CYBER GIRLS

IMPLEMENTING THE MITRE ATT&CK FRAMEWORK IN SOC OPERATIONS: DISCUSS HOW THE MITRE ATT&CK CAN BE INTEGRATED INTO THE SOC PROCESSES TO ENHANCE THREAT DETECTION AND RESPONSE

An Initiative of cybersafe. FOUNDATION

CYBER GIRLS

INTRODUCTION

Objective:

This project focuses on integrating the **MITRE ATT&CK Framework** into the **Security Operations Center (SOC)** processes to enhance threat detection, investigation, and response capabilities. The **ATT&CK Framework**, which maps adversary behavior across the attack lifecycle, provides SOC analysts with a detailed understanding of various tactics and techniques used by cyber attackers. By embedding this framework into SOC workflows, the goal is to enhance visibility into attacks, streamline the response process, and improve overall cybersecurity posture.

CYBER GIRLS

BACKGROUND OF THE MITRE ATT&CK FRAMEWORK

MITRE ATT&CK was created in 2013 and publicly released in 2015 through MITRE's Fort Meade Experiment (FMX). In this project, researchers simulated both adversary and defender actions to improve threat detection on Windows systems, using telemetry and behavioral analysis. The key question driving their work was, “How effective are we at detecting documented adversary behavior?” **ATT&CK** was built to categorize and assess these behaviors, and since its release, it has expanded to cover Linux, macOS, mobile devices, cloud, and industrial control systems (ICS).

Unlike other cybersecurity models focusing primarily on defense mechanisms, MITRE ATT&CK takes the attacker’s perspective. This approach enables organizations to see how adversaries think and operate, making anticipation of their moves and mitigating risks easier. Initially used for threat detection, the framework is now widely adopted for vulnerability management, threat intelligence, and incident response.

CYBER GIRLS

DEFINITION OF THE MITRE ATT&CK FRAMEWORK

The {MITRE ATT&CK} framework stands for MITRE Adversarial Tactics, Techniques, and Common Knowledge. It is a detailed knowledge base that organizes and models the behaviors of cyber adversaries, highlighting different stages of an adversary's attack lifecycle and the platforms they commonly target.

Key milestones in the framework’s evolution

- 2017: Expansion to cover macOS and Linux.
- 2017: Introduction of the Mobile ATT&CK Matrix for threats targeting mobile devices.
- 2019: Launch of ATT&CK for Cloud, focusing on cloud environments like AWS, Azure, and Google Cloud.
- 2020: Introduction of sub-techniques to add granularity to existing techniques, allowing for more precise documentation of adversarial behaviors.

CYBER GIRLS

UNDERSTANDING THE MITRE ATT&CK MATRIX

Enterprise ATT&CK Matrix

The Enterprise ATT&CK matrix covers tactics and techniques adversaries use to attack enterprise networks, including various platforms like Windows, macOS, Linux, Azure AD, and SaaS environments.

ICS ATT&CK Matrix

The ICS ATT&CK matrix is designed for industrial control systems in the energy, manufacturing, and utilities sectors. This matrix includes tactics and techniques unique to ICS environments, such as manipulating control system devices or exploiting industrial protocols.

Mobile ATT&CK Matrix

The Mobile ATT&CK matrix focuses on threats to mobile devices. It highlights tactics and techniques for iOS and Android platforms. It also covers methods attackers use without requiring physical access to the device, such as exploiting mobile apps or network services.

CYBER GIRLS

COMPONENTS OF THE MITRE ATT&CK FRAMEWORK

The MITRE ATT&CK framework is built around three core components: **TACTICS:** The “why” of an attack. Each tactic represents a goal an adversary wants to achieve, such as gaining initial access or executing a malicious payload**. TECHNIQUES:** The “how” of an attack. These are the methods adversaries use to achieve their tactical goals. **SUB-TECHNIQUES**: More detailed descriptions of the techniques. For example, the brute force technique can be divided into sub-techniques like password guessing, password cracking, password spraying, and credential stuffing. **PROCEDURES:** Specific instances of techniques used in actual attacks.

CYBER GIRLS

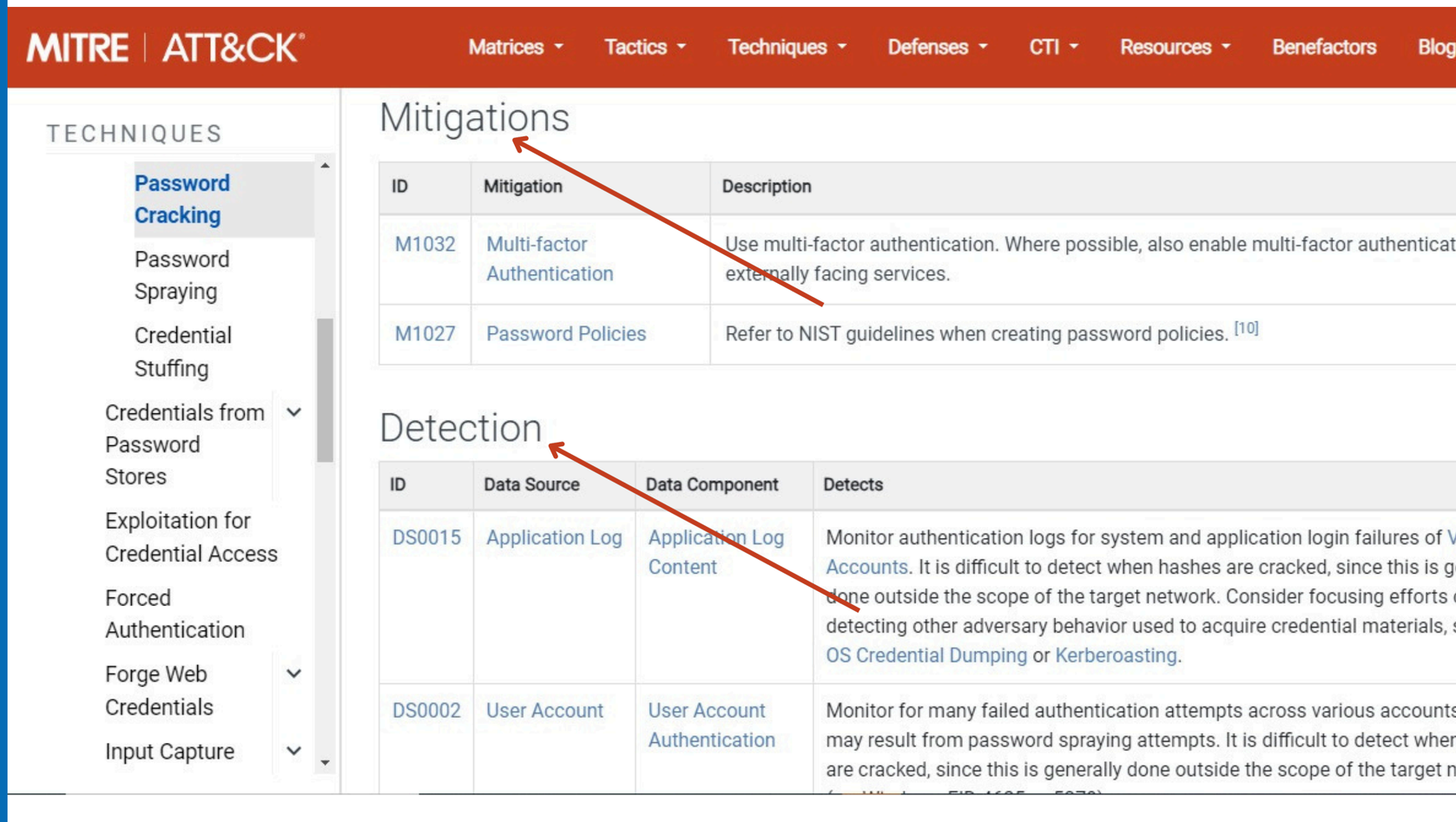
SUPPORTING COMPONENTS

Mitigation

Provides preventative measures organizations can take to stop or reduce the likelihood of successful techniques. These could be technical controls, process changes, or user education.

Detection & Data source

These are types of logs, events, and system outputs (e.g., process monitoring, network traffic analysis, file monitoring) used to detect adversary behaviors. ATT&CK maps these data sources to techniques, guiding SOC analysts on where to look for evidence of specific tactics, and making it easier to set up detection mechanisms.



CYBER GIRLS

THE ENTERPRISE ATT&CK MATRIX TACTICS

1. Reconnaissance
2. Resource development
3. Initial access
4. Execution
5. Persistence
6. Privilege escalation
7. Defense evasion
8. Credential access
9. Discovery
10. Lateral movement
11. Collection
12. Command & control
13. Exfiltration
14. Impact

CYBER GIRLS

How the MITRE ATT&CK Framework Enhances SOC Capabilities

Provides a Unified Classification System

The ATT&CK framework provides a common language for describing adversary activities. This standardization improves communication between SOC teams, allowing for better coordination across different tools and skill sets.

Expanding Detection Coverage

The framework lists hundreds of adversary tactics and techniques, making it easier for SOC teams to identify gaps in their current detection methods. By comparing existing capabilities with the ATT&CK matrix, SOCs can pinpoint blind spots and add new detection strategies.

Improving Detection Accuracy

The framework helps improve the accuracy of detection mechanisms. Analysts can use specific techniques and sub-techniques to create more accurate alerts, reducing false positives.

Better Threat Hunting

ATT&CK can also guide proactive threat-hunting efforts. By understanding how adversaries typically operate once they gain access, hunters can search for early indicators of attack, potentially identifying threats before significant damage occurs.

CYBER GIRLS

How the MITRE ATT&CK Framework Enhances SOC Capabilities

- **Enhanced Incident Investigation**

SOC analysts can use the ATT&CK framework as a reference when investigating incidents. By mapping evidence to known tactics and techniques, they can quickly determine how an adversary operates and anticipate their next move. This makes investigations more focused and effective.

- **Prioritizing Defense Efforts**

Using the ATT&CK framework, organizations can prioritize their security investments by focusing on the most critical tactics and techniques used by adversaries. This ensures resources are allocated to address the highest-risk areas, improving overall defenses.

CYBER GIRLS

Step-by-Step Guide to Implementing MITRE ATT&CK in Your SOC

STEP 1

Understand the MITRE ATT&CK Framework

STEP 2

Assess Your Current SOC Capabilities

STEP 3

Map MITRE ATT&CK to Your SOC Tools and Processes

STEP 4

Develop Use Cases and Detection Rules

STEP 5

Implement Threat Intelligence Integration

STEP 6

Enhance Incident Response

STEP 7

Train Your SOC Team

STEP 8

Continuously Monitor and Improve

STEP 9

Document and Share Insights

CYBER GIRLS

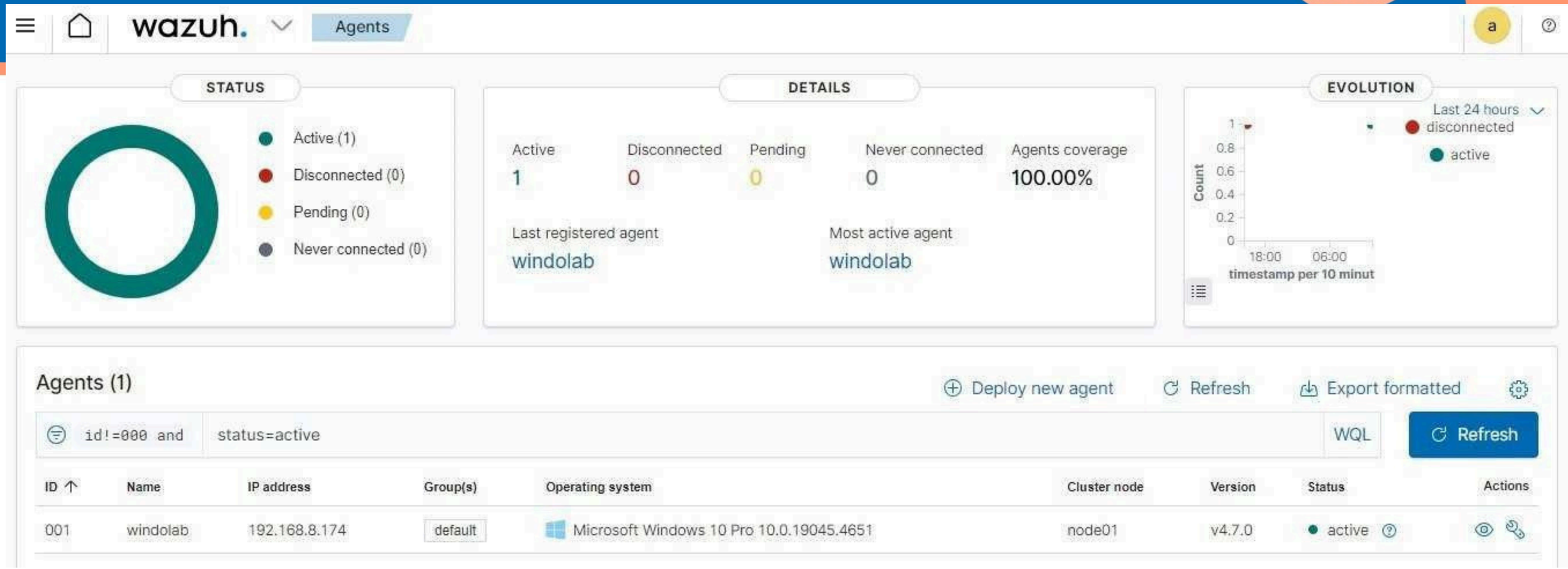
Security Tools with Built-in MITRE ATT&CK Integration

Several security tools integrate the MITRE ATT&CK framework, leveraging its structured approach to identify and classify adversarial tactics, techniques, and procedures. Here are some prominent ones:

Splunk
Microsoft Defender for Endpoint
IBM QRadar
CrowdStrike Falcon
ThreatConnect
Exabeam
Cortex XSOAR (Palo Alto Networks)
FireEye Helix
Wazuh

CYBER GIRLS

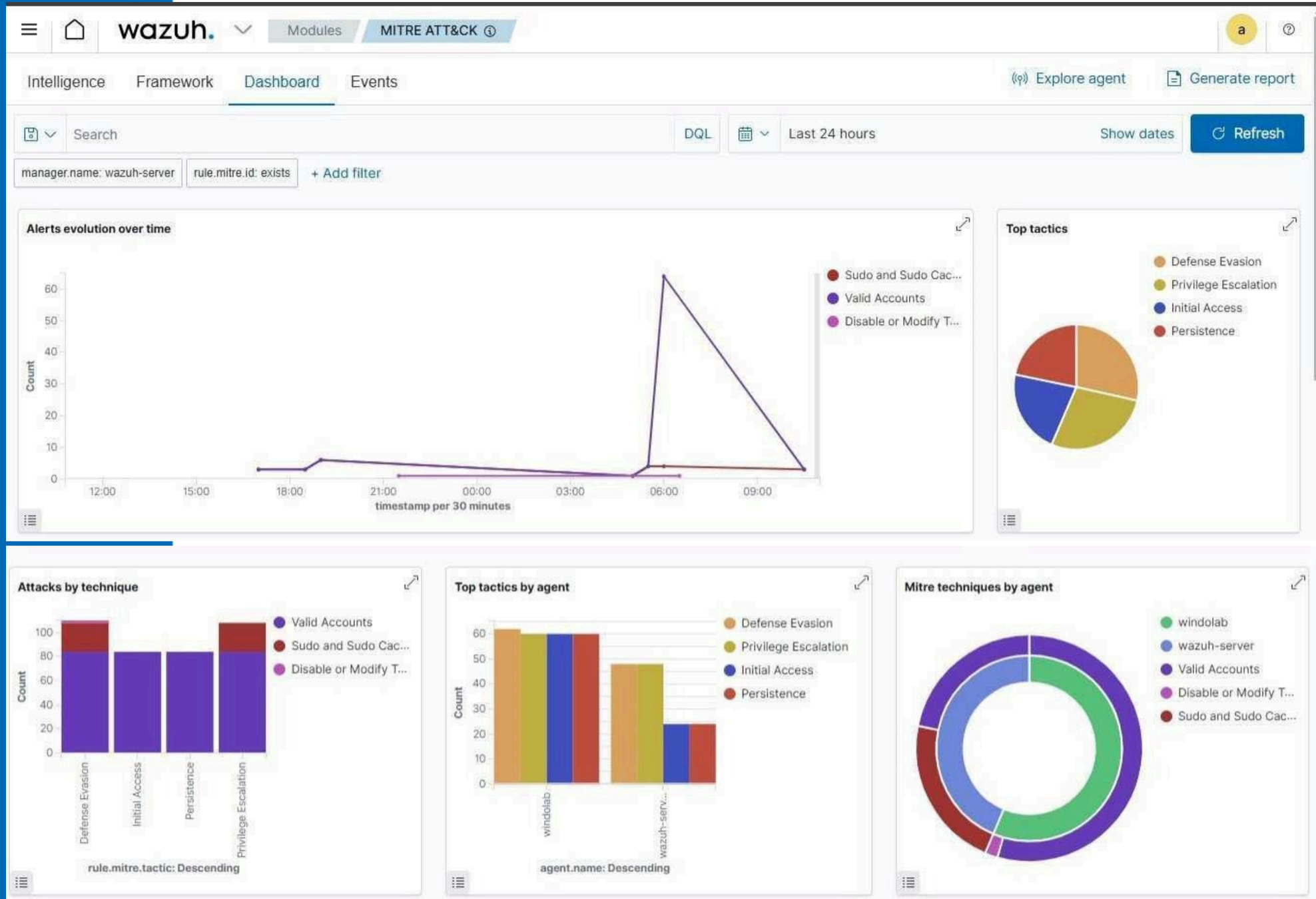
Pratical

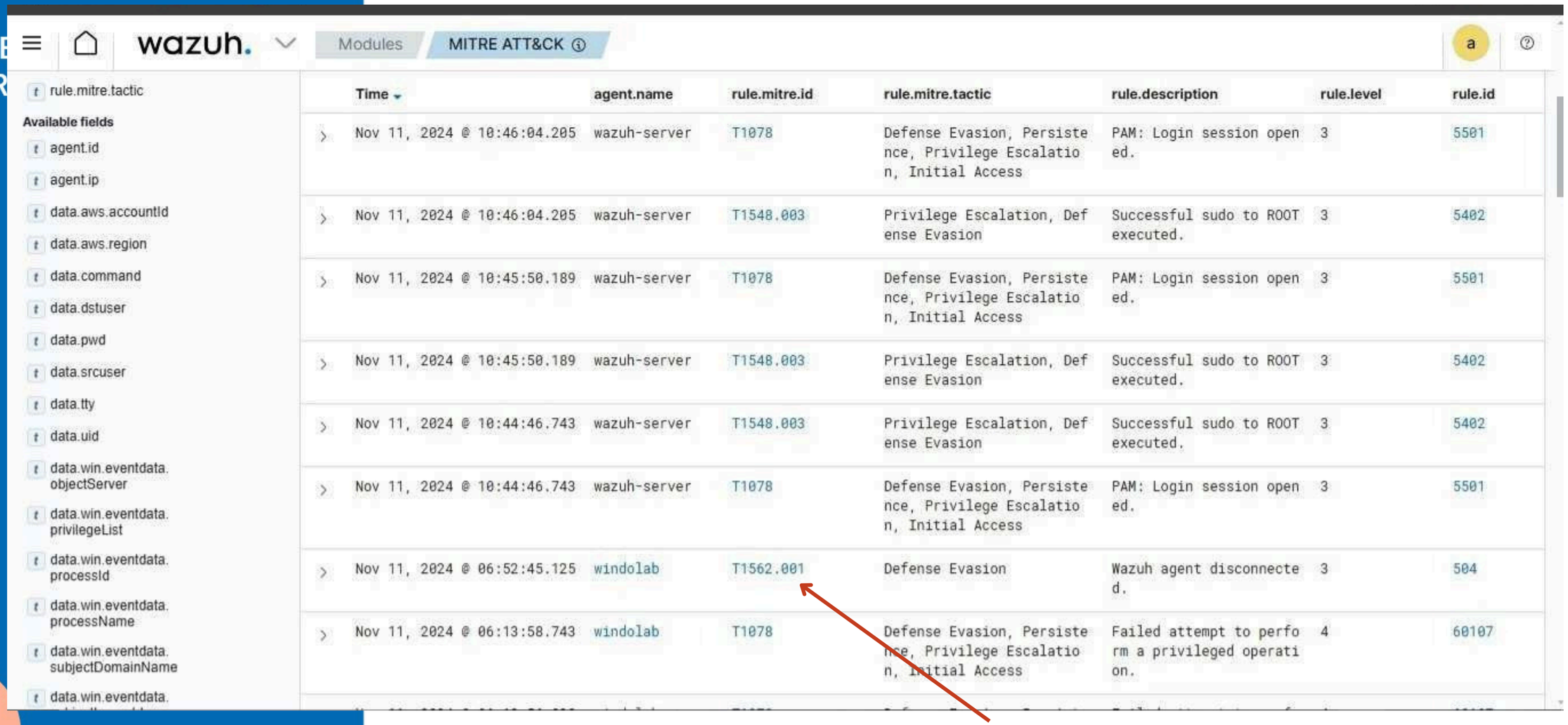


For this demonstration, we used the WAZUH SIEM tool, which already has a module integrated with the MITRE ATT&CK. We also used ATOMIC We will be using this tool to simlate an attack on our Windows OS (VM), then use the SIEM to capture the logs and analyze how the SIEM detects and categorizes the detected tactics according to the MITRE ATT&CK framework.

CYBER GIRLS

Dashboard showing metrics for the detected potential threats





A list showing a number of malicious events that was captured by the SIEM during the simulation and the various categorization according to the MITRE ATT&CK framework. We will be focusing on T1562.00

CYBER GIRLS

wazuh. Modules MITRE ATT&CK

Disable or Modify Tools

T1562.001

Tactics
Defense Evasion

Version
1.2

Recent events

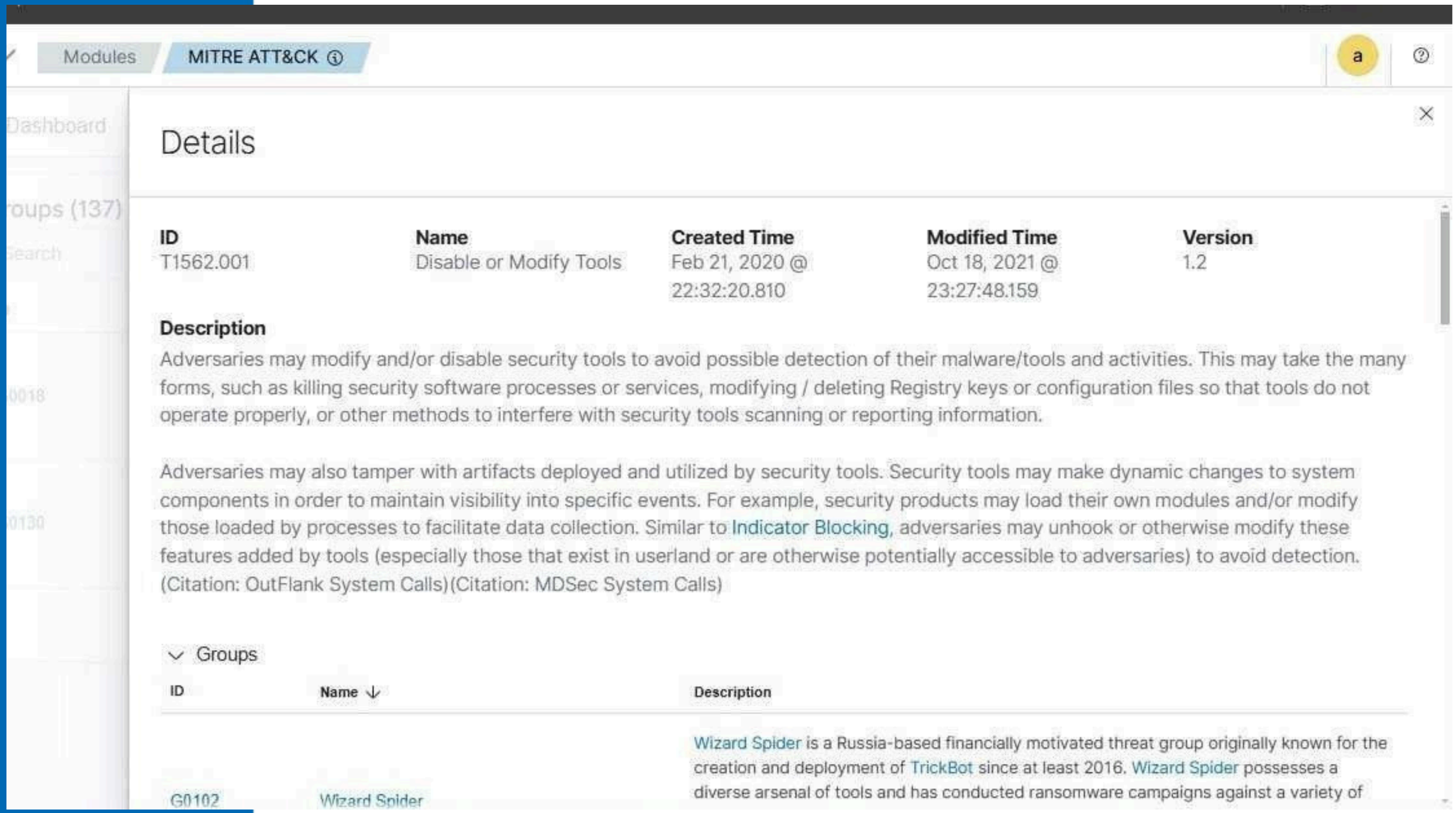
2 hits

Search DQL Last 24 hours Show dates Refresh

+ Add filter

Time	Agent	Agent Name	Technique(s)	Tactic(s)	Level	Rule ID	Description
Nov 11, 2024 @ 06:52:45.125	001	windolab	T1562.001	Defense Evasion	3	504	Wazuh agent disconnected.
Nov 10, 2024 @ 21:32:16.270	001	windolab	T1562.001	Defense Evasion	3	504	Wazuh agent disconnected.

CYBER GIRLS


Modules
MITRE ATT&CK
a
Dashboard
roups (137)
Search
Details
ID
T1562.001
Name
Disable or Modify Tools
Created Time
Feb 21, 2020 @ 22:32:20.810
Modified Time
Oct 18, 2021 @ 23:27:48.159
Version
1.2
Description
Adversaries may modify and/or disable security tools to avoid possible detection of their malware/tools and activities. This may take the many forms, such as killing security software processes or services, modifying / deleting Registry keys or configuration files so that tools do not operate properly, or other methods to interfere with security tools scanning or reporting information.
Adversaries may also tamper with artifacts deployed and utilized by security tools. Security tools may make dynamic changes to system components in order to maintain visibility into specific events. For example, security products may load their own modules and/or modify those loaded by processes to facilitate data collection. Similar to Indicator Blocking, adversaries may unhook or otherwise modify these features added by tools (especially those that exist in userland or are otherwise potentially accessible to adversaries) to avoid detection. (Citation: OutFlank System Calls)(Citation: MDSec System Calls)
Groups
ID
Name
Description
G0102
Wizard Spider
Wizard Spider is a Russia-based financially motivated threat group originally known for the creation and deployment of TrickBot since at least 2016. Wizard Spider possesses a diverse arsenal of tools and has conducted ransomware campaigns against a variety of

CYBER GIRLS

wazuh. Modules MITRE ATT&CK

Intelligence Framework Dashboard Events

Search in all resour

- Groups
- Mitigations
- Software
- Tactics
- Techniques

Groups (137)

Search WQL

ID	Name	Description
G0018	admin@338	admin@338 is a China-based cyber threat group. It has previously used newsworthy events as lures to deliver malware and has primarily targeted organizations involved in financial, economic, and trade policy, typically using publicly available RATs such as PoisonIvy, as well as some non-public backdoors. (Citation: FireEye admin@338)
G0130	Ajax Security Team	Ajax Security Team is a group that has been active since at least 2010 and believed to be operating out of Iran. By 2014 Ajax Security Team transitioned from website defacement operations to malware-based cyber espionage campaigns targeting the US defense industrial base and Iranian users of anti-censorship technologies.(Citation: FireEye Operation Saffron Rose 2013)
		Andariel is a North Korean state-sponsored threat group that has been active since at least 2009. Andariel has primarily focused its operations–which have included destructive attacks–against South

CYBER GIRLS

wazuh. Modules MITRE ATT&CK

Intelligence Framework Dashboard

Search in all resour

Groups

Mitigations

Software

Tactics

Techniques

Groups (137)

Search

ID

G0018

G0130

Details

Mitigations

ID	Name	Description
M1018	User Account Management	Manage the creation, modification, use, and permissions associated to user accounts.
M1024	Restrict Registry Permissions	Restrict the ability to modify certain hives or keys in the Windows Registry.
M1022	Restrict File and Directory Permissions	Restrict access by setting directory and file permissions that are not specific to users or privileged accounts.

Rows per page: 5

1

Software

ID	Name	Description
S0412	ZxShell	ZxShell is a remote administration tool and backdoor that can be downloaded from the Internet, particularly from Chinese hacker websites. It has been used since at least 2004. (Citation: FireEye APT41 Aug 2019)(Citation: Talos ZxShell Oct 2014)

CYBER GIRLS

Risks/ challenges of Integrating MITRE ATT&CK and mitigations

1. Tool Compatibility Issues

Mitigation: Conduct thorough tool assessments to ensure seamless integration of ATT&CK mappings.

2. Overwhelming Data Volume and Complexity Risk

Mitigation: - Focus on Critical TTPs
- Automation
- Phased Integration

3. Misaligned Detection Capabilities Risk(Tool Incapabilities)

Mitigation: - Gap Analysis
- Enhanced Logging and Monitoring
- Third-Party Integrations

4. Over-Reliance on the Framework Risk

Mitigation: - Complement ATT&CK with other frameworks and threat intelligence sources to ensure a well-rounded security posture.

5. Resource Constraints and Skill Gaps Risk

Mitigation: - Training and Upskilling
- Hiring and External Support
- Leverage Existing Tools

CYBER GIRLS

How MITRE ATT&CK, SIEM, and SOC work together to secure organisations

THE SIEM

SIEM tools are one part of a tripod system for automated threat detection and response. The SIEM relies on two key supports: a TTP knowledge base and an experienced SOC. TTPs enable SIEM to connect unusual activity to known threats and suggest responses, while the SOC provides essential human insight to distinguish real threats from false positives and choose the right actions. With most breaches involving human error, the SOC plays a critical role in reporting to management and promoting robust security practices.

THE ROLE OF SOC

The automated aspect of security requires human management as well. The tuning of the SIEM so that it strikes the right balance between false positives and missed concerns requires judgment and experience. The prioritization of security issues depends on an understanding which assets are most critical and most likely to be targeted.

CYBER GIRLS

Conclusion

The **MITRE ATT&CK framework**, **SIEM**, and **SOC** form a tripod essential for operational security. The **ATT&CK** matrix provides a foundational knowledge base for identifying and classifying hostile actions, but it's vast and frequently updated content requires expertise to use fully. For many purposes, software can use that information more effectively than humans. The **SIEM** system uses that information to recognize the occurrence of these threats and counter them.

The **SOC** then acts on **SIEM** alerts, analyzing reports, managing security, and responding to potential threats across the network. **SIEM** systems can use its API to query for information about patterns of action and zero in on specific threats and solutions. while security teams use the **ATT&CK** Navigator to explore threat patterns and drill down interactively for information by reviewing the list of techniques that could implement a tactic.Constant updates to the ATT&CK matrix keep teams informed on evolving threats, enabling adjustments to defenses and system configurations.

Together, **ATT&CK**, **SIEM**, and **SOC** provide a comprehensive defense, combining intelligence, automation, and human insight to maintain strong security.

CYBER GIRLS

References

- *Martin Johnson, (2024) Guide to the MITRE ATT&CK Framework | Balbix. Retrieved Oct 2024, from: https://www.balbix.com/insights/what-is-the-mitre-attck-framework*
- *Trellix, (2024)What Is the MITRE ATT&CK Framework? | Get the 101 Guide | Trellix*
- *Paul Kirvan, Kinza Yasar, Ben Lutkevich, (2024)What is the Mitre ATT&CK Framework? | Definition from TechTarget*
- *Alex Stevens, (2024)How to use the MITRE ATT&CK Framework to Develop a Threat-Driven Security Operations Center (SOC)*
- *Jason Miller, (2020) How to Use MITRE ATT&CK, SIEM and SOC to Improve Security*
- *Alsheh, E. (2023) Creating a smarter SOC with the MITRE ATT&CK framework. Retrieved Oct 2024,from: https://www.cyberproof.com/blog/creating-a-smarter-soc-with-the-mitre-attck-framework/.*
- *erik.episcopo, (2023) What is the Mitre Att&ck Framework? | CrowdStrike. Retrieved Oct 2024, from: https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/mitre-attack-framework/.*
- *Cardona, H. (2024) Enhancing SOC Assessments with MITRE ATT&CK:. Retrieved Oct 2024, from: https://www.winmill.com/enhancing-soc-assessments-with-mitre-attck/.*

CYBER GIRLS

Thank You

An Initiative of cybersafe. FOUNDATION