exabeam

WHITE PAPER

USING THE MITRE ATT&CK KNOWLEDGE BASE TO IMPROVE THREAT HUNTING AND INCIDENT RESPONSE

SUMMARY

THREAT HUNTING AND INCIDENT RESPONSE ARE CRITICAL ROLES OF SECURITY OPERATIONS CENTER (SOC) ANALYSTS. WITH THE EVER-RISING SOPHISTICATION OF NEW AND EMERGING ATTACKS, ANALYSTS NEED AN EDGE TO STAY AHEAD OF ADVERSARIES.

Many SOC analysts seek that edge by using indicators of compromise (IoCs) for alerting and guidance. IoCs are artifacts observed on a network or in an operating system that indicate a computer intrusion with a high degree of confidence. While useful, they pose limitations that demand more contextual insight. Toward this end is a strategic enhancement called tactics, techniques and procedures (TTPs).

TTPs demonstrate adversary behavior such as what attackers are doing and how they are doing it. Behaviors revealed by TTPs are more generally applicable for developing contextual understanding across incidents, campaigns and threat actors.

To systematically achieve this understanding, enterprises and the security industry are turning to an open TTP knowledge base called MITRE ATT&CK. The knowledge base provides hundreds of scenarios grounded in empirically documented threat activity, helping guide an organization to prioritize what to address for more effective threat hunting and response. This white paper describes the MITRE ATT&CK framework, what the model offers to SOC analysts, and why you should consider using the knowledge base. It concludes by describing how Exabeam supports MITRE ATT&CK should you decide to use a modern security information and event management (SIEM) solution to leverage the model.

REFINING THE STRATEGY FOR THREAT HUNTING

With the rising complexity of attacks, today's threat detection and prevention tools are all about getting more data for analytics and insight. A popular term or category for a critical type of security data is the indicator of compromise. An IoC is an artifact observed on a network or in an operating system that indicates a computer intrusion with a high degree of confidence. Examples of IoCs include antivirus signatures, hashes, file names, IP addresses, URLs or domains.

Proponents of using IoCs are on the right track, but reliance on this type of data alone can result in a sense of false confidence at detecting all critical threats and preventing related damage. IoCs provide information about a single data point. Taken in isolation, it's difficult to interpret what they mean without additional artifacts that add context. Mitigating risks to complex IT-driven business operations requires more than a few vague clues of trouble.

Acquiring context is a big deal for security management. If an IoC pertains to a potentially rogue IP, security analysts need to know: Who is behind the IP? Are there other vectors? Is the threat targeting my industry? And so forth. Legacy SIEMs try to enrich IoCs with available tools, but they require a lot of manual effort for correlation.

IoCs also suffer the inherent vulnerability of addressing only known threats. They may provide high fidelity data and be useful in mitigating certain types of attacks. But IoCs do not address unknown threats or unusual issues developing in the early phases of a sophisticated new type of attack.

For this reason, security best practices are rapidly augmenting IoCs with a new type of security data focused on tactics, techniques and procedures. These TTPs demonstrate adversary behavior such as what attackers are doing and how they are doing it. For example, a tactic could be what is accomplished during an attack, such as achieving initial access to a network or using legitimate credentials for accessing resources. Corresponding techniques for execution of a tactic would be exploiting a public-facing application or using a brute force procedure to guess a legitimate password.

Behaviors revealed by TTPs are more generally applicable in developing contextual understanding across incidents, campaigns and threat actors. To systematically achieve this understanding, organizations are turning to a global open knowledge base called MITRE ATT&CK.

FOCUSED INSIGHT: MITRE ATT&CK KNOWLEDGE BASE

The MITRE Corporation is a not-for-profit company operating U.S. federally funded research and development centers since 1958. After starting research in 2010 to help organizations defend against advanced persistent threats (APTs), MITRE discovered that "using analytics based on a combination of host and network behaviors provides a useful way to detect post-compromise adversary behavior."[1]

Based on this research, MITRE released its ATT&CK model (short for "Adversarial Tactics, Techniques, and Common Knowledge") in 2015.

[1]MITRE, *"Finding Cyber Threats with ATT&CK-Based Analytics,"* June 2017, p. 1

MITRE ATT&CK provides an open knowledge base of adversary tactics and techniques based on real-world observations – i.e., the endpoint and network telemetry data collected 24x7 by an array of tools and usually centralized for threat hunting in a security information and event management (SIEM) platform. MITRE says the "knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community."[2]

MITRE ATT&CK is a threat-based approach for defensive and offensive purposes. The framework's TTPs are purposely "descriptive" in nature as they characterize what adversarial behavior is occurring and how the threat actors are doing it. TTPs are abstracted from specific observed instances within individual specific incidents so that they may be more generally applicable in developing contextual understanding across incidents, campaign and threat actors. Knowledge acquired from TTPs enables more effective offensive moves by an organization to mitigate advanced threats. The ATT&CK framework also helps organizations meet detection requirements for audit and security purposes. It uses a behavioral model based on five principles:[3]

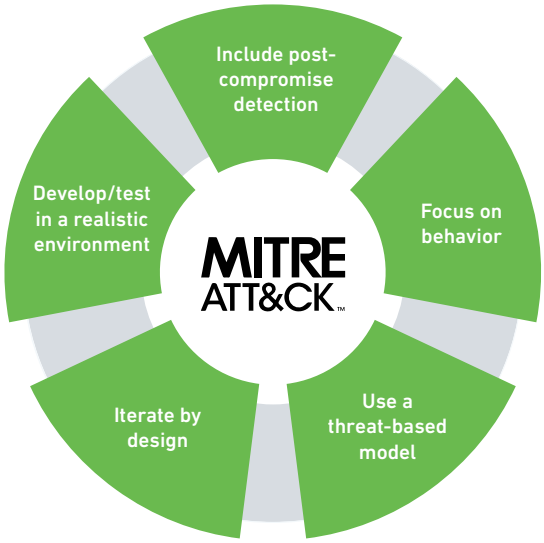
Principle 1: *Include Post-Compromise Detection* – For identifying threats that bypass established defenses or use new means to enter a network.

Principle 2: *Focus on Behavior* – Detecting and learning from post-compromise adversary behavior helps address limitations of signatures and indicators.

Principle 3: *Use a Threat-based Model* – To ensure that detection activities are effective against realistic and relevant adversary behaviors.

Principle 4: *Iterate by Design* – To account for changing adversary behavior and to understand how networks are compromised by an advanced persistent threat (APT).

Principle 5: *Develop and Test in a Realistic Environment* – Analytic development and refinement must address emulation of adversary behavior as it affects your environment.



[2]Cited on *MITRE ATT&CK home page*

[3]MITRE, *"Finding Cyber Threats with ATT&CK-Based Analytics,"* June 2017, p. 5

WHAT THE KNOWLEDGE BASE OFFERS TO SECURITY ANALYSTS

MITRE presents its knowledge base as a matrix of TTPs. The ATT&CK mapping is based on possible attack stages of the adversary. The matrix visually arranges these elements in an easy-to-understand format.

The ATT&CK matrix below shows the model's 12 Enterprise Tactics across the top in blue; these represent the attack stages beginning with "Initial Access" on the left side and proceeding to "Impact" on the right side. There are currently 266 Enterprise Techniques[4] mapped below the tactics, which are partially shown here. The assignment of techniques varies and may appear multiple times under different tactics used by an adversary.

ATT&CK MATRIX FOR ENTERPRISE

TACTICS →

TECHNIQUES ↓

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Application Access Token	Bash History	Application Window Discovery	Application Access Token	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Application Deployment Software	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	BITS Jobs	Cloud Instance Metadata API	Cloud Service Dashboard	Component Object Model and Distributed COM	Data from Cloud Storage Object	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Bypass User Account Control	Credential Dumping	Cloud Service Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	Clear Command History	Credentials from Web Browsers	Domain Trust Discovery	Internal Spearphishing	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Network Shared Drive	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Code Signing	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Removable Media	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compile After Delivery	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data Staged	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Compiled HTML File	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Email Collection	Fallback Channels	Transfer Data to Cloud Account	Network Denial of Service

[4] *MITRE Enterprise Techniques* listed as of Nov. 2019

12 ENTERPRISE TACTICS IN MITRE ATT&CK*

ID	Name	Description
TA0001	Initial Access	The adversary is trying to get into your network.
TA0002	Execution	The adversary is trying to run malicious code.
TA0003	Persistence	The adversary is trying to maintain their foothold.
TA0004	Privilege Escalation	The adversary is trying to gain higher-level permissions.
TA0005	Defense Evasion	The adversary is trying to avoid being detected.
TA0006	Credential Access	The adversary is trying to steal account names and passwords.
TA0007	Discovery	The adversary is trying to figure out your environment.
TA0008	Lateral Movement	The adversary is trying to move through your environment.
TA0009	Collection	The adversary is trying to gather data of interest to their goal.
TA0011	Command and Control	The adversary is trying to communicate with compromised systems to control them.
TA0010	Exfiltration	The adversary is trying to steal data.
TA0040	Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.

*Descriptions of a tactic's respective techniques are listed at *https://attack.mitre.org/tactics/enterprise/*

ATT&CK specifies common knowledge and procedures for each of the model's techniques. Elements for each technique include a description, examples of how the technique can be implemented (including adversaries such as individuals and groups, and software tools), advice on how to mitigate the technique, and advice on how to detect the technique. This information about adversaries and software is a work in progress so analysts must remain alert for variations in how techniques could be applied to various tactics.

By systematically categorizing real-world attack behavior, MITRE ATT&CK provides a concrete tool for helping security analysts and other stakeholders create more effective strategies and processes to detect, investigate and respond to known, new and emerging attacks.

CASE STUDY: PREVENTING THE CAPITAL ONE DATA BREACH

Incident: Theft of personally identifiable data for 106 million customers of Capital One Financial Corp. in March 2019.

What happened: Attacker exploited a vulnerability in a web application firewall running in an Amazon AWS instance that was used by Capital One. The exploit allowed the attacker to acquire administrative credentials, access Amazon's metadata service and exfiltrate data, first to a local drive and then to a cloud service.

How MITRE ATT&CK and Exabeam could have helped: Capital One was not using either MITRE ATT&CK or Exabeam Advanced Analytics. The integrated capabilities of these solutions could have prevented this incident in several ways.[5]

- *Detecting the attack.* Each step in the Capital One attack kill chain was clearly defined in the ATT&CK framework. These included 11 techniques that are supported by the Exabeam Security Management Platform (SMP). Each of these techniques is an opportunity for detection.
- *Interpreting behavior.* Exabeam Advanced Analytics preprocesses all logs and combines them with other data sources to baseline normal user and asset activities. Unlike other vendors, Exabeam only alerts on MITRE ATT&CK techniques, such as those associated with the Capital One attack, when they are identified as anomalous behavior.
- *Investigation.* Advanced Analytics correlates all the events (normal and abnormal) and presents them in a chronological order to make it very easy for analysts to gain visibility into the timeline of an attack. Exabeam Smart Timelines provides analysts with the new method of incident investigation – requiring no prior knowledge of an attacker's tactics and techniques.

[5]For technical details, see Pramod Borkar and Shubham Goel's article, *"A Look at the Capital One Data Breach Through the Lens of MITRE ATT&CK,"* 23 Aug. 2019.

WHY YOU SHOULD CONSIDER USING MITRE ATT&CK

With an ever-growing sophistication in attacks, enterprise SOCs are expressing more interest in using the MITRE ATT&CK model to improve their abilities to detect, investigate and respond to adversaries.[6] As a reflection of this interest and a result of collaborative contributions to the MITRE ATT&CK effort, the size of the MITRE ATT&CK knowledge base is growing too. Since 2016, the knowledge base has more than doubled from 100 enterprise techniques to 266 as of November 2019.[7]

Strategic use of the MITRE ATT&CK model provides evidence-grounded guidance for helping SOC analysts keep their organizations more secure. MITRE ATT&CK is useful to SOCs because it's focused on the last part of the attack cycle, which applies to their roles for detection, investigation and response. Other frameworks exist. One example is the Lockheed Martin Cyber Kill Chain, which addresses earlier phases beginning with reconnaissance by adversaries. This model is more theoretical because it is not based on actual experience. As a fixed model, it does not provide an evolutionary path for evolving threats. It also has less granularity in the attack chain tactics than those defined by MITRE. MITRE ATT&CK delineates the techniques that can be used at each stage while the Lockheed Martin Cyber Kill Chain does not. The illustration shows where MITRE ATT&CK relates to that model.

MITRE ATT&CK USE CASES

Adversary Emulation – Create adversary emulation scenarios to test and verify defenses against common adversary techniques.

Red Teaming – Create red team plans and organize operations to avoid certain defensive measures that may be in place within a network.

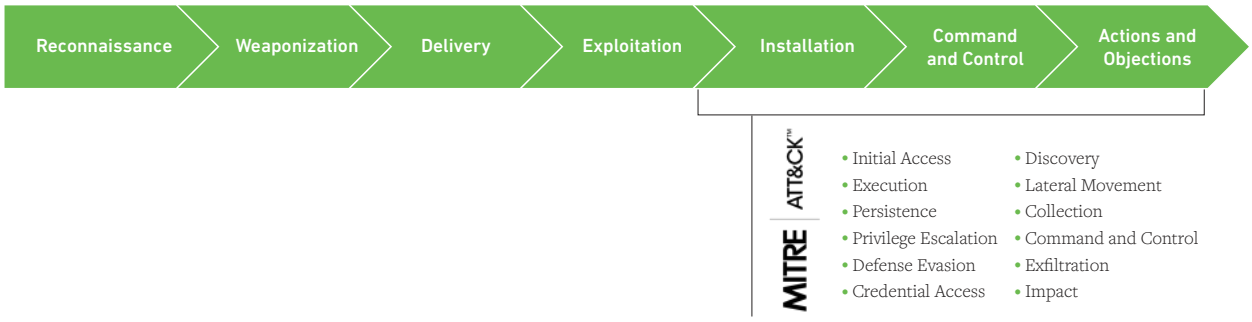
Behavioral Analytics Development – Construct and test behavioral analytics models to detect adversarial behavior within an environment.

Defensive Gap Assessment – Provide a common behavior-based adversary model to assess tools, monitoring and mitigations of existing defenses within an organization's enterprise.

SOC Maturity Assessment – Determine how effective a SOC is at detecting, analyzing and responding to intrusions.

Cyber Threat Intelligence Enrichment – Understand and document adversary group profiles from a behavioral perspective that is agnostic of the tools a group may use.

LOCKHEED MARTIN CYBER KILL CHAIN



[6]Based on Google search data, interest in MITRE ATT&CK spiked higher in Oct. 2018 and is higher today. [7]See *https://attack.mitre.org/matrices/enterprise/*

USING EXABEAM SMP WITH MITRE ATT&CK

Exabeam SMP leverages the MITRE ATT&CK framework to improve how SOC teams detect, investigate and respond to attacks.

Exabeam SMP tells you which incidents to prioritize, converting "signal from noise" to identify risky behaviors. For the MITRE ATT&CK model, Exabeam SMP currently monitors and analyzes 51 techniques across all 12 tactics.

To illustrate one integration, consider the MITRE ATT&CK technique, *Pass the Hash* (T1075). This exploit re-uses a stolen (and uncracked) hashed user credential to trick an authentication system into creating a new authenticated session on the same network. The technique frequently is used to move laterally in a network in search of sensitive data and assets. Perhaps the attack began by compromising a low-level employee account. Once inside, the hacker probes other assets for vulnerabilities in order to switch accounts, machines and IP addresses. Opportunity knocks once the attacker secures administrative privileges.

Lateral movement is extremely difficult to detect using legacy security tools because parts of the attack are scattered across the IT environment, spread among different credentials, IP addresses and machines; the seemingly unrelated events all appear to be normal. Exabeam SMP is able to detect a Pass the Hash attack by auditing all logon and credential use events and reviewing for discrepancies. Unusual remote logins that correlate with other suspicious activity (such as writing and executing binaries) may indicate suspicious activity. These are elevated to SOC analysts for investigation.

Exabeam SMP also appends MITRE ATT&CK tactic and technique labels to events to speed investigations. For organizations using MITRE ATT&CK, the mappings in Exabeam SMP offer both a common taxonomy for security analysts to label adversary behavior and enable improved collaboration. Exabeam also enables security analysts to view and filter MITRE ATT&CK techniques within Smart Timelines, which are machine-created timelines that sequence events into plainly worded narratives. Smart Timelines allow security teams to easily investigate event details with minimal technical expertise and without querying multiple systems. Analysts can mouse over event labels for MITRE techniques for a pop-up description or click on labels to open the MITRE webpage for a detailed description.

Searches for MITRE ATT&CK tactics and techniques are also integrated with Exabeam Threat Hunter. Analysts can search for attacker techniques across users and devices using drop-down menus and a point-and-click interface uniquely provided by Exabeam. The integration replaces the need for complex queries in legacy SIEMs.

Exabeam continues to add new analytic models mapped to MITRE ATT&CK techniques. Its researchers also contribute new techniques to MITRE for consideration as additions to the framework. The MITRE Corporation has accepted Exabeam's submission of new MITRE techniques: *Domain Generation Algorithms* (T1483) and *Credentials from Web Browsers* (T1503), making Exabeam the first and only SIEM provider to have a technique submission accepted to the knowledge base. Contributions like these provide benefits to the entire security industry.

exabeam

TO LEARN MORE ABOUT HOW EXABEAM CAN HELP YOU, VISIT **EXABEAM.COM** TODAY.

SUMMARY

As the cadence and complexity of attacks continue to rise, SOC analysts more than ever need a reliable edge for effective threat hunting and incident response. The MITRE ATT&CK framework provides that edge with data-proven tactics, techniques and procedures for detection and mitigation of security incidents. The framework becomes especially useful and practical when integrated with a modern SIEM to provide a centralized enterprise hub for data analytics and automatic correlation as part of SOC analysts' workflows. Exabeam SMP integrates MITRE ATT&CK's TTPs with advanced behavioral analytics to automate the detection of security incidents, hunt threats and quickly respond for mitigation. We invite you to consider a demonstration of how these capabilities can be used in your enterprise SOC. To schedule a demonstration, please visit *exabeam.com/demo.*

ABOUT EXABEAM

Exabeam is the Smarter SIEM™ company. We help security operations and insider threat teams work smarter, allowing them to detect, investigate and respond to cyberattacks in 51 percent less time. Security organizations no longer have to live with excessive logging fees, missed distributed attacks and unknown threats, or manual investigations and remediation. With the modular Exabeam Security Management Platform, analysts can collect unlimited log data, use behavioral analytics to detect attacks, and automate incident response, both on-premises or in the cloud. Exabeam Smart Timelines, sequences of user and device behavior created using machine learning, further reduce the time and specialization required to detect attacker tactics, techniques and procedures. For more information, visit *https://exabeam.com.*