Using MITRE ATT&CK® in Threat Hunting and Detection

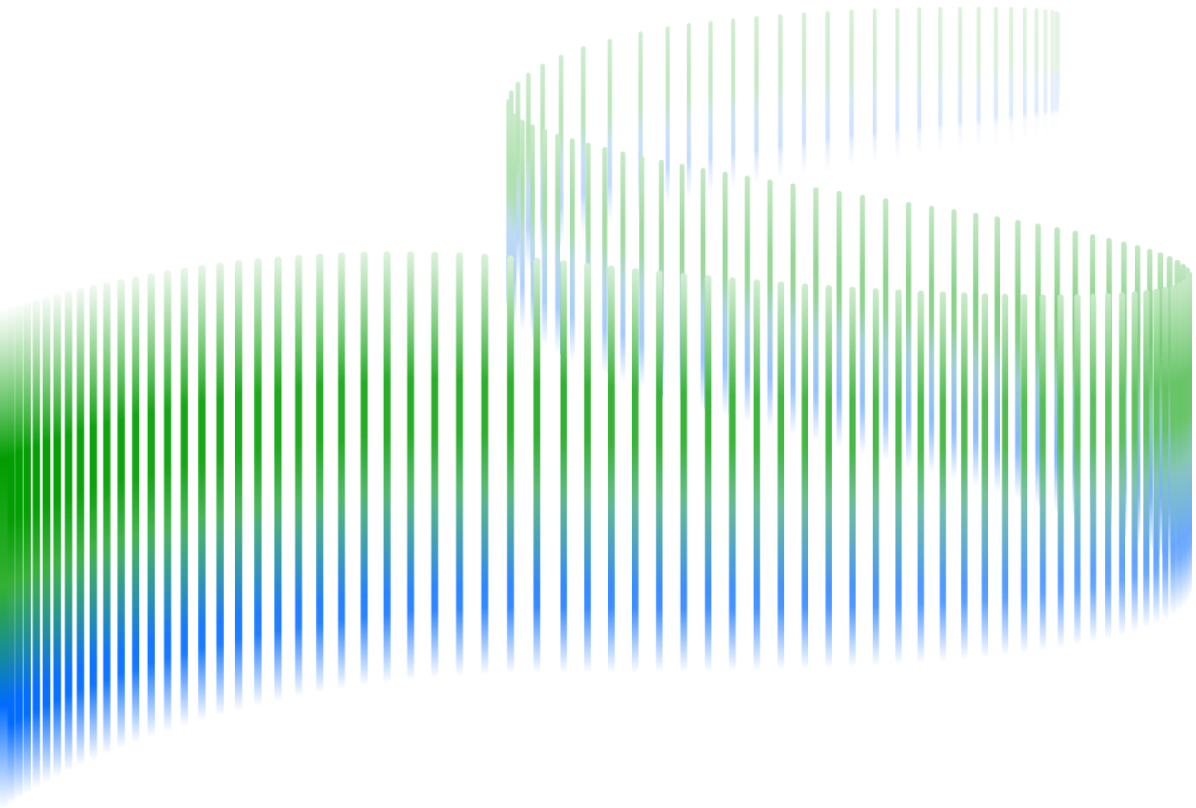


Table of Contents

Executive Summary

MITRE ATT&CK® is an open framework that catalogs adversary tactics and techniques based on real-world observations. It provides a standardized language for describing adversaries' objectives and methods, crucial for communication within the security community. Beyond serving as a taxonomy, ATT&CK is a practical tool that helps you improve your detection efforts, identify gaps, and understand where you're blind to specific attack behaviors.

This paper introduces ATT&CK and its related tools and resources. You'll learn how to apply ATT&CK for effective threat hunting and detection.

Understanding MITRE ATT&CK

In this section, we break down ATT&CK's structure, which includes:

- **Tactics**: The strategic goals of an attacker (for example, gaining initial access or exfiltrating data)
- **Techniques**: The specific methods attackers use to achieve their tactics
- **Mitigation**: Suggested methods to prevent or reduce the impact of these techniques
- **Detection**: Ways to identify when attackers are using these techniques

Using MITRE ATT&CK

After providing an overview of ATT&CK's broad use cases, we'll focus specifically on how to:

- Perform a gap analysis to identify the malicious behaviors you're currently missing
- Improve your threat detection and hunting capabilities
- Test your detection rules to ensure they trigger the right alerts when needed

We'll also explore five key techniques from ATT&CK, selected for their relevance to threat hunting and detection. You'll learn how attackers use these techniques, how to detect them, which logs to collect, the audit policies to implement, and how Exabeam integrates detection logic for these techniques into our LogRhythm SIEM and New-Scale Security Operations Platforms.

Understanding MITRE ATT&CK

Tactics

Tactics are the highest level of organization in the ATT&CK framework. They represent the strategic objectives an attacker seeks to achieve, such as extorting ransom, stealing data, or disrupting systems. Attackers must achieve these goals through a series of incremental, short-term objectives.

The updated ATT&CK framework now includes additional tactics that reflect adversaries' evolving methods:

- **Reconnaissance (TA0043)**: Gathering information to plan future operations, such as identifying system weaknesses or researching target infrastructure
- **Resource Development (TA0042)**: Establishing resources like infrastructure, tools, and accounts to support attack activities.

Most attacks begin with **Reconnaissance (TA0043)**, where adversaries gather information to plan their next steps. They may then move on to **Resource Development (TA0042)**, setting up infrastructure and tools to support their attack. Once these preparations are in place, attackers gain **Initial Access (TA0001)**, followed by tactics like **Execution (TA0002)** and **Persistence (TA0003)**. If the goal is data theft, the attacker will proceed to **Collection (TA0009)** and **Exfiltration (TA0010)**. Throughout the attack, they may use **Lateral Movement (TA0008)** or employ **Defense Evasion (TA0005)** to avoid detection.

Tactics focus on an attacker's intent—what they aim to accomplish at each phase. They don't specify the methods used. Following is a table outlining some of the key tactics in the ATT&CK framework, highlighting the primary phases of an adversary's attack lifecycle.

ID	Name	Description
TA0001	Initial Access	Methods used by adversaries to gain entry into a network
TA0002	Execution	Techniques that result in the execution of adversary-controlled code on a local or remote system
TA0003	Persistence	Actions taken to maintain access to a system despite interruptions, such as restarts or credential loss
TA0004	Privilege Escalation	Techniques that enable adversaries to gain higher levels of system access or privileges
TA0005	Defense Evasion	Methods used to avoid detection or bypass defenses
TA0006	Credential Access	Techniques for obtaining control over system or service credentials, allowing adversaries to assume identities
TA0007	Discovery	Techniques that provide adversaries with knowledge about the system and internal network
TA0008	Lateral Movement	Techniques allowing adversaries to access and control remote systems on a network
TA0009	Collection	Methods for gathering sensitive data, such as files or system information, in preparation for exfiltration
TA0010	Exfiltration	Techniques used to remove data from a network
TA0011	Command and Control	Methods for establishing communication between adversaries and compromised systems
TA0040	Impact	Techniques aimed at damaging or disrupting the confidentiality, integrity, or availability of systems or data
TA0042	Resource Development	Techniques for establishing resources like infrastructure or tools for attacks
TA0043	Reconnaissance	Techniques used to gather information about a target prior to execution

Table 1. **ATT&CK Tactics**

Techniques

While tactics define an attacker's goal, techniques describe the methods used to achieve those goals.

For instance, in **Persistence (TA0003)**, attackers aim to maintain access even after reboots or logon sessions. On Windows, this might involve using registry keys that execute system commands during predictable events like system start or logon. One such technique is T1547.001 - Registry Run Keys/Startup Folder. Another is T1543.003: New Service, where an attacker installs a malicious program as a system service.

Some techniques apply to more than one tactic. For instance, **T1543.003: New Service** is used in both **Persistence** and **Privilege Escalation** tactics.

ATT&CK provides details for each technique, including:

- **Applicable platforms** (for example, Windows, Linux)
- **Permissions required** to exploit the technique
- **Data sources for detection** (for example, logs)
- **References to related attack patterns** in CAPEC (a catalog of common attack patterns for application security)

Examples

ATT&CK provides real-world examples for each technique, including:

- Groups: Sets of related intrusion activities tracked under a common name (for example, APT29, FIN7)
- Software: Tools (custom or commercial) used by adversaries to conduct attacks

Each example is accompanied by references, such as blog posts and threat alerts, which help defenders understand how attackers operate and combine tactics and techniques in broader campaign.

Mitigation

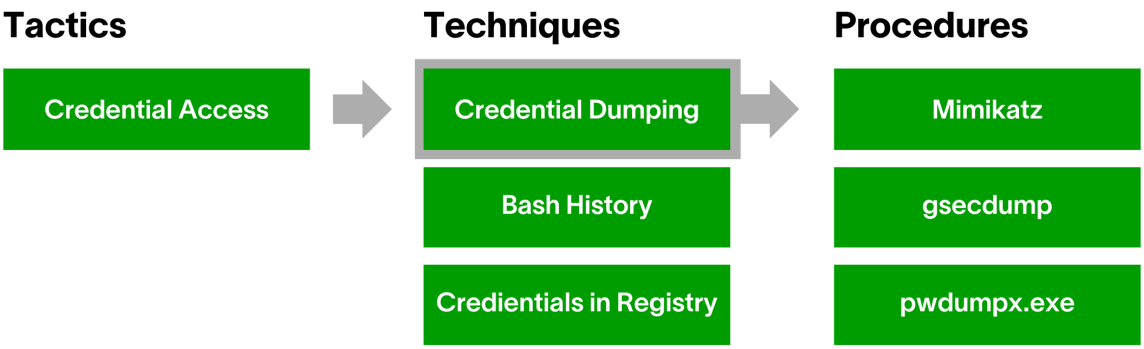
ATT&CK also suggests mitigations for each technique. Some mitigations are straightforward, while others, like T1055: Process Injection, are more complex because they exploit operating system design features.

For **T1055: Process Injection**, mitigating Windows API calls could interfere with legitimate software, including security products. The focus, therefore, should be on detecting malicious activity early in the attack chain.

While tactics define an attacker's goal, techniques describe the specific methods used to achieve that goal—offering a structured way to understand how attacks unfold and how to defend against them.

Detection

While preventing attacks is critical, detection is equally important. ATT&CK provides extensive guidance on detecting adversary techniques by leveraging logs and other security analytics. Defense-in-depth requires multiple layers of protection, and with the right detection controls, you can catch attackers in the act and minimize their impact.



MITRE ATT&CK Stays Up to Date

The threat environment constantly changes, with attackers and defenders adapting to new challenges. MITRE updates the ATT&CK framework regularly based on community input. For example, the Impact (T0040) tactic was added in 2019 to address the rise of disruptive attacks like REvil and Conti, which are notorious for targeting critical infrastructure and demanding large ransoms. The **Impact** tactic includes 14 techniques focused on reducing the availability or integrity of systems, services, or networks. Additionally, the **Reconnaissance (TA0043)** and **Resource Development (TA0042)** tactics were introduced to reflect the growing importance of the planning and preparation stages in modern cyberattacks.

Using MITRE ATT&CK

ATT&CK is a versatile tool for all roles within the cybersecurity community. For red teams, it simulates real-world adversary tactics and techniques. For blue teams, it provides a comprehensive way to understand attackers' methods and assess defenses. It also offers a standardized framework for comparing threat coverage across vendor products.

This paper focuses on ATT&CK's detective use cases, with an emphasis on security information and event management (SIEM) technology.

Assess

With many potential threats, it's impossible for any organization to cover every adversary technique across its entire network. Prioritization is essential. ATT&CK helps answer questions like:

- Which tactics are we weakest in monitoring?
- Which techniques should we focus on first?
- Which techniques lack practical preventive controls, making them more critical to detect?

Enhance

Once you identify tactics or techniques needing better detection, ATT&CK provides the technical details to help you build automated monitoring rules or support proactive threat hunts.

Test In Your Environment

Never assume that your technology or controls are fully effective. Map your detection controls to ATT&CK techniques and simulate attacks to test if your SIEM and related security technologies can detect, alert, and respond as intended.

Tools like Red Canary's Atomic Red Team are particularly useful for testing your detective controls based on the ATT&CK framework.

MITRE ATT&CK Clients

The community has developed various tools for querying ATT&CK using TAXII and STIX, such as:

- PoSh_ATTCK
- ATTACK-Python-Client
- DIY (Python with Python-Stix2 library)

These tools allow you to query the ATT&CK framework dynamically and integrate its data into your threat detection processes, helping to automate and streamline threat hunting and detection workflows.

Resources

The ATT&CK knowledge base is accessible through various tools that help you leverage its full potential:

- **MITRE ATT&CK website:** The primary platform for accessing ATT&CK content
- **ATT&CK Navigator:** A web application that allows you to explore ATT&CK content dynamically. The Navigator lets you create custom views (layers) to focus on specific techniques or adversary groups and visualize them interactively.
- **Automation tools:**
  - **TAXII Server:** A protocol for sharing cyberthreat intelligence in a scalable manner
  - **STIX:** A format for exchanging threat intelligence, with ATT&CK expressed in STIX 2.0 available for integration into your environment.

Threat Detection and Hunting With Five Common Techniques

Outcomes Navigator, part of the New-Scale Security Operations Platform, provides security teams with an interactive view of coverage strength mapped to the ATT&CK framework. Customers can compare their current threat coverage—including custom and prebuilt dashboards and report rules—against available product coverage. This helps identify gaps between existing defenses and desired security goals.

Outcomes Navigator categorizes use cases into compromised insiders, malicious insiders, and external threats.

In this section, we will:

- Explore five key ATT&CK techniques in depth:
  - **T1036.003 - Masquerading: Rename System Utilities**
  - **T1090.001 - Internal Proxy**
  - **T1048 - Exfiltration Over Alternative Protocol**
  - **T1189 - Drive-By Compromise**
  - **T1569.002 - Service Execution**
- Highlight how attackers use these techniques and how you can detect them
- Identify which logs to collect and what to look for in them
- Provide relevant tests from Atomic Red Team to help test your detection logic. You'll also see how Exabeam has implemented detection logic for these techniques in LogRhythm SIEM. Some of these detection rules depend on Microsoft Sysmon.

Masquerading: Rename System Utilities (T1036.003)

Masquerading is a **Defense Evasion (TA0005)** tactic where attackers manipulate the name or location of an executable (either legitimate or malicious) to evade detection. For example, renaming cmd.exe to lsass.exe and placing it in C:\Windows\System32\Temp makes it appear as the trusted Local Security Authority System Service (LSASS) process.

Atomic Red Team includes a test for this technique: **Masquerading: Rename System Utilities**, providing a practical way to check detection rules.

Exabeam has implemented a detection rule that identifies this variation by checking the hashes of executables in the system root against Microsoft Sysmon Event ID 1 – Process Creation using a PowerShell script:

```
get-childitem c:\windows\system32 -recurse| where {$_. extension -eq '.exe'}|Get- FileHash -Algorithm
md5|select hash|Out- File '.\hashes.txt'
```

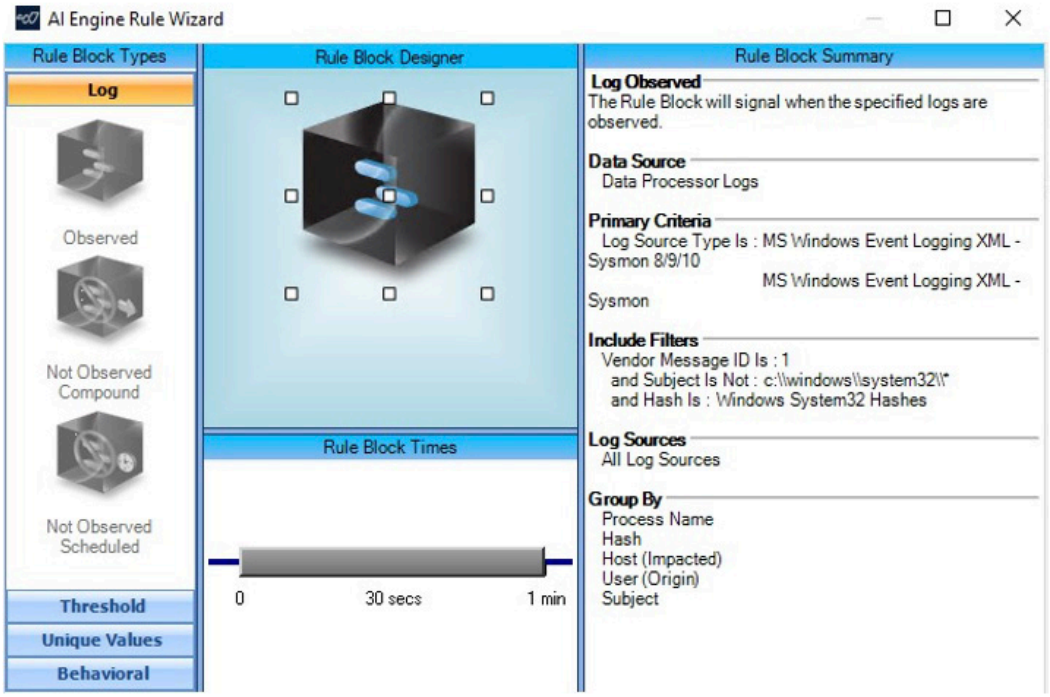


Figure 2. **AI Engine looks for Microsoft Sysmon Event ID 1: Process Creation**

Internal Proxy (T1090.001)

Internal Proxy facilitates Command and Control (TA0011) by redirecting network traffic between systems or acting as intermediaries. Tools like HTRAN, ZXProxy, and ZXPortMap are often used for this.

Atomic Red Team offers a test for **Internal Proxy**, which helps simulate proxy tool usage and validates detection of unusual network behaviors.

To detect **Internal Proxy**, ATT&CK recommends looking for processes that use the network but don't normally do so or have never been seen before. Also, examine network data for unusual patterns, such as a client sending much more data than it receives or traffic between systems that don't normally communicate.

Exabeam has built a detection rule based on Microsoft Sysmon Event ID 3 – Network Connection, looking for processes that establish inbound and outbound connections in suspicious patterns. Note that this rule depends on the entity structure being set up accurately so that the SIEM knows the directionality of the traffic.

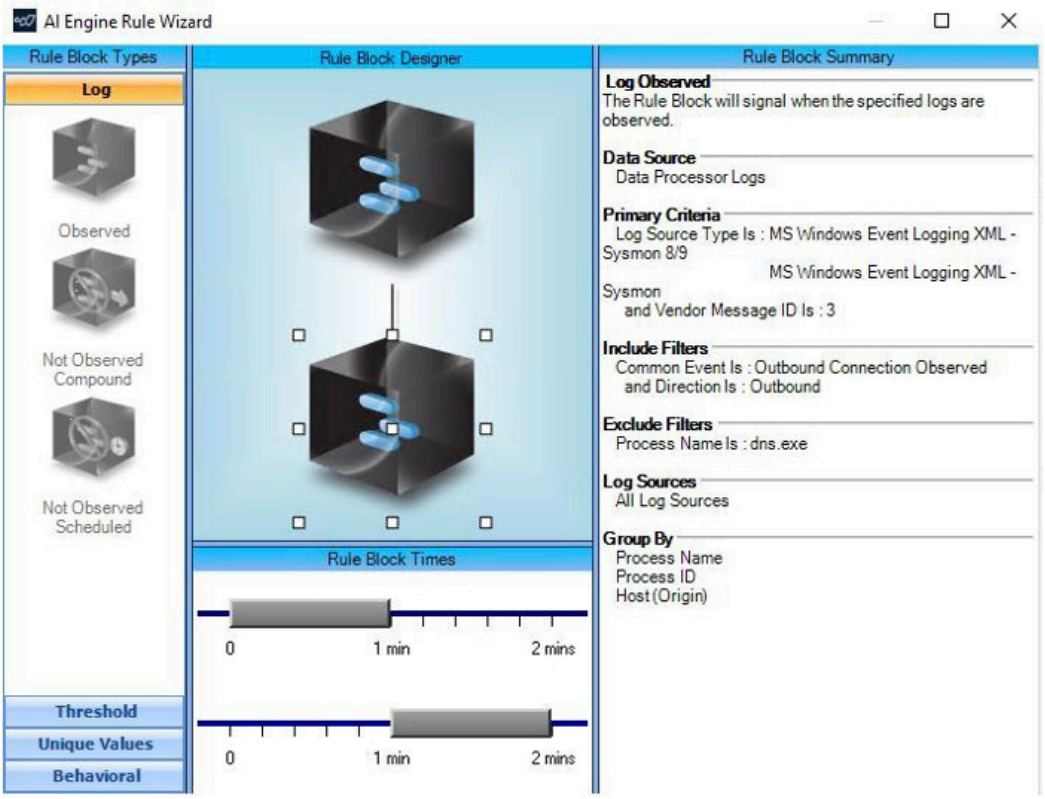


Figure 3. **Rule Block 2 of the AI Engine rule to detect the Connection Proxy technique**

Exfiltration Over Alternative Protocol (T1048)

When attackers successfully gain access to data, they need to exfiltrate it covertly. **Exfiltration Over Alternative Protocol** involves using protocols like FTP, SMTP, or HTTP/S to avoid detection.

Atomic Red Team includes a test for this technique: **Exfiltration over Alternative Protocol – SSH**, simulating data exfiltration via SSH.

To detect this technique, ATT&CK suggests analyzing network traffic for uncommon data flows, such as a client sending more data than it receives.

Exabeam developed a detection rule that uses NetMon data to track network traffic patterns and trigger alerts when applications send more data than they receive.

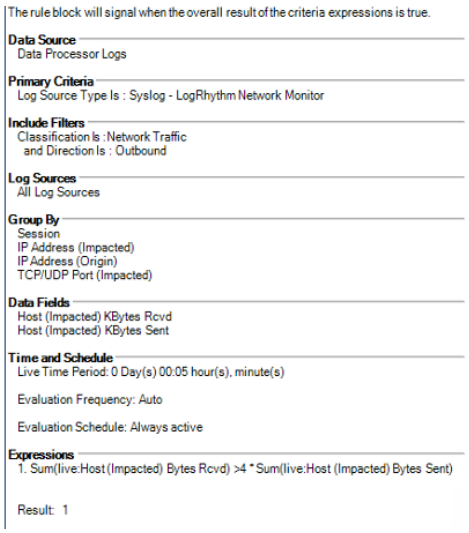


Figure 4. **AI Engine detection rule for Exfiltration Over Alternative Protocol technique**

1	Application	Host (Impacted) KBytes Rcvd	Host (Impacted) KBytes Sent	Outbound percent of Inbound
188	stickyads	3.651367188	9.385742188	39%
189	stun	122.6367188	112.5019531	109%
190	symantec	2.853515625	6.615234375	43%
191	t_mobile_app	4.754882813	306.4355469	2%
192	taboola	30.06835938	13.54296875	222%
193	tcp	539.9072266	3697.595703	15%
194	teads	6.299804688	21.07910156	30%
195	teamviewer	1.93359375	2.16796875	89%
196	telegram	2.594726563	2.05859375	126%
197	tidaltv	13.5	6.525390625	207%
198	truste	18.41210938	81.93261719	22%

Figure 5. **Analysis of outbound versus inbound traffic volume for network applications.**

Drive-By Compromise (T1189)

Drive-By Compromise occurs when attackers gain access through a user visiting a compromised website. The attack targets the browser and exploits vulnerabilities.

ATT&CK's detection guidance for this technique emphasizes the need to look for unusual behavior on the endpoint, such as abnormal browser processes or suspicious files written to disk.

Atomic Red Team includes a test for **Drive-By Compromise**, allowing you to simulate this type of web-based attack and validate detection methods.

Exabeam created a rule that correlates IDS or AV logs with browser processes saving files to the %**temp**% directory.

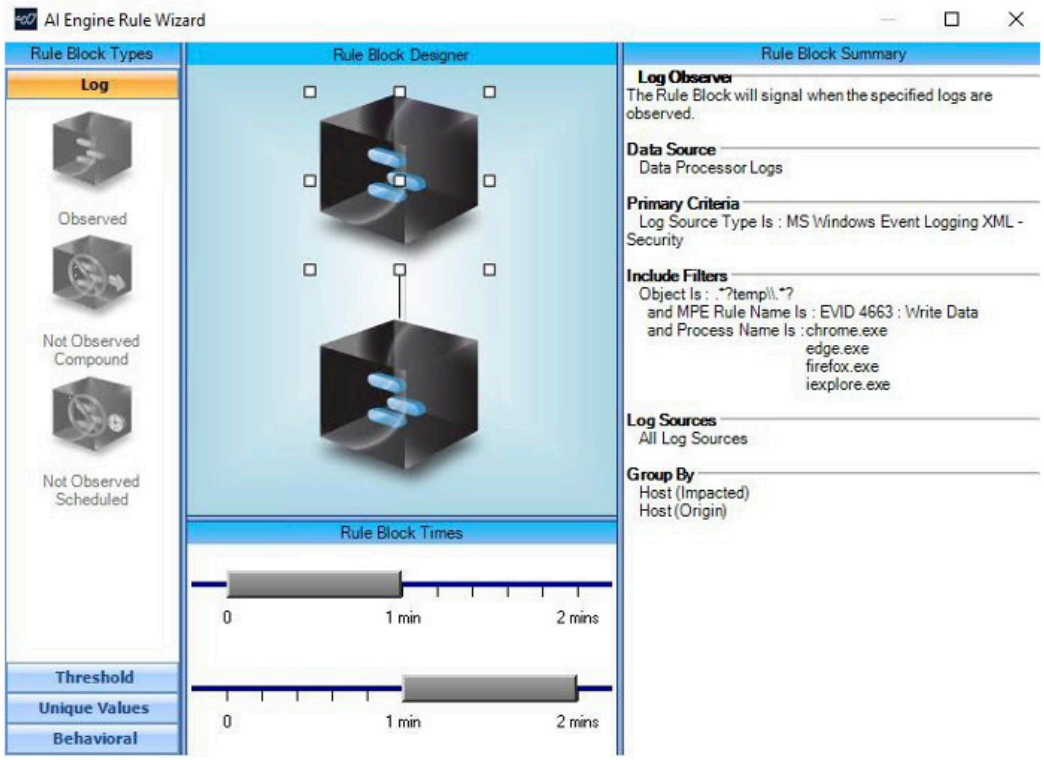


Figure 6. **Rule Block 1 of the AI Engine rule for the Drive-By Compromise attack technique**

Service Execution (T1569.002)

Service Execution is a technique where an attacker uses the Windows Service Control Manager to execute malicious code. This can be done by creating or modifying a service.

Atomic Red Team includes a test for **Execute a Command as a Service**, which simulates the execution of code by creating or modifying a service, providing a practical way to validate your detection logic.

To detect this technique, ATT&CK recommends monitoring registry changes and command-line invocations that modify services. Key events to track include:

- Event ID 4657 **(registry value modified)**, which identifies the root activity of creating or modifying a service.
- Event ID 4688 **(process start)**, which can be useful if the command line includes "sc start" or "sc create," indicating the use of the sc command to create or start a service. However, this event may not be as comprehensive as **Event ID 4657**, since attackers could bypass the sc command by directly modifying the ImagePath registry value or using the Win32Api StartService function.

You can detect this technique by enabling registry auditing of changes to the keys where services are defined (SYSTEM\CurrentControlSet\Services) and monitoring for **Event ID 4657**. Specifically, look for modifications where the affected value's name is ImagePath. This event captures the root activity of creating or modifying a service, regardless of the method used.

Additionally, Event ID 4697 **(new service installed)** is useful for tracking when a new service has been created, helping to detect **Service Execution**.

Exabeam has implemented a ruleset to detect **Service Execution**. This rule uses complex filters to encompass different log source types. It detects service installation through registry modifications, command-line invocations of services, and Windows Event ID 7045.

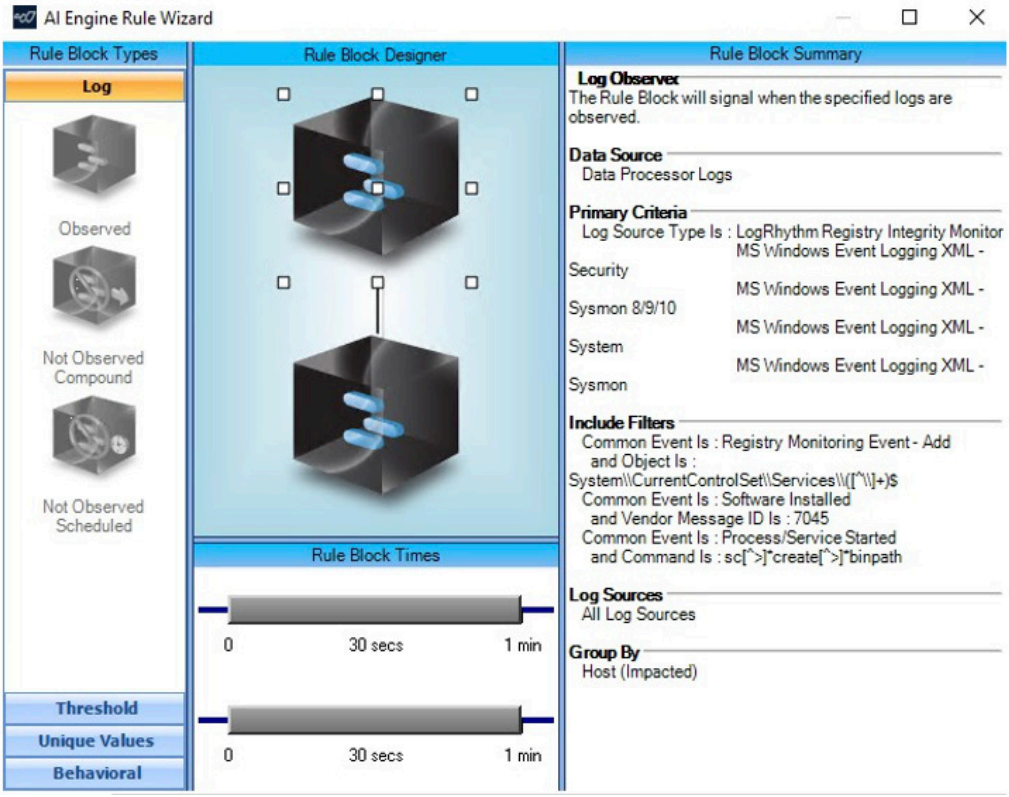


Figure 7. **Rule Block 1 of the AI Engine rule to detect the Service Execution technique**

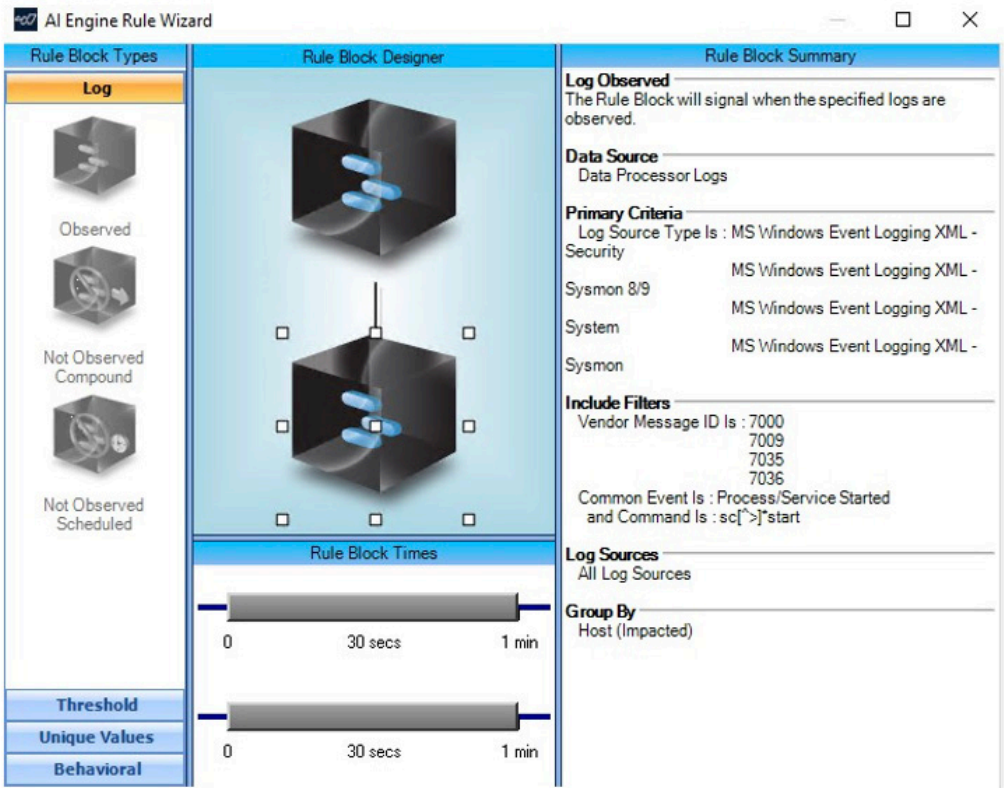


Figure 8. **Rule Block 2 of the AI Engine rule to detect the Service Execution technique**

Conclusion

ATT&CK is a powerful framework for classifying and understanding adversary techniques. It provides valuable insights into how attackers operate, enabling you to strengthen defenses and improve detection.

This paper has shown how ATT&CK enhances, analyzes, and tests your threat detection efforts, providing a structured approach to finding and closing security gaps.

Exabeam is committed to integrating ATT&CK into both our cloud-native and self-hosted SIEM platforms, ensuring you have comprehensive, up-to-date, and reliable tools for detecting and responding to emerging threats.

About Exabeam

Exabeam is a global cybersecurity leader that delivers AI-driven security operations. High-integrity data ingestion, powerful analytics, and workflow automation power the industry's most advanced self-hosted and cloud-native security operations platform for threat detection, investigation, and response (TDIR). With a history of leadership in SIEM and UEBA, and a legacy rooted in AI, Exabeam empowers global security teams to combat cyberthreats, mitigate risk, and streamline security operations.

exabeam™

Learn more at
www.exabeam.com →