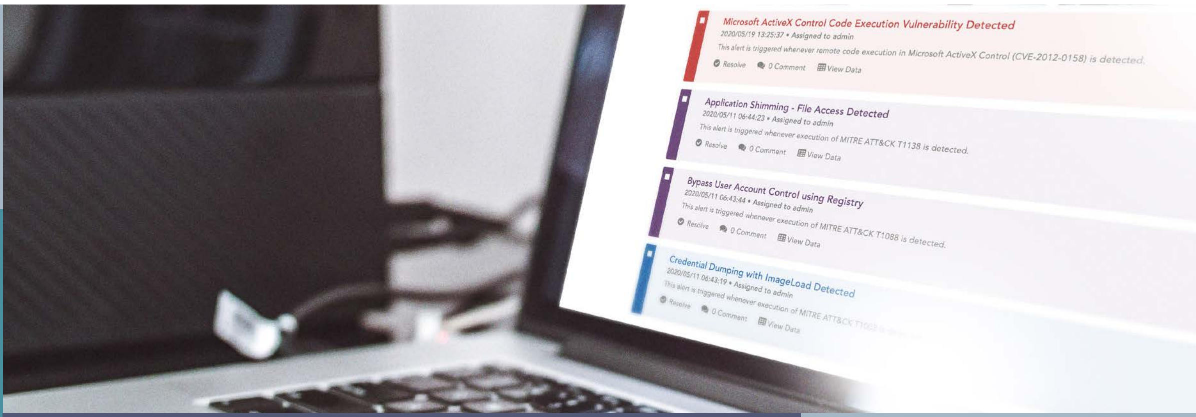
LOGPOINT


Microsoft ActiveX Control Code Execution Vulnerability Detected
2020/05/19 13:25:37 • Assigned to admin
This alert is triggered whenever remote code execution in Microsoft ActiveX Control (CVE-2012-0158) is detected.
Resolve 0 Comment View Data

Application Shimming - File Access Detected
2020/05/11 06:44:23 • Assigned to admin
This alert is triggered whenever execution of MITRE ATT&CK T1138 is detected.
Resolve 0 Comment View Data

Bypass User Account Control using Registry
2020/05/11 06:43:44 • Assigned to admin
This alert is triggered whenever execution of MITRE ATT&CK T1088 is detected.
Resolve 0 Comment View Data

Credential Dumping with ImageLoad Detected
2020/05/11 06:43:19 • Assigned to admin
This alert is triggered whenever execution of MITRE ATT&CK T1003
Resolve 0 Comment View Data

How LogPoint uses MITRE ATT&CK®

Technical white paper

Threat actors and cyberattacks are continually evolving and becoming more sophisticated. It becomes more critical than ever for organizations to map their defense systems and identify gaps in the security posture. Using MITRE ATT&CK, a standard framework that classifies adversary behaviors, organizations can identify holes in defenses and prioritize them based on risk.

The intuitive framework provides intelligence about cybersecurity threats and is a useful tool for all organizations.

Introduction

This white paper will describe a brief history, functionality and utility of the MITRE ATT&CK framework and how it fits into the modern enterprise security environment. The white paper will also provide information about how, why and to what extent the ATT&CK framework is implemented in LogPoint security information and event management (SIEM) and user entity and behavior analytics (UEBA) products.

An overview of MITRE ATT&CK

Within the last decade, it quickly became apparent to the broader cybersecurity community that cybersecurity organizations needed to increase collaboration to strengthen defense efforts[1]. If defense efforts fell short, attackers were likely to gain the upper hand. The MITRE Corporation is a result of the realization that collaboration within the cybersecurity community is the foundation of a robust defense. As a non-profit, MITRE has a goal to improve security posture across the entire ecosystem. Its most notable efforts focus primarily on the classification of threats.

The ATT&CK framework is what many consider MITRE's flagship product. ATT&CK is a collection of adversarial technique descriptions, which aims to unify existing attack methods across the industry. The tactics and techniques are independent of either the specific adversary or the business the adversary is attacking. Typically presented as a table with columns for each consecutive attack stage, the ATT&CK framework contains every single known tactic used to breach an organization perimeter. Each tactic has an assigned ID, which acts as a unique identifier to help document the techniques.

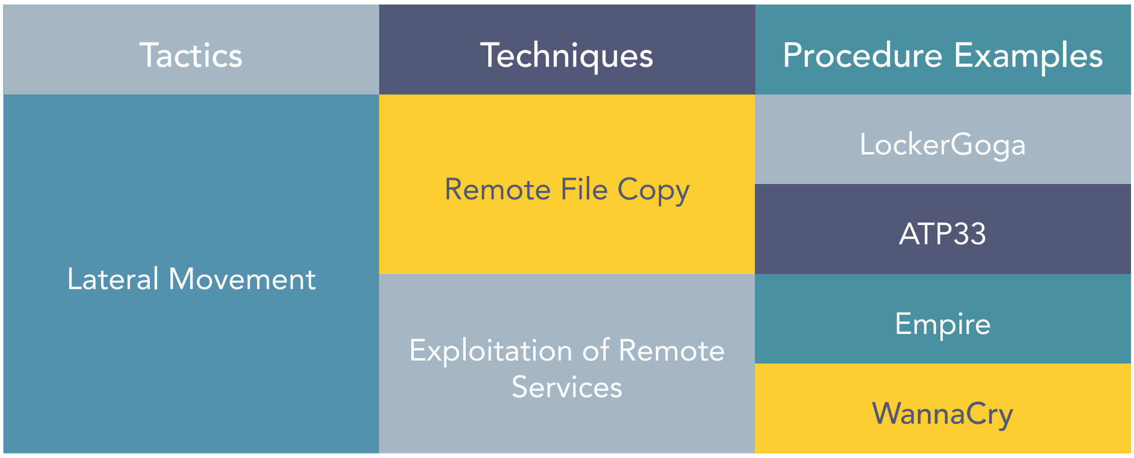
MITRE ATT&CK in short

MITRE ATT&CK is framework of cyber threat actor tactics and techniques to understand threat actor behavior and how they carry out attacks.

What is a tactic?
Tactics are threat actors' high-level objectives or goals.

What is a technique?
Techniques are the specific technical methods threat actors use to achieve their goals (tactics).

[1] Skopik, Florian, et al. "A Problem Shared Is a Problem Halved: A Survey on the Dimensions of Collective Cyber Defense through Security Information Sharing." Computers & Security, vol. 60, 2016, pp. 154–176.



Tactics	Techniques	Procedure Examples
Lateral Movement	Remote File Copy	LockerGoga
		ATP33
	Exploitation of Remote Services	Empire
		WannaCry

Illustration of MITRE ATT&CK tactics, techniques and procedure examples.

How the ATT&CK framework helps

It's not uncommon for companies to mainly see cybersecurity as a way to prevent attackers from breaching their networks. However, with the increased sophistication of cyberattacks[2] , companies need to recognize that attackers can circumvent even the best security controls and policies.

Once adversaries have access to the network, it's pertinent to stop them as soon as possible to reduce the damage. Many security professionals are using the ATT&CK framework as a way to understand and predict adversary attack methods. Here are some of the most beneficial ways security teams can use the ATT&CK framework.

Incident response

Incident response is a primary way to use the framework for several reasons. ATT&CK increases security teams' ability to predict offensive activity. For example, if a malicious or unsanctioned activity falls into the Discovery tactic category, organizations can accurately predict the next step of the attack because the ATT&CK framework is sequential. When security teams can predict offensive behavior, it's easy to take remediation measures. Security teams don't even need precise knowledge of the specific technique. It is often enough to know, for example, if the attacker is about to start the Discovery tactic phase in order to secure the corresponding resources.

Security teams can predict even more information about an attack if threat intelligence is available. For example, incident response teams can get an early lead on protecting against an attack if they know a set of techniques correlates with those of

[2] Information Security Forum: Threat Horizon 2019 report, p. 8

a known threat group. Even IT employees who use the framework can get a much better picture of ongoing threat activity until a dedicated individual or team is assigned.

The documentation aspect is also highly relevant. Inidividuals without specialized education in security can help protect against a cyberattack if they can determine the ATT&CK IDs of the detected abnormal activity. The framework is a remarkable tool to provide a common taxonomy for attacks across all disciplines.

In addition to ATT&CK, automation can also help less-skilled security analysts respond to incidents. Incidents are not necessarily catastrophic occurrences. Most incidents are minor and not particularly relevant. The ability to log and automatically categorize a large number of minor incidents helps speed up the response. Furthermore, the ability to auto-remediate incidents and exchange data with other products is extremely valuable, especially when dealing with the current shortage of security analysts[3] who are sufficiently equipped to deal with anomaly analysis in its full volume.

Security analysis

Security analysis is arguably the most dynamic field within security. Most security analysts believe that they need to actively monitor the entire environment and that passive preventative measures are not sufficient to secure perimeters. Given that analysis requires human expertise and active monitoring, staffing and retaining security analysts is expensive[4].

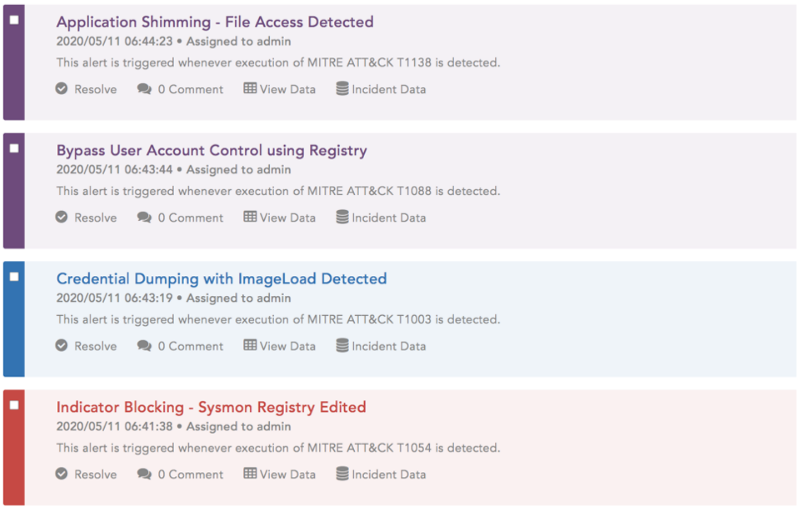
ATT&CK can make analysis quicker. For example, an analyst might prioritize the use of late-stage tactics and techniques as a signal of higher criticality. Or perhaps analysts know based on experience that early-stage attacks are relatively common, but they are not often critical, so analysts can de-prioritize them.

Cost and cybersecurity skill level are common concerns when hiring security operations center (SOC) personnel. It's a massive benefit that anyone who has a baseline understanding

To help reduce costs, analysts can speed up their tasks by classifying alerts based on the ATT&CK framework.

[3] (ISC)² and Center for Cyber Safety and Education: 2017 Global Information Security Workfoce Study, p. 2-3

[4] SACA: 2020 State of Cybersecurity report, part one


Application Shimming - File Access Detected
2020/05/11 06:44:23 • Assigned to admin
This alert is triggered whenever execution of MITRE ATT&CK T1138 is detected.

Bypass User Account Control using Registry
2020/05/11 06:43:44 • Assigned to admin
This alert is triggered whenever execution of MITRE ATT&CK T1088 is detected.

Credential Dumping with ImageLoad Detected
2020/05/11 06:43:19 • Assigned to admin
This alert is triggered whenever execution of MITRE ATT&CK T1003 is detected.

Indicator Blocking - Sysmon Registry Edited
2020/05/11 06:41:38 • Assigned to admin
This alert is triggered whenever execution of MITRE ATT&CK T1054 is detected.

The ATT&CK framework gives threat hunters information about the stage of the attack, so they know how to respond and can predict what will happen next.

of IT can easily understand the main concepts of the framework. The simplicity of the framework relieves the pressure of SOCs to find the most skilled analysts for the lowest price.

The ATT&CK framework also makes it easier for analysts to convey information to each other regularly. Knowledge sharing is a significant element of all security efforts, whether they are internal or inter-organizational. Teams that file alerts using a standard taxonomy are easier to analyze, parse and verify. ATT&CK also provides a much better tactical overview for a relatively minor investment. Improving analyst collaboration has been one of the main elements where LogPoint implemented the ATT&CK framework, which will be discussed later.

Threat hunting

Threat hunting requires an additional skillset compared to analytics. Deductive reasoning is not sufficient. During an investigation, threat hunters need to use abductive and inductive reasoning in the pursuit of possible leads. At the same time, threat hunters shouldn't be frivolous with assigning malice and abnormality to network activity. ATT&CK shines in threat hunting. The framework allows the hunter to base his actions around concrete tactics rather than doing guesswork.

Using the framework, the hunter can determine the stage of the attack and confirm whether the attack exists in the first place. Knowing what to look for saves time and effort. ATT&CK can also help with compliance. In threat hunting, there needs to be a constant feedback and documentation loop to maintain compliance. Hunters need to verify their findings and maintain accountability for all individuals involved in the investigation. Documents and records can also assist in remediation. A formalized framework like ATT&CK means professionals across the field can understand records.

Threat intelligence

In one sense, the fact that ATT&CK helps document information about security threats is already an asset relating to threat intelligence. However, the framework has more profound benefits for threat intelligence.

The framework represents the very lifecycle of a threat. Regardless of if the threat is an advanced persistent threat (APT), a criminal effort or anything else, the threat fits on the framework.

Once security teams apply the threat to the framework, it is easy to communicate.

ATT&CK simplifies the stages of an attack, which has led to a significant, emerging trend. Companies have been developing software, rules, shareable security knowledge and intelligence content around the framework. SIEM rules are one relevant example of the pattern of aligning with ATT&CK.

Strategy and gap analysis

Companies can translate their security posture between its higher and lower representations using the ATT&CK framework. It's much easier, for example, to represent gaps in the security posture of an organization using the framework as opposed to traditional approaches. The framework provides a much better set of instructions for security personnel while also maintaining the simplicity to inform higher management. In fact, a large number of security consulting organizations and managed security service providers (MSSPs) are already using the framework.

ATT&CK is also a convenient tool for evaluating various services, from simple antiviruses to active security monitoring services, both as a customer and as a provider. ATT&CK removes the ambiguity of marketing and broad claims and instead provides a set of easily understandable categories.

Finally, ATT&CK is beneficial when it comes to planning. An advantage of having the framework at hand is knowing what stages are the most threatening to any given organization. Using the sequential nature of the framework matrix as a guide, companies can allocate the budget based on which items in it are the most affected. For example, if security teams know that the Privilege Escalation tactic stage of the framework has the fewest covered techniques in their security defense, they have a solid argument for more budget. There are also plenty of resources available free of charge for this very purpose.

Red Team applications

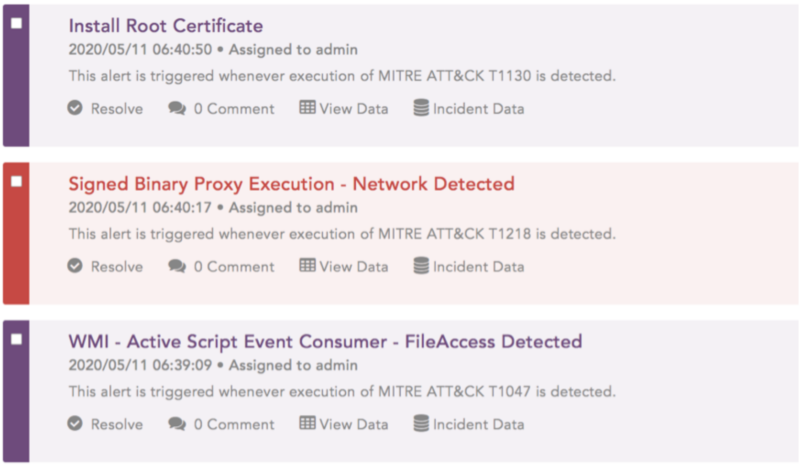
Although ATT&CK is mainly useful for Blue Teams, or the defensive side of security, it can also serve as a way to implement Red Team or real-world attack scenarios. The framework is perhaps not as advantageous to a hacker as, for example, a regular kill chain style guide, but there are some cases where using ATT&CK is more appropriate.

Tabletop exercises are well-suited for the framework. Red Teams can use ATT&CK in all aspects of tabletop exercises, from gamified awareness training to actual full-on war room scenarios, such as incident simulation. ATT&CK brings not only a high degree of realism but easy-to-learn, relatable instruction on exactly what to expect from modern threat actors.

Various complex frameworks for Red Teams also incorporate the ATT&CK framework as a building block.

The benefit of ATT&CK in a nutshell

Overall, the fundamental advantage of the ATT&CK framework is the increased speed of information transfer. When information is shared quickly, it leads to a better, faster and a more efficient observe-orient-decide-act (OODA) loop for the collective security ecosystem. Cybersecurity is concerned with systems and information, so fast knowledge sharing is a crucial advantage. Adversaries are increasingly capable of using scalable and collectivized solutions to achieve their objectives, so security organizations need to be able to share information to stay ahead.



Install Root Certificate
2020/05/11 06:40:50 • Assigned to admin
This alert is triggered whenever execution of MITRE ATT&CK T1130 is detected.

Signed Binary Proxy Execution - Network Detected
2020/05/11 06:40:17 • Assigned to admin
This alert is triggered whenever execution of MITRE ATT&CK T1218 is detected.

WMI - Active Script Event Consumer - FileAccess Detected
2020/05/11 06:39:09 • Assigned to admin
This alert is triggered whenever execution of MITRE ATT&CK T1047 is detected.

In LogPoint, every alert has an ATT&CK ID, making it easy for analysts to combine different alerts as part of one established attack sequence.

Future developments

MITRE is continually updating ATT&CK, and because it is fully open source, the framework is immensely valuable for individuals, enterprises and the broader security community. An important new feature from MITRE is pre-ATT&CK, which focuses on the preliminary steps of attacking an enterprise. Pre-ATT&CK is useful mostly for intelligence reasons, but it touches upon almost every other category within defensive cybersecurity.

LogPoint and the ATT&CK framework

We're developing LogPoint's security features, so they fully support the framework. When we talk about LogPoint as a security solution, we're primarily referencing the ATT&CK framework. The following sections discuss the different way LogPoint has implemented ATT&CK in its security solutions.

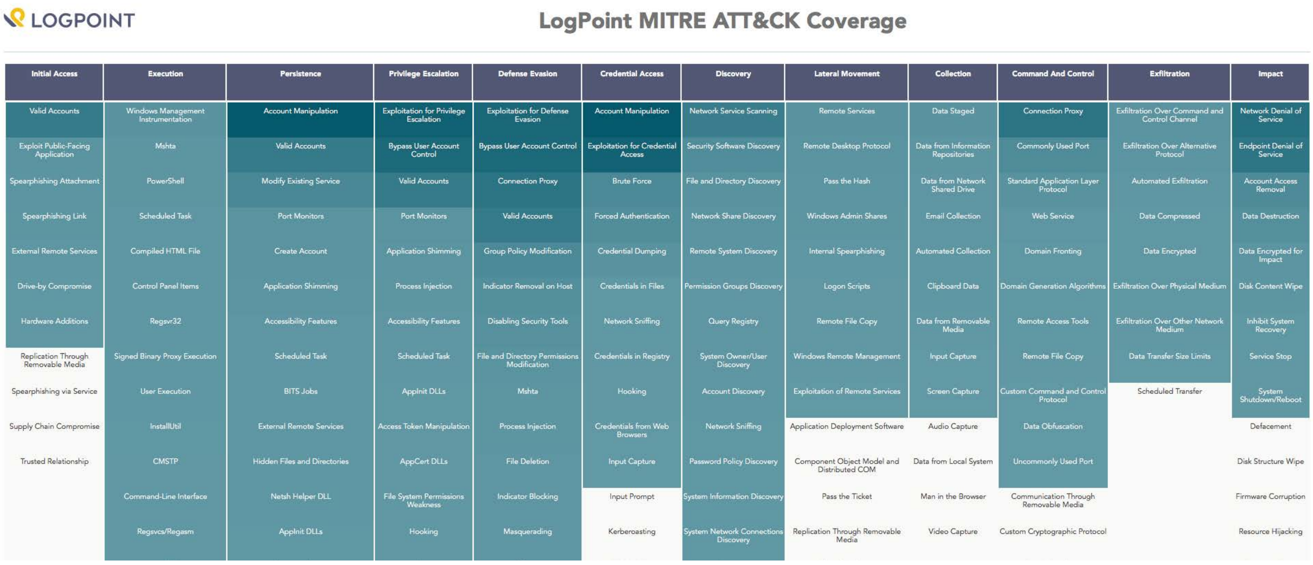
ATT&CK as a foundation in LogPoint

LogPoint maps all of its basic queries to the ATT&CK framework. Mapping queries means that when a customer uses LogPoint, they should be able to know, with a small margin of ambiguity, that there is a set of ATT&CK use cases that are covered out-of-the-box if they enable all of the alert rules. Some additional configuration may be required, but that goes for all SIEM soltuions.

ATT&CK is also relevant for LogPoint rules. Every single enabled alert rule will return an alert that already has its ATT&CK ID attached. The ID makes it easy for an analyst to see whether the disparate alerts are matching with a single attack that is following the established sequence.

Full transparency of ATT&CK and LogPoint

Many SIEM providers offer a particular coverage of the framework, but few are



LOGPOINT

LogPoint MITRE ATT&CK Coverage

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
Valid Accounts	Windows Management Instrumentation	Account Manipulation	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Account Manipulation	Network Service Scanning	Remote Services	Data Staged	Connection Proxy	Exfiltration Over Command and Control Channel	Network Denial of Service
Exploit Public-Facing Application	Mshta	Valid Accounts	Bypass User Account Control	Bypass User Account Control	Exploitation for Credential Access	Security Software Discovery	Remote Desktop Protocol	Data from Information Repositories	Commonly Used Port	Exfiltration Over Alternative Protocol	Endpoint Denial of Service
Spearphishing Attachment	PowerShell	Modify Existing Service	Valid Accounts	Connection Proxy	Brute Force	File and Directory Discovery	Pass the Hash	Data from Network Shared Drive	Standard Application Layer Protocol	Automated Exfiltration	Account Access Removal
Spearphishing Link	Scheduled Task	Port Monitors	Port Monitors	Valid Accounts	Forced Authentication	Network Share Discovery	Windows Admin Shares	Email Collection	Web Service	Data Compressed	Data Destruction
External Remote Services	Compiled HTML File	Create Account	Application Shimming	Group Policy Modification	Credential Dumping	Remote System Discovery	Internal Spearphishing	Automated Collection	Domain Fronting	Data Encrypted	Data Encrypted for Impact
Drive-by Compromise	Control Panel Items	Application Shimming	Process Injection	Indicator Removal on Host	Credentials in Files	Permission Groups Discovery	Logon Scripts	Clipboard Data	Domain Generation Algorithms	Exfiltration Over Physical Medium	Disk Content Wipe
Hardware Additions	Regsvr32	Accessibility Features	Accessibility Features	Disabling Security Tools	Network Sniffing	Query Registry	Remote File Copy	Data from Removable Media	Remote Access Tools	Exfiltration Over Other Network Medium	Inhibit System Recovery
Replication Through Removable Media	Signed Binary Proxy Execution	Scheduled Task	Scheduled Task	File and Directory Permissions Modification	Credentials in Registry	System Owner/User Discovery	Windows Remote Management	Input Capture	Remote File Copy	Data Transfer Size Limits	Service Stop
Spearphishing via Service	User Execution	BITS Jobs	AppInit DLLs	Mshta	Hooking	Account Discovery	Exploitation of Remote Services	Screen Capture	Custom Command and Control Protocol	Scheduled Transfer	System Shutdown/Reboot
Supply Chain Compromise	InstallUtil	External Remote Services	Access Token Manipulation	Process Injection	Credentials from Web Browsers	Network Sniffing	Application Deployment Software	Audio Capture	Data Obfuscation		Defacement
Trusted Relationship	CMSTP	Hidden Files and Directories	AppCert DLLs	File Deletion	Input Capture	Password Policy Discovery	Component Object Model and Distributed COM	Data from Local System	Uncommonly Used Port		Disk Structure Wipe
	Command-Line Interface	Netsh Helper DLL	File System Permissions Weakness	Indicator Blocking	Input Prompt	System Information Discovery	Pass the Ticket	Man in the Browser	Communication Through Removable Media		Firmware Corruption
	Regsvcs/Regasm	AppInit DLLs	Hooking	Masquerading	Kerberoasting	System Network Connections Discovery	Replication Through Removable Media	Video Capture	Custom Cryptographic Protocol		Resource Hijacking

The LogPoint ATT&CK navigator provides more information about the tactics and techniques and indicates which are covered by LogPoint SIEM and UEBA. The navigator is available on the LogPoint website: www.logpoint.com/mitre.

capable of putting a specific number on the use cases covered. It's easier to get a complete picture of the actual value of the SIEM solution when the number of use cases covered by AT&CK is transparent.

Before companies buy LogPoint, they can see the extent of use cases covered by ATT&CK, which helps plan the security budget, make purchasing decisions and determine project/ program workload. LogPoint strives to maintain full transparency when it comes to security coverage to ensure companies choose the best SIEM solution for their needs. All LogPoint data relating to the ATT&CK framework is fully available on the public website.

UEBA

LogPoint UEBA represents the entire spectrum of the ATT&CK framework. The technology behind UEBA enables us to perfectly match the detection capability with the tactical methods in the framework. Instead of rigid queries, searches or other data constructs that typically come together with a SIEM, LogPoint UEBA matches the machine learning algorithms to actual practical scenarios rather than non-cohesive, singular items of interest. UEBA covers a significant part of the framework, which is visible on our public ATT&CK navigator, and we intend to base UEBA around ATT&CK entirely.

Future development

LogPoint SIEM is in a significant transition state. New technologies are one of the main focuses of our development effort. We are looking toward the future of cybersecurity and implementing innovative features to support future trends. We are also challenging the notion that implementing various security frameworks and standards in a SIEM product boils down to deploying several new data structures, such as queries/searches or reports.

Introducing new data structures is insufficient. We are aware of the fact that community efforts, such as ATT&CK, are crucial now and in the future. In an environment where threats increasingly evolve to affect more substantial strata of organizations and companies no longer feel that secrecy around threat intelligence benefits their business model, we see a genuine opportunity for collective effort.

The ATT&CK framework is central to LogPoint. We use research from outside sources to inform every development and improvement of the products. We will continually survey the product to ensure all areas of the framework are covered and determine which areas need an update. If we find that an area, such as the Discovery tactic, needs more coverage in LogPoint, we will allocate development effort to that area.

Our agile approach to development means we can also adapt to the changing cybersecurity market. If we see a spike in some form of threat, such as ransomware, we will research and analyze the relevant intelligence. Then we will immediately restructure development efforts around the items in the framework to address the particular ransomware.

Additionally, as MITRE undertakes new research, we will accordingly analyze and adjust the capabilities of our products. As mentioned, a new feature for MITRE is the pre-ATT&CK framework. The implementation of pre-ATT&CK in LogPoint is dependent on a higher level of maturity on the MITRE side as well as broader industry publicity.

Practical advice for using the ATT&CK framework

Regardless of whether or not companies decide to use LogPoint SIEM, there are important considerations when implementing the ATT&CK framework.

LogPoint and the ATT&CK framework

To get the basic implementation of the LogPoint ATT&CK functionality in terms of queries, security teams should simply turn on all alerts and then proceed to tune them as they would any other SIEM solution. Particularly interesting items are alerts that rely on quantified values, such as the number of seconds or number of attempts because this is where baselining comes to play an important part.

We do not advise that security teams change the alerting rules, apart from the tuning mentioned above, because LogPoint specifically develops rules to cover particular scenarios. We base alerting on a significant amount of experience, from both internal and community knowledge. If security teams want to introduce customized commands, they should copy the commands they find relevant or interesting and then change the copies, to preserve the ability to reference the original.

LogPoint has classified most of the output under the framework, which means it’s essential to ensure a basic understanding of ATT&CK among the management as well as relevant security and IT staff. A basic understanding will ensure that security teams gain the utmost benefit from ATT&CK’s unified taxonomy and can shorten the cycle of regular tasks, such as reporting.

Using the ATT&CK framework in isolation

A company can also use the framework in isolation – with or without LogPoint or any other security product. First, security teams should ensure that there is a broad understanding of the framework and its purposes among

To get the most value from ATT&CK, security teams should standardize internal security procedures around the framework.

the relevant staff. High-level management must understand the basics of the framework because they aren't typically included in overly technical discussions and activities. One of the essential uses of ATT&CK is to bridge the gap between technical and non-technical teams.

It can be difficult to standardize in an immature, sparsely documented environment. However, keep in mind that starting to use ATT&CK does not require an overhaul. Security teams can simply begin future projects with ATT&CK in mind. Regardless, it's a good idea to recognize that going forward, documentation and interoperability services will increasingly rely on ATT&CK and other standardized frameworks.

Conclusion

MITRE ATT&CK is a modern framework for classifying malicious activities in a computerized environment. ATT&CK is applicable in a variety of scenarios, and it is easy to share. In a very short time, there has been a broad community effort to develop tools, methodologies and procedures based around this framework. The cybersecurity community's embrace of ATT&CK has solidified it as the current standard for documenting and formalizing threat information.

LogPoint covers a significant part of the framework's use cases, and we are continually working to maintain and increase LogPoint's ability to support the framework. We are committed to basing all updates to both current and future product features on ATT&CK.

The implementation of ATT&CK in an organizational environment is dependent mostly on the interpretation and codification of security. Organizations need to prioritize security activities in proportion to their desire to implement and stick to ATT&CK.

The need to prioritize security efforts applies to all organizations looking to use ATT&CK regardless if they use LogPoint, other security products or no security products at all.

The ATT&CK framework also possesses a comprehensive capability to enhance defensive aspects, even if it's adapted in part or isolation. Its abilities to support offensive testing are limited, yet worth consideration.

About LogPoint

LogPoint is committed to creating the best SIEM in the world. We enable organizations to convert data into actionable intelligence: supporting cybersecurity, compliance, IT operations, and business analytics. LogPoint's modern SIEM with UEBA provides advanced analytics and AI-driven automation capabilities that enable our customers to securely build-, manage, and effectively transform their businesses. Our flat licensing model, based on nodes rather than data volume, drastically reduces the cost of deploying a SIEM solution on-premise, in the cloud or as an MSSP.

Contact LogPoint

If you have any questions or want to learn more about LogPoint and our next-gen SIEM solution, do not hesitate to contact us at ➡ sales@logpoint.com