis was concluded.

[2] To be conservative in our analysis, we excluded two techniques that SIEMs are ill-equipped to address: Process Injection and Credential Dumping.

2.4 % of default vendor-supplied detection content that is disabled

On average, 75% of default out-of-the box (OOB) rules provided by SIEM vendors are disabled, due to the difficulty of adapting generic rules to each organization's unique infrastructure, log sources, naming conventions, etc..

2.5 Top log sources with no detections

- The top 3 log sources that are ingested by the SIEM – but not being used for any detections – are identity sources; SaaS productivity suites such as Office 365 and G Suite; and cloud infrastructure log sources.
- In fact, **75% of organizations that forward identity log sources** to their SIEM, such as Active Directory and Okta, do not use them for any detection use cases.
- This appears to be a major opportunity to enhance detection coverage for one of the most critical log sources for strengthening zero-trust.

> "Contrary to recent opinion, monitoring, detection and response play a critical role in **zero trust** deployments. In many cases, robust visibility controls over identities, access and endpoints are essential to make zero trust a success."
>
> **- Dr. Anton Chuvakin**
>
> Head of Security Solution Strategy, Google Cloud
> "20 Years of SIEM – SANS Webinar Q&A"

3.0

BEST PRACTICE RECOMMENDATIONS

> “**MITRE is a really good method of categorizing, measuring, and enhancing security operations.** Those that are most successful use MITRE to communicate with others in their businesses, to measure processes and success.”
>
> Blog by industry analyst

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

3.1 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
  - 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.?

3.2 Become more intentional about how you develop and manage detection content

Focus on effectiveness, coverage, and improvements. Ask your team questions such as:

- What do I need to detect based on our business priorities, crown jewel assets, industry sector, etc.?
- What do I detect today?
- Do I really detect it?
- Do I detect it well?
- Do I triage and respond correctly?
- What is our current coverage compared to adversary techniques most relevant to our organization?
- Are we missing data sources that would improve our coverage in high-priority areas?

3.3 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.

3.4 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.

> "The kill chain framework was a very popular approach for use case development until the ATT&CK framework came and expanded upon it. Essentially, this builds on the kill chain with more depth and more value for most use cases today. **I would probably focus my analysis on the ATT&CK framework and not on the original kill chain model** (while keeping my awareness of it, of course)."
>
> **- Dr. Anton Chuvakin**
>
> Head of Security Solution Strategy, Google Cloud
> "20 Years of SIEM – SANS Webinar Q&A"

4.0

HOW CARDINALOPS CAN HELP

> “**Network defenders do not need 100 percent accuracy in our models to support risk decisions.** We can strive to simply reduce our uncertainty about ranges of possibilities. The concept of measurement is not the elimination of uncertainty but the abatement of it. If we can collect a metric that helps us reduce that uncertainty, even if by just a little, then we have improved our situation from not knowing anything to knowing something.”
>
> **- Douglas Hubbard**
>
> (as reviewed by Rick Howard, former CISO at Palo Alto Networks)
>
> How to Measure Anything: Finding the Value of ‘Intangibles’ in Business

CardinalOps' cloud-based platform continuously ensures your SIEM/XDR has high-fidelity detections for the adversary techniques most relevant to your business priorities and infrastructure, mapped to the MITRE ATT&CK framework.

Leveraging proprietary analytics and AI-powered, API-driven automation, the platform continuously delivers new detection content and metrics enabling your SOC team to stay ahead of constant change in the attack surface and threat landscape – plus continuously identify and remediate broken rules and misconfigured log sources – so you can close the riskiest detection gaps that leave your organization exposed.

After connecting to the SIEM/XDR via its API, the service will analyze all rules, alerts, and log source types to:

4.1 Visualize coverage based on MITRE ATT&CK heat map

Provide a coverage heat map based on MITRE ATT&CK for all use cases in your production SIEM/XDR

4.2 Recommend, test, and automatically deploy new rules to close gaps in threat coverage

- Recommend missing rules from a knowledge base of best practice detections to improve threat detection coverage and close gaps in threat coverage
- Enable new rules to be reviewed, tested (versus historical data), and automatically deployed with a single click after approval (or via the API for Git-based CI/CD workflows)
- Customize rules to the organization's field mappings, thresholds, exclusions, and naming conventions

4.3 Identify, test, and automatically remediate broken or noisy rules

- Identify all broken or misconfigured rules (i.e., rules that will never fire due to missing fields, misconfigured log sources, etc.)
- Identify noisy rules that can be tuned to further reduce alert fatigue (e.g., by modifying thresholds and exclusions)
- Recommend remediations to broken or sub-optimum rules
- Enable remediations to be reviewed, tested (versus historical data), and automatically deployed after approval with a single click — or via the API if using Git-based CI/CD workflows

4.4 Enable risk-based prioritization based on organizational requirements

Enable risk-based prioritization by:

- Log source type
- Platform type (cloud, Windows, Linux, containers, etc.)
- Increasing your MITRE ATT&CK coverage score
- Adversary group (APT28, FIN7, etc.)
- High profile attacks (log4j, SolarWinds, etc.)
- Threat severity

4.5 Identify log sources not contributing to threat coverage

- Identify log sources that are ingested but not contributing to threat coverage.
- This information can be used to reduce ingestion costs and/or develop new rules to expand threat coverage by incorporating these log sources.

4.6 Produce independent metrics to measure detection posture and demonstrate continuous improvement

- Help CISOs answer the question “How prepared are we to detect the highest priority threats?”
- Generate independent, board-level metrics to measure SOC effectiveness
- Track continuous improvement over time

1.0 2.0 3.0 6.0 7.0 8.0

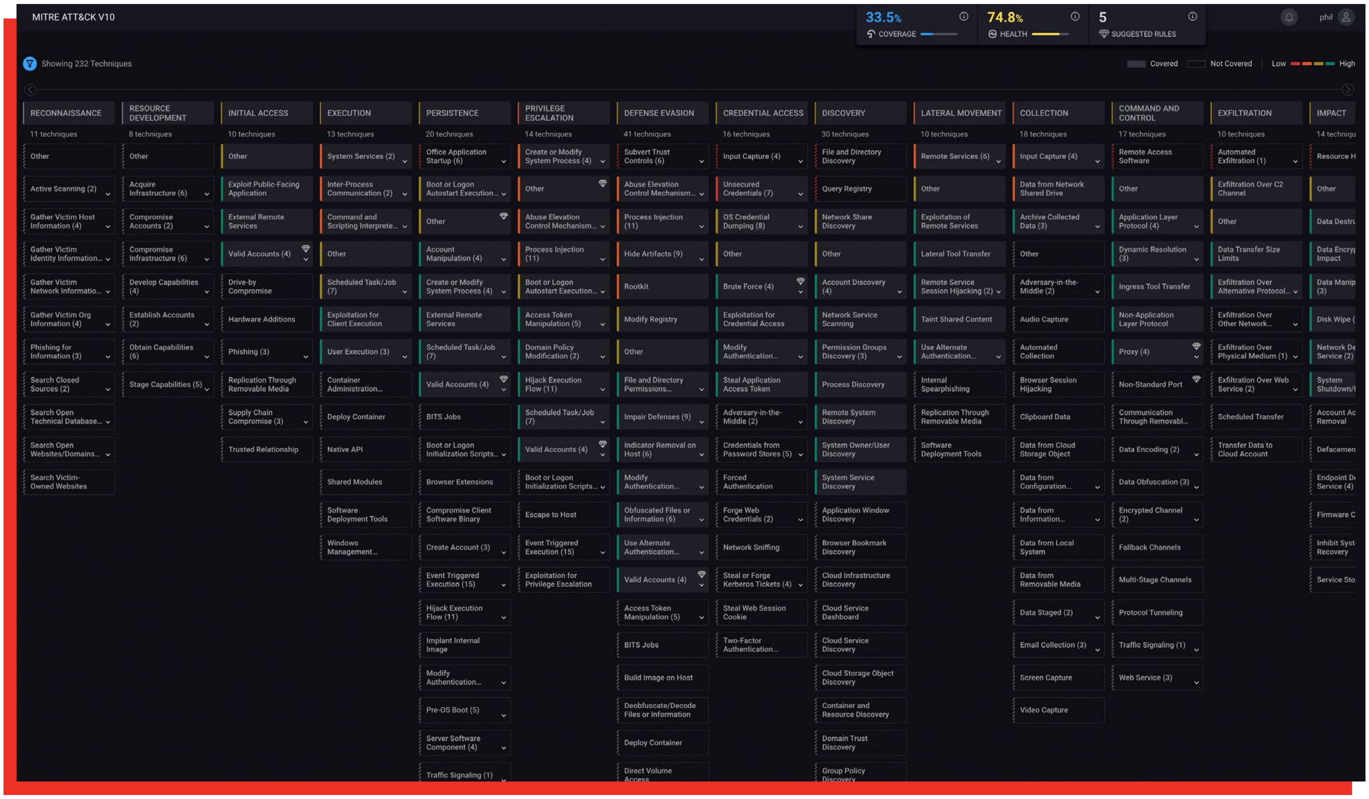
5.0

Screenshot Examples

You can also view a 2-minute demo here.

5.1 MITRE ATT&CK heat map

Map with all ATT&CK techniques color-coded according to health of detection rules. Techniques shown with vertical cross-hatched lines are not covered by any detections.



MITRE ATT&CK V10

33.5% COVERAGE | 74.8% HEALTH | 5 SUGGESTED RULES

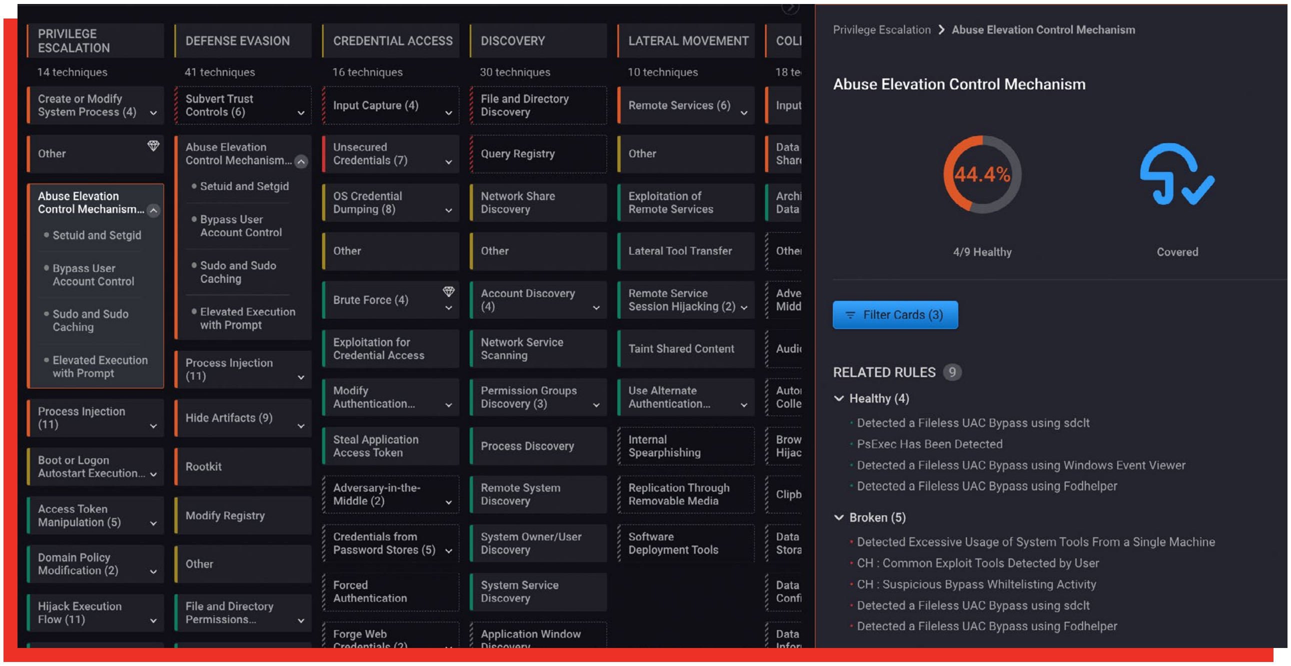
phil

Showing 232 Techniques

Covered | Not Covered | Low High

RECONNAISSANCE	RESOURCE DEVELOPMENT	INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	DEFENSE EVASION	CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND AND CONTROL	EXFILTRATION	IMPACT
11 techniques	8 techniques	10 techniques	13 techniques	20 techniques	14 techniques	41 techniques	16 techniques	30 techniques	10 techniques	18 techniques	17 techniques	10 techniques	14 techniqu
Other	Other	Other	System Services (2)	Office Application Startup (6)	Create or Modify System Process (4)	Subvert Trust Controls (6)	Input Capture (4)	File and Directory Discovery	Remote Services (6)	Input Capture (4)	Remote Access Software	Automated Exfiltration (1)	Resource H
Active Scanning (2)	Acquire Infrastructure (6)	Exploit Public-Facing Application	Inter-Process Communication (2)	Boot or Logon Autostart Execution...	Other	Abuse Elevation Control Mechanism...	Unsecured Credentials (7)	Query Registry	Other	Data from Network Shared Drive	Other	Exfiltration Over C2 Channel	Other
Gather Victim Host Information (4)	Compromise Accounts (2)	External Remote Services	Command and Scripting Interprete...	Other	Abuse Elevation Control Mechanism...	Process Injection (11)	OS Credential Dumping (8)	Network Share Discovery	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Other	Data Destru
Gather Victim Identity Information...	Compromise Infrastructure (6)	Valid Accounts (4)	Other	Account Manipulation (4)	Process Injection (11)	Hide Artifacts (9)	Other	Other	Lateral Tool Transfer	Other	Dynamic Resolution (3)	Data Transfer Size Limits	Data Encryp Impact
Gather Victim Network Informatio...	Develop Capabilities (4)	Drive-by Compromise	Scheduled Task/Job (7)	Create or Modify System Process (4)	Boot or Logon Autostart Execution...	Rootkit	Brute Force (4)	Account Discovery (4)	Remote Service Session Hijacking (2)	Adversary-in-the-Middle (2)	Ingress Tool Transfer	Exfiltration Over Alternative Protocol...	Data Manip (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Hardware Additions	Exploitation for Client Execution	External Remote Services	Access Token Manipulation (5)	Modify Registry	Exploitation for Credential Access	Network Service Scanning	Taint Shared Content	Audio Capture	Non-Application Layer Protocol	Exfiltration Over Other Network...	Disk Wipe (
Phishing for Information (3)	Obtain Capabilities (6)	Phishing (3)	User Execution (3)	Scheduled Task/Job (7)	Domain Policy Modification (2)	Other	Modify Authentication...	Permission Groups Discovery (3)	Use Alternate Authentication...	Automated Collection	Proxy (4)	Exfiltration Over Physical Medium (1)	Network De Service (2)
Search Closed Sources (2)	Stage Capabilities (5)	Replication Through Removable Media	Container Administration...	Valid Accounts (4)	Hijack Execution Flow (11)	File and Directory Permissions...	Steal Application Access Token	Process Discovery	Internal Spearphishing	Browser Session Hijacking	Non-Standard Port	Exfiltration Over Web Service (2)	System Shutdown/I
Search Open Technical Database...		Supply Chain Compromise (3)	Deploy Container	BITS Jobs	Scheduled Task/Job (7)	Impair Defenses (9)	Adversary-in-the-Middle (2)	Remote System Discovery	Replication Through Removable Media	Clipboard Data	Communication Through Removabl...	Scheduled Transfer	Account Ac Removal
Search Open Websites/Domains...		Trusted Relationship	Native API	Boot or Logon Initialization Scripts...	Valid Accounts (4)	Indicator Removal on Host (6)	Credentials from Password Stores (5)	System Owner/User Discovery	Software Deployment Tools	Data from Cloud Storage Object	Data Encoding (2)	Transfer Data to Cloud Account	Defacemen
Search Victim-Owned Websites			Shared Modules	Browser Extensions	Boot or Logon Initialization Scripts...	Modify Authentication...	Forced Authentication	System Service Discovery		Data from Configuration...	Data Obfuscation (3)		Endpoint D Service (4)
			Software Deployment Tools	Compromise Client Software Binary	Escape to Host	Obfuscated Files or Information (6)	Forge Web Credentials (2)	Application Window Discovery		Data from Information...	Encrypted Channel (2)		Firmware C
			Windows Management...	Create Account (3)	Event Triggered Execution (15)	Use Alternate Authentication...	Network Sniffing	Browser Bookmark Discovery		Data from Local System	Fallback Channels		Inhibit Syst Recovery
				Event Triggered Execution (15)	Exploitation for Privilege Escalation	Valid Accounts (4)	Steal or Forge Kerberos Tickets (4)	Cloud Infrastructure Discovery		Data from Removable Media	Multi-Stage Channels		Service Sto
				Hijack Execution Flow (11)		Access Token Manipulation (5)	Steal Web Session Cookie	Cloud Service Dashboard		Data Staged (2)	Protocol Tunneling		
				Implant Internal Image		BITS Jobs	Two-Factor Authentication...	Cloud Service Discovery		Email Collection (3)	Traffic Signaling (1)		
				Modify Authentication...		Build Image on Host		Cloud Storage Object Discovery		Screen Capture	Web Service (3)		
				Pre-OS Boot (5)		Deobfuscate/Decode Files or Information		Container and Resource Discovery		Video Capture			
				Server Software Component (4)		Deploy Container		Domain Trust Discovery					
				Traffic Signaling (1)		Direct Volume Access		Group Policy Discovery					

Map with examples of sub-techniques and broken rules within the technique.



PRIVILEGE ESCALATION — 14 techniques
- Create or Modify System Process (4)
- Other
- Abuse Elevation Control Mechanism...
  - Setuid and Setgid
  - Bypass User Account Control
  - Sudo and Sudo Caching
  - Elevated Execution with Prompt
- Process Injection (11)
- Boot or Logon Autostart Execution...
- Access Token Manipulation (5)
- Domain Policy Modification (2)
- Hijack Execution Flow (11)

DEFENSE EVASION — 41 techniques
- Subvert Trust Controls (6)
- Abuse Elevation Control Mechanism...
  - Setuid and Setgid
  - Bypass User Account Control
  - Sudo and Sudo Caching
  - Elevated Execution with Prompt
- Process Injection (11)
- Hide Artifacts (9)
- Rootkit
- Modify Registry
- Other
- File and Directory Permissions...

CREDENTIAL ACCESS — 16 techniques
- Input Capture (4)
- Unsecured Credentials (7)
- OS Credential Dumping (8)
- Other
- Brute Force (4)
- Exploitation for Credential Access
- Modify Authentication...
- Steal Application Access Token
- Adversary-in-the-Middle (2)
- Credentials from Password Stores (5)
- Forced Authentication
- Forge Web Credentials (2)

DISCOVERY — 30 techniques
- File and Directory Discovery
- Query Registry
- Network Share Discovery
- Other
- Account Discovery (4)
- Network Service Scanning
- Permission Groups Discovery (3)
- Process Discovery
- Remote System Discovery
- System Owner/User Discovery
- System Service Discovery
- Application Window Discovery

LATERAL MOVEMENT — 10 techniques
- Remote Services (6)
- Other
- Exploitation of Remote Services
- Lateral Tool Transfer
- Remote Service Session Hijacking (2)
- Taint Shared Content
- Use Alternate Authentication...
- Internal Spearphishing
- Replication Through Removable Media
- Software Deployment Tools

COLI — 18 te
- Input
- Data Shar
- Archi Data
- Othe
- Adve Midd
- Audi
- Auto Colle
- Brow Hijac
- Clipb
- Data Stora
- Data Confi
- Data Infor

Privilege Escalation > Abuse Elevation Control Mechanism

Abuse Elevation Control Mechanism

44.4% — 4/9 Healthy

Covered

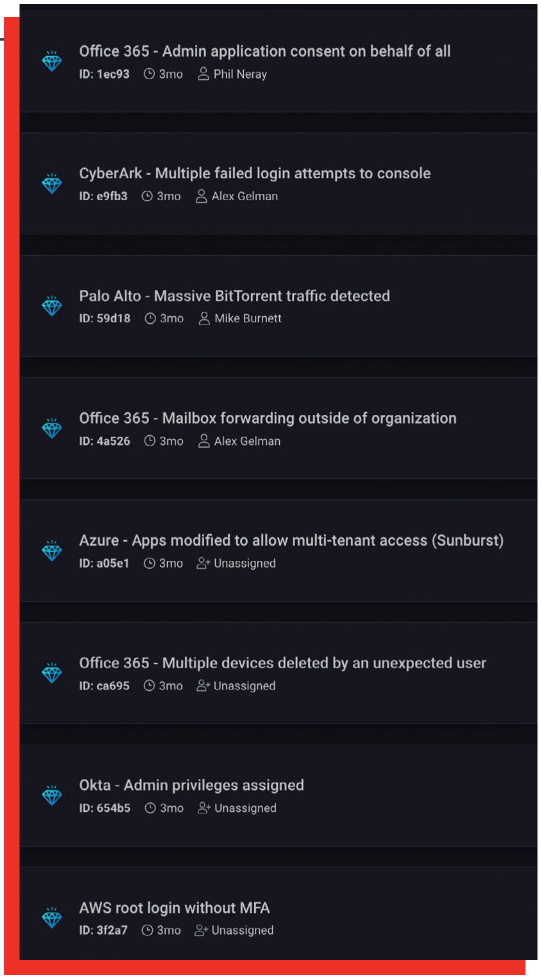
Filter Cards (3)

RELATED RULES 9

Healthy (4)
- Detected a Fileless UAC Bypass using sdclt
- PsExec Has Been Detected
- Detected a Fileless UAC Bypass using Windows Event Viewer
- Detected a Fileless UAC Bypass using Fodhelper

Broken (5)
- Detected Excessive Usage of System Tools From a Single Machine
- CH : Common Exploit Tools Detected by User
- CH : Suspicious Bypass Whiltelisting Activity
- Detected a Fileless UAC Bypass using sdclt
- Detected a Fileless UAC Bypass using Fodhelper

5.2 Recommended rules to close gaps in threat coverage



Office 365 - Admin application consent on behalf of all
ID: 1ec93 3mo Phil Neray

CyberArk - Multiple failed login attempts to console
ID: e9fb3 3mo Alex Gelman

Palo Alto - Massive BitTorrent traffic detected
ID: 59d18 3mo Mike Burnett

Office 365 - Mailbox forwarding outside of organization
ID: 4a526 3mo Alex Gelman

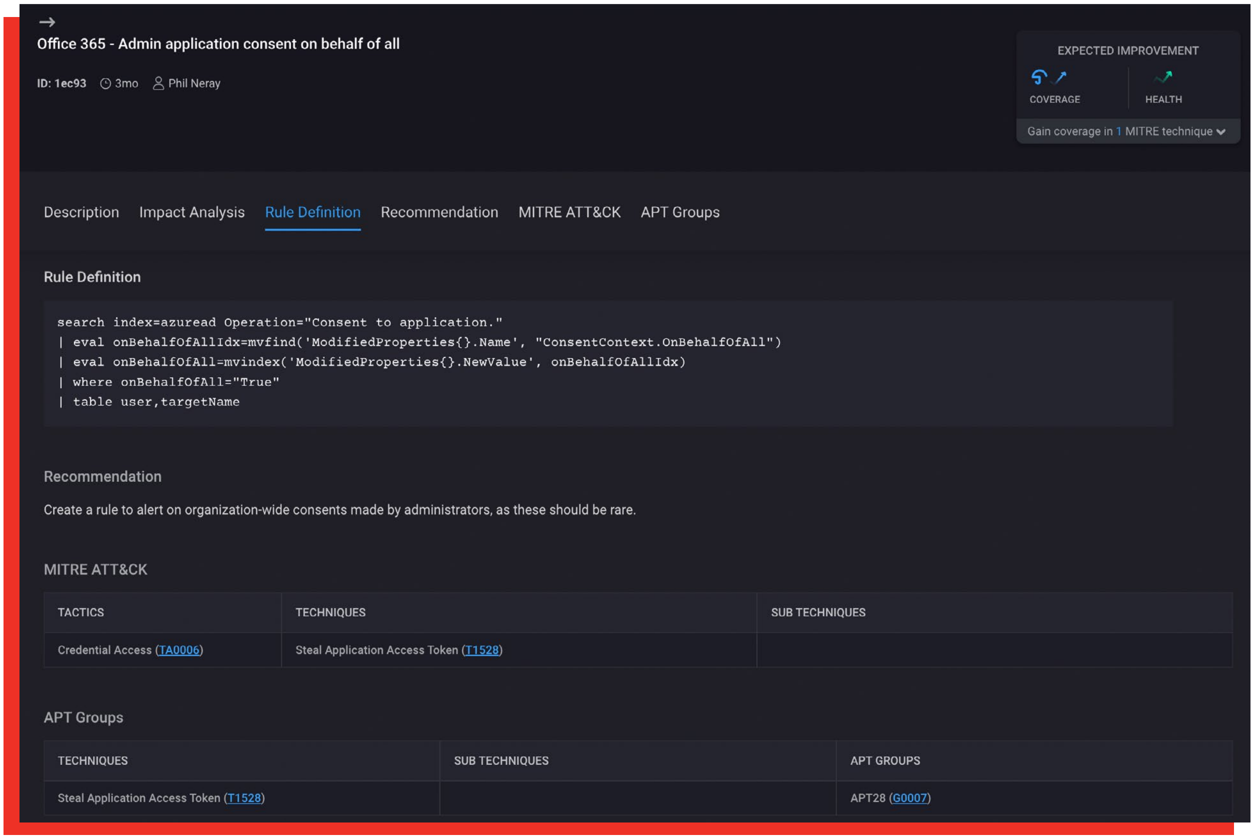
Azure - Apps modified to allow multi-tenant access (Sunburst)
ID: a05e1 3mo Unassigned

Office 365 - Multiple devices deleted by an unexpected user
ID: ca695 3mo Unassigned

Okta - Admin privileges assigned
ID: 654b5 3mo Unassigned

AWS root login without MFA
ID: 3f2a7 3mo Unassigned

5.3 Example of recommended best practice rule to close gaps in ATT&CK coverage



Office 365 - Admin application consent on behalf of all

ID: 1ec93 3mo Phil Neray

Rule Definition

```
search index=azuread Operation="Consent to application."
| eval onBehalfOfAllIdx=mvfind('ModifiedProperties{}.Name', "ConsentContext.OnBehalfOfAll")
| eval onBehalfOfAll=mvindex('ModifiedProperties{}.NewValue', onBehalfOfAllIdx)
| where onBehalfOfAll="True"
| table user,targetName
```

Recommendation

Create a rule to alert on organization-wide consents made by administrators, as these should be rare.

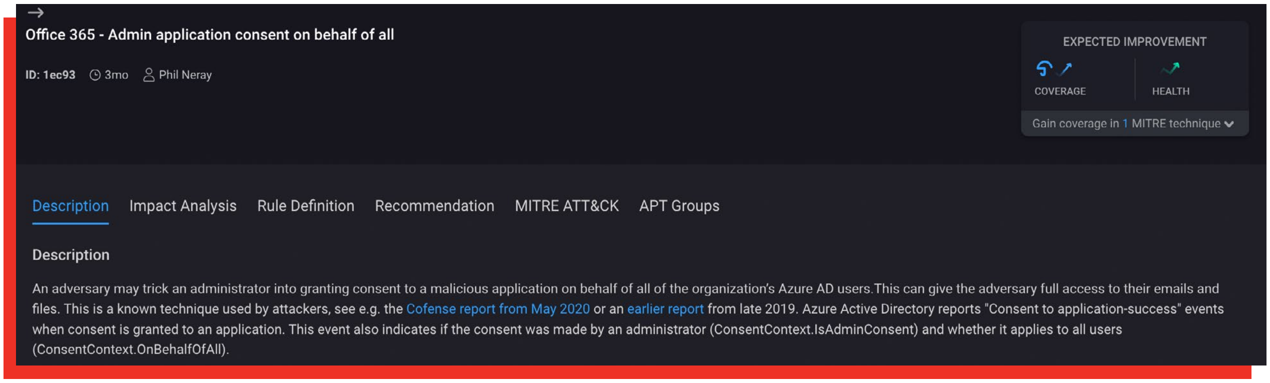
MITRE ATT&CK

TACTICS	TECHNIQUES	SUB TECHNIQUES
Credential Access (TA0006)	Steal Application Access Token (T1528)	

APT Groups

TECHNIQUES	SUB TECHNIQUES	APT GROUPS
Steal Application Access Token (T1528)		APT28 (G0007)

5.4 Description for recommended rule



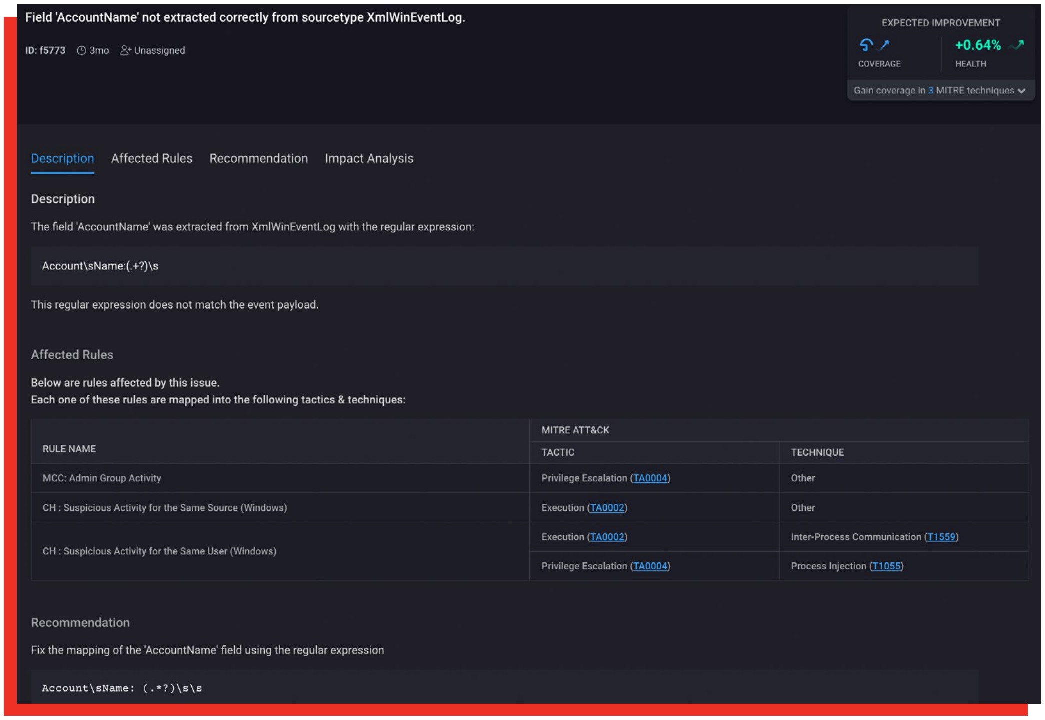
Office 365 - Admin application consent on behalf of all

ID: 1ec93 3mo Phil Neray

Description

An adversary may trick an administrator into granting consent to a malicious application on behalf of all of the organization's Azure AD users.This can give the adversary full access to their emails and files. This is a known technique used by attackers, see e.g. the Cofense report from May 2020 or an earlier report from late 2019. Azure Active Directory reports "Consent to application-success" events when consent is granted to an application. This event also indicates if the consent was made by an administrator (ConsentContext.IsAdminConsent) and whether it applies to all users (ConsentContext.OnBehalfOfAll).

5.5 Example of broken rule with remediation



Field 'AccountName' not extracted correctly from sourcetype XmlWinEventLog.

ID: f5773 · 3mo · Unassigned

Description

The field 'AccountName' was extracted from XmlWinEventLog with the regular expression:

```
Account\sName:(.+?)\s
```

This regular expression does not match the event payload.

Affected Rules

Below are rules affected by this issue.
Each one of these rules are mapped into the following tactics & techniques:

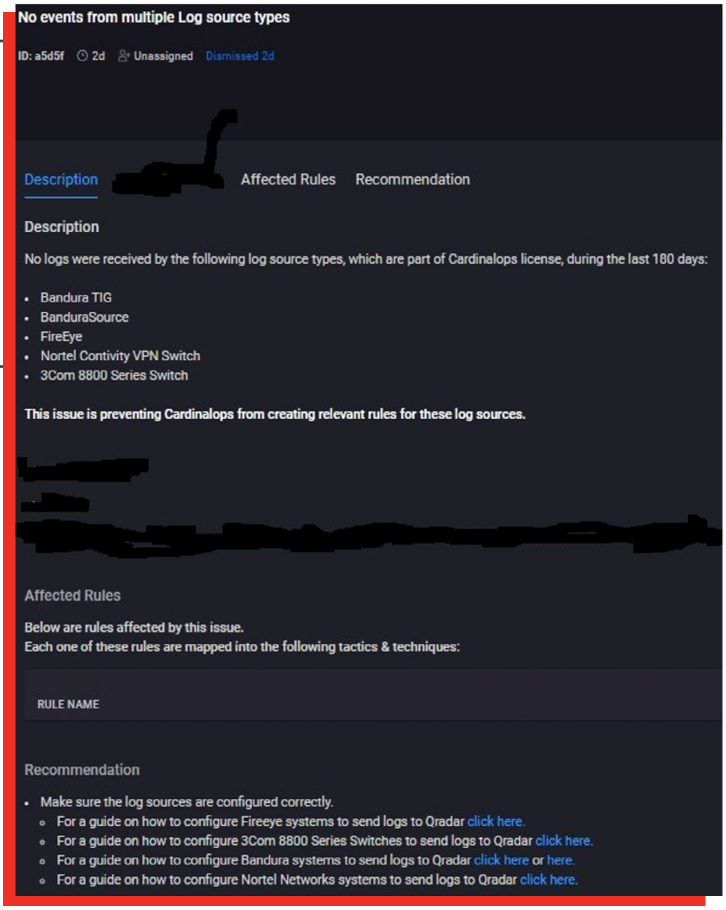
RULE NAME	MITRE ATT&CK	
	TACTIC	TECHNIQUE
MCC: Admin Group Activity	Privilege Escalation (TA0004)	Other
CH : Suspicious Activity for the Same Source (Windows)	Execution (TA0002)	Other
CH : Suspicious Activity for the Same User (Windows)	Execution (TA0002)	Inter-Process Communication (T1559)
	Privilege Escalation (TA0004)	Process Injection (T1055)

Recommendation

Fix the mapping of the 'AccountName' field using the regular expression

```
Account\sName: (.*?)\s\s
```

5.6 Log source types not contributing to detection coverage



No events from multiple Log source types

ID: a5d5f · 2d · Unassigned · Dismissed 2d

Description

No logs were received by the following log source types, which are part of Cardinalops license, during the last 180 days:

- Bandura TIG
- BanduraSource
- FireEye
- Nortel Contivity VPN Switch
- 3Com 8800 Series Switch

This issue is preventing Cardinalops from creating relevant rules for these log sources.

[redacted]

Affected Rules

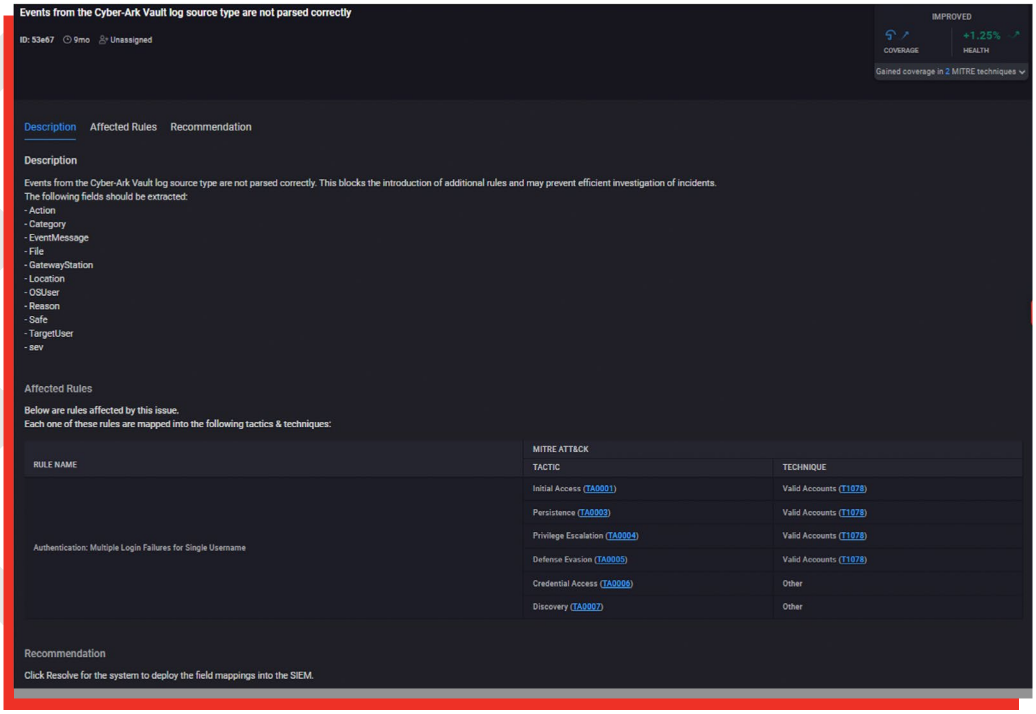
Below are rules affected by this issue.
Each one of these rules are mapped into the following tactics & techniques:

RULE NAME

Recommendation

- Make sure the log sources are configured correctly.
  - For a guide on how to configure Fireeye systems to send logs to Qradar click here.
  - For a guide on how to configure 3Com 8800 Series Switches to send logs to Qradar click here.
  - For a guide on how to configure Bandura systems to send logs to Qradar click here or here.
  - For a guide on how to configure Nortel Networks systems to send logs to Qradar click here.

5.7 Log source types not parsed correctly



Events from the Cyber-Ark Vault log source type are not parsed correctly

ID: 53e67 9mo Unassigned

Description

Events from the Cyber-Ark Vault log source type are not parsed correctly. This blocks the introduction of additional rules and may prevent efficient investigation of incidents.
The following fields should be extracted:
- Action
- Category
- EventMessage
- File
- GatewayStation
- Location
- OSUser
- Reason
- Safe
- TargetUser
- sev

Affected Rules

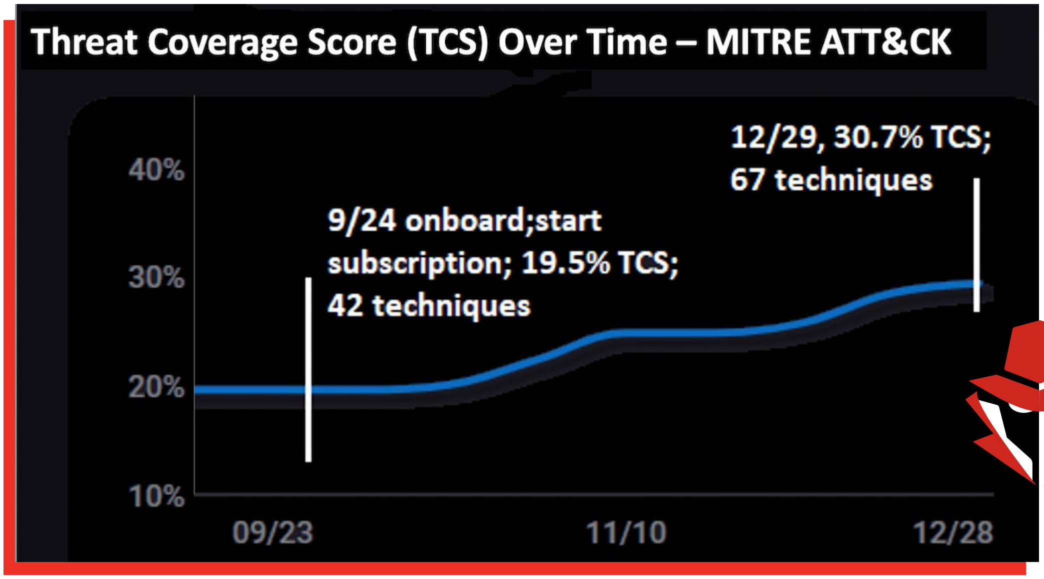
Below are rules affected by this issue.
Each one of these rules are mapped into the following tactics & techniques:

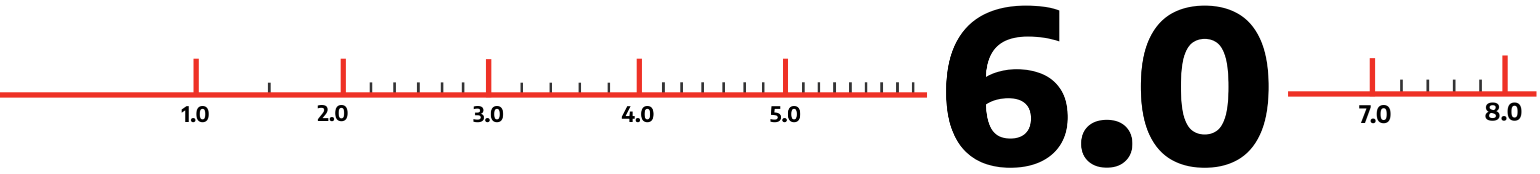
RULE NAME	MITRE ATT&CK	
	TACTIC	TECHNIQUE
Authentication: Multiple Login Failures for Single Username	Initial Access (TA0001)	Valid Accounts (T1078)
	Persistence (TA0003)	Valid Accounts (T1078)
	Privilege Escalation (TA0004)	Valid Accounts (T1078)
	Defense Evasion (TA0005)	Valid Accounts (T1078)
	Credential Access (TA0006)	Other
	Discovery (TA0007)	Other

Recommendation

Click Resolve for the system to deploy the field mappings into the SIEM.

5.8 MITRE ATT&CK coverage score over time





Rapid, Secure, API-Driven Deployment

Deployment is typically achieved in less than an hour.

- The platform connects to your SIEM/XDR's API via provided credentials.
- Secure network connectivity is achieved via your preferred process (Azure Lighthouse, onsite broker VMs, etc.).
- To get an initial health check, you can configure the platform with read-only credentials and only expand permissions later to derive the full platform value from automated provisioning of new and remediated rules.
- The platform never obtains or requires access to log data because it uses the SIEM to run queries on that data. Raw events never leave the SIEM. The platform only requires access to SIEM/XDR configuration information and metadata around detection rules, connectors, data sources, etc.
- Integration with Git-based CI/CD platforms is also enabled via our API.
- The CardinalOps platform is SOC-2 compliant for security and confidentiality, ensuring your SIEM/XDR configuration data is always protected using best practices.

7.0

Key initiatives benefiting from detection use case management

7.1 Operationalize MITRE ATT&CK in your SIEM/XDR

Most organizations track coverage of MITRE ATT&CK using static, manual approaches like spreadsheets. Although some SIEM/XDR vendors have recently begun displaying a coverage map in their platforms, true operationalization requires going beyond simple mapping to include rule recommendations, identification of data quality issues, and customization of detection content to your organizational priorities and infrastructure.

7.2 Securely accelerate cloud transformation initiatives

Organizations are increasingly moving business-critical applications to the cloud. Security teams want to support the business by accelerating cloud initiatives – but without introducing unnecessary risk.

Adding complexity, each cloud platform has its own monitoring tools, which need to be onboarded as log sources to the SIEM/XDR. For example, AWS log sources include S3, VPC, EC2, CloudWatch, and Cloud Trail, as well as both system- and application-layer log sources for containers such as Kubernetes. Plus, new cloud security tools like CSPM and CIEM also require onboarding of new log sources.

CardinalOps helps securely accelerate your cloud initiatives by providing pre-built, ready-to-use detection content for these new log sources.

7.3 Rapidly update detections for high-profile vulnerabilities and attacks

Community sharing, blog posts, and subscription-based content can be helpful with new threats — but copying and pasting generic content is often insufficient for addressing complex threats like log4shell and SolarWinds. CardinalOps can help with rich, high-fidelity detection content that's specifically adapted to your log sources and infrastructure.

7.4 Scale effectiveness of detection engineering teams by 10x

Security talent is hard to find and retain. With CardinalOps, you leverage AI-powered, API-driven automation and analytics to replace tedious and mundane activities (like looking for Regex typos and misconfigured collectors) – so that your best talent can focus on higher-value, more strategic activities — such as researching new and novel attack techniques — thereby boosting morale and retention.

In fact, customers tell us the platform has increased the detection content output of their security engineering teams by a factor of 10 compared to their previous manual approaches.

8.0 Customer Examples

The CardinalOps platform is currently in SOCs protecting some of the world's largest and most complex organizations, across diverse verticals including financial services, manufacturing, hospitality, media, transportation & logistics, law firms, and managed security services.

Chosen by Global Organizations

Top 10 CPG Manufacturer

Top 10 Private Equity Firm

Top 20 Retail Cosmetics firm

Top 10 Casino Company

Top 10 Money Transfer Firm

Top 10 US Law Firm

Top 15 MDR Prodivder

$3B Fteight Logistics Firm

Top 10 Cable Operator

ABOUT CARDINALOPS

CardinalOps' cloud-based platform continuously ensures your SIEM/XDR has high-fidelity detections for the adversary techniques most relevant to your business priorities and infrastructure, as measured by the MITRE ATT&CK framework.

Leveraging proprietary analytics and API-driven automation, the platform continuously delivers automatically customized, deployment-ready detection content and metrics enabling your SOC team to stay ahead of constant change in the attack surface and threat landscape – plus continuously identify and remediate broken rules and misconfigured log sources – so you can close the riskiest detection gaps that leave your organization exposed.

Founded in early 2020, CardinalOps is led by serial entrepreneurs whose previous companies were acquired by Palo Alto Networks, HP, Microsoft Security, IBM Security, and others. The company's advisory board includes Dr. Anton Chuvakin, recognized SIEM expert and former Gartner Research VP (now Head of Security Solution Strategy at Google); Dan Burns, former Optiv CEO and founder of Accuvant; and Randy Watkins, CTO of Critical Start.

For more information, please visit www.cardinalops.com.

X X X X X X X X

X X X X X X X X

X X X X X X X X