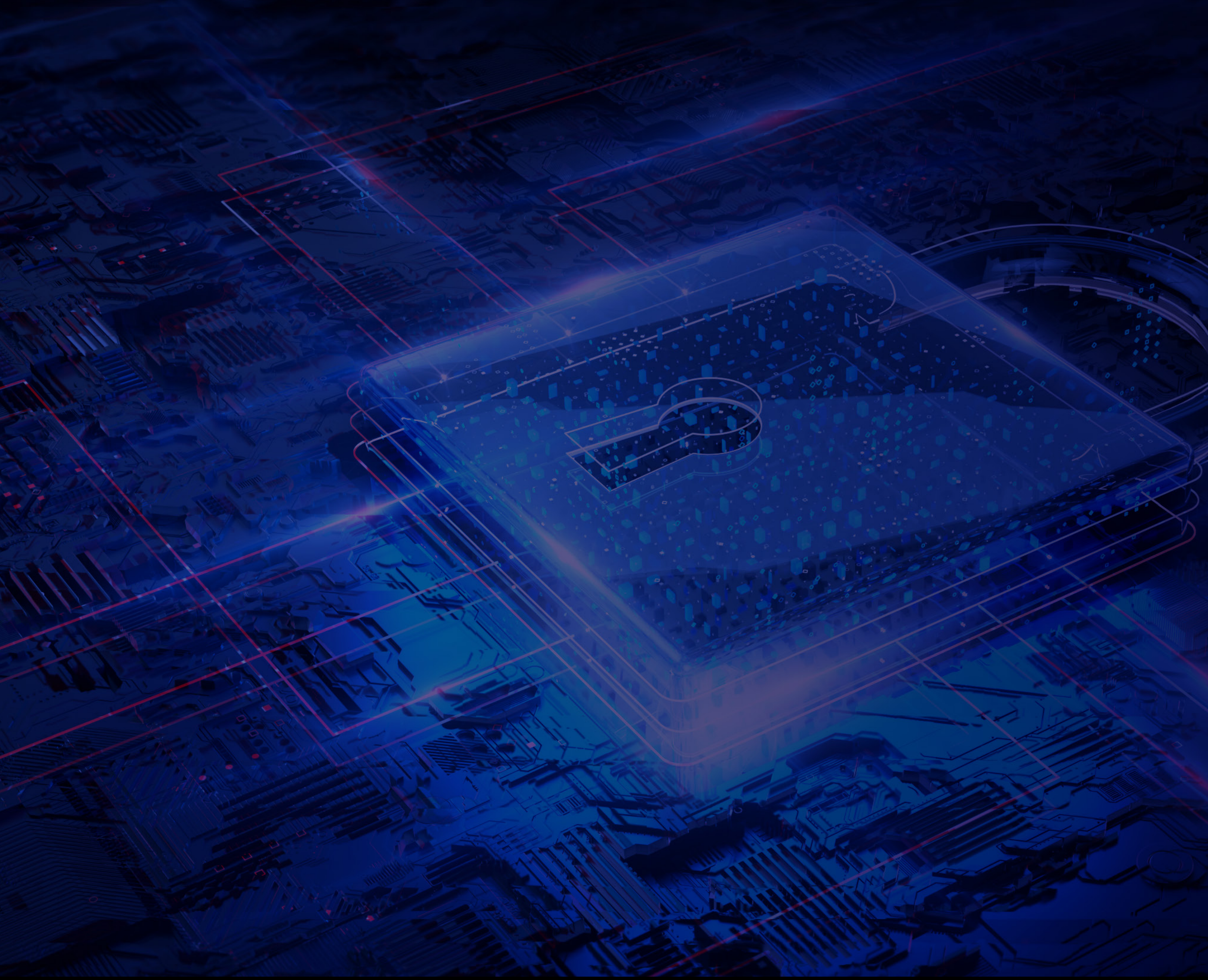

5 Step Guide to Getting Started with the MITRE ATT&CK Framework

Implementing a best practices framework for better detection and response

WHITE PAPER

DEVO

Table of Contents

How using the MITRE ATT&CK framework delivers better security outcomes

Two of the biggest hurdles every security operations team needs to overcome are the lack of time and a shortage of available resources. No matter what aspect of cyber security you're delivering, it takes both to properly plan, implement, tune, and manage an effective program.

Any inefficiency can result in a failure to detect and respond to critical threats in time to prevent a costly breach or other potentially catastrophic damage. That's why a standardized approach to security based on community shared best practices is so important.

While there isn't a universal method of detection and response, one of, if not the most important aspects of a standards-based approach is that it draws upon the collective experience of an expert community. This allows for a broad range of perspectives and analytical viewpoints that ensures that the framework is not artificially skewed by a specific methodology or approach. And although there are a few different industry standards for structuring a security program, one of the fastest growing methodologies is the MITRE ATT&CK framework.

This whitepaper discusses the MITRE ATT&CK framework and gives a brief introduction on how to get started with the framework to effectively deliver better and more consistent security outcomes.

MITRE | ATT&CK®

MITRE ATT&CK® is a globally-accessible knowledge base of adversary Tactics and Techniques based on real-world observations.

COMMON USE CASES

Detections & Analytics

Cyber defenders can develop analytics that detect the techniques used by an adversary.

Threat Intelligence

Analysts can use a common language to structure, compare, and analyze threat intelligence.

Adversary Emulation & Red Teaming

Red teams can leverage a common language and framework to emulate specific threats and plan their operations.

Assessment & Engineering

Assess an organization's capabilities and drive engineering decisions, such as which tools or logging to implement.

MITRE ATT&CK (ADVERSARIAL TACTICS, TECHNIQUES & COMMON KNOWLEDGE)

The MITRE ATT&CK framework has been developed over the years drawing from an extensive body of work related to real-world observations by security experts of how adversary groups operate. It was designed to deliver a common language for security experts to discuss the methods that these groups use.

Attacks are organized by "Tactics" and "Techniques" categories with specific sub-techniques that attackers use through various stages of an attack. This delivers a more comprehensive view of the attack life-cycle and also provides context around the attacker's intent.

The ATT&CK framework isn't limited to defining Tactics and Techniques. It also delivers a wide range of suggested best practices for detecting and responding to individual threats.

Following the framework's recommendations not only simplifies the process of implementing a formal detection and response program, it also enforces a more consistent and uniform approach to threat defense that delivers better security outcomes in a shorter amount of time.

The MITRE ATT&CK framework was designed for adaptability so that it can evolve to match changes in adversary behavior.

TECHNIQUES

The specific activities that attackers use to achieve their objectives are known as Techniques, which have been further broken down into sub-techniques. There are currently hundreds of techniques and sub-techniques with associated detection and mitigation recommendations.

TACTICS

- Reconnaissance
- Resource Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral movement
- Collection
- Command and Control
- Exfiltration
- Impact

Step 1: Intelligently Integrate Everything

You can't detect what you can't see, and the ability to effectively leverage the MITRE ATT&CK framework starts with visibility. Attackers rarely use a single tactic or technique and lack of visibility into specific threat vectors can leave you blind to not only individual attacks, but the broader picture as well. And it's critical to be able to see how multiple Tactics and Techniques fit together to identify a multi vector attack faster.

But you also need to be efficient. That means collecting only what you need now, while retaining the ability to access additional event context as needed.

So how is that accomplished? First, you define the level of detection and the data sources necessary to deliver real-time, comprehensive visibility and multi-vector threat detection.

This includes cloud, endpoint, network and user data to ensure that you have the broadest and deepest visibility into the Tactics and Techniques targeting your environment. Then you determine which data sources need to be monitored and analyzed in real time, and which are more effective for attack verification, forensic analysis and threat hunting.

Upfront planning is critical for optimizing your playbooks for automated analysis and alert triage, autonomous threat detection, and rapid incident response.

It's critical to see how multiple Tactics and Techniques identified by the MITRE ATT&CK framework fit together to identify a multi-vector attack faster.

How Devo Delivers:

The Devo Platform integrates with the tools you already have in place, collecting and analyzing all critical security data, delivering comprehensive threat detection and response for cloud, endpoint, network and user-oriented attacks. Attackers rarely use a single tactic or technique, and lack of visibility into specific threat vectors can leave you blind to not only individual attacks, but the broader picture as well. With Devo, you can natively leverage MITRE ATT&CK to assess your defenses with MITRE ATT&CK Adviser. Analysts can better understand their coverage against the MITRE ATT&CK matrix across detections and data sources to craft their action plan against ATPs. It also allows them to determine which data sources need to be monitored and analyzed in real-time, and which are more effective for attack verification, forensic analysis and threat hunting.

Step 2: Automate Threat Analysis and Triage

Despite the proliferation of specialized security tools, and in many ways exacerbated by them, threat detection is often an inefficient and manual process. Analysts can waste hours simply cutting and pasting data from one platform to another, bouncing between screens to read through individual alerts, searching for potential IOCs, verifying relevant incident details and filling out case information.

The majority of alerts are false positives, meaning security analysts end up wasting as much as 70% of their time investigating benign activity, while legitimate threats are not investigated for hours or days. In the case of many breaches, dwell times can last for weeks or months.

In addition to wasting the majority of their time on repetitive, unproductive activities, security analysts are often separated into different operating silos while following inconsistent processes that can vary greatly between individual analysts.

This creates significant gaps in critical threat context, which makes detecting and correlating related attack behaviors difficult and limits the effectiveness of a security framework like MITRE ATT&CK, which is designed to promote a best practices approach to threat detection and response.

Security automation is a critical step in alleviating these issues to remove the margin of human error and deliver accurate detection detail aligned to specific Tactics and Techniques for each potential threat.

By codifying analysis and triage activities into automated playbooks, a consistent process mapped to the MITRE ATT&CK framework can be followed for every alert.

How Devo Delivers:

Using an extensive library of expert-defined automated detection playbooks with over 700 alert types directly aligned to the MITRE ATT&CK framework, Devo SOAR accurately analyzes threat data at machine speeds and rapidly identifies valid IOCs. This enables analysts to get a comprehensive view of an incident's lifecycle, access all documentation in a single platform and speed investigative and response actions through automated insight. Every potential threat is analyzed and scored according to risk, and the resulting alerts are automatically triaged, letting your SOC analysts stay focused on investigating true threats faster.

Step 3: Correlate Associated Threat Vectors

Attackers can (and usually will) employ multiple Tactics and Techniques to compound their ability to bypass your defenses. That makes the traditional, overly reactive focus on eliminating individual threats both inefficient and ineffective over the long run, requiring the ability to correlate multiple threats that may be tied to larger, coordinated advanced attack.

Being able to identify multi-vector attacks by correlating the use of multiple MITRE ATT&CK Tactics and Techniques delivers invaluable visibility for building the complete picture of an attack profile. But accomplishing this requires the ability to quickly identify commonalities between the different Tactics and Techniques that are being employed. The most effective way to do this is to implement automated playbooks that can quickly identify and correlate common threat vectors and IOCs.

Playbooks need to evaluate at the individual threat, determine alert fidelity and use a combination of behavioral analysis and event context to assign an accurate risk rating. This includes applying embedded logic to assess how many different MITRE ATT&CK Tactics and Techniques were employed for that specific threat.

It should then rapidly identify one or more likely commonalities and automatically search for and intelligently correlate other threats that may be part of the same attack.

This delivers a comprehensive view of the entire attack sequence while providing mitigation guidance for every individual threat.

Correlating the use of multiple MITRE ATT&CK Tactics and Techniques delivers invaluable visibility.

How Devo Delivers:

Devo SOAR uses an automated process to perform fast and consistent intelligent case association that correlates related cases together. It aggregates and consolidates associated threat cases without requiring human intervention, automatically appending new cases to an existing case when relevant to eliminate redundancy. Devo playbooks automatically evaluate data wherever event context is validated, retrieving the right event context to assess the likelihood that a specific threat is part of a wider attack. Overall likelihood of an associated threat and the resulting risk is then calculated based on a variety of factors, including how many different MITRE ATT&CK Tactics and Techniques are employed in a single overall attack. This sets up your security team for ongoing success by delivering the speed, insights and capabilities they need to combat even the most sophisticated cyberthreats.

Step 4: Streamline Expert Investigations

Security expertise is a highly valuable skill set that requires continual training to keep up with the rapid evolution of the threat landscape. Automation increases speed and efficiency by eliminating many manual tasks and aggregating critical threat context, but the need for and benefits of automation don't eliminate the value of human expertise. Machine learning and behavioral analytics capabilities continue to improve but are nowhere close to the analytical and critical thinking capabilities of a highly trained and skilled security analyst.

The key component of running an effective security operations team is ensuring that your expert resources spend their time investigating and responding to valid security incidents rather than digging through the typical avalanche of false positive.

That means having the systems and processes in place to quickly analyze and assess an incident, and MITRE ATT&CK mapping provides an invaluable reference point for a security analyst to evaluate each true threat and assess the Tactic and Technique being used.

Formalized processes allow analysts to start significantly farther down the attack chain. They can then better leverage their expertise by staying focused on performing deep analysis on legitimate threats, assessing and executing recommended responses and providing additional feedback throughout the process.

The need for and benefits of automation don't eliminate the value of human expertise.

How Devo Delivers:

Seconds matter when it comes to defending your organization. Devo arms your analysts with the fastest query capabilities, real-time alerting and data analytics, and 400 days of always-hot data. Analysts can seamlessly integrate all your data sources and support thousands of always real-time concurrent queries as well. All together you get unsurpassed visibility and the ability to keep pace with attackers. Get the speed and efficiency you need to protect your enterprise. Devo makes it easy to ingest your data, enrich it, correlate it, visualize it, and most importantly act on it — with confidence.

Step 5: Automate Incident Response Playbooks

The MITRE ATT&CK framework not only explains how to detect specific threats, it also provides recommended mitigation responses for each Technique. These actions are based on years of research and drawn from the wider community of expert security professionals. And by having the appropriate mitigation for each technique, security analysts are able to significantly reduce mean time to resolution (MTTR) for MITRE-defined attacks.

In most cases, taking quick action in response to an attack is critical, yet few solutions give you the ability to respond quickly in a way that easily adapts to your requirements. Typically, available response options are limited to providing access to a narrow set of automated containment actions or delivering recommendations that require you to manually initiate any response. Or when automation is available, it's binary in nature, requiring 100% confidence that the triggering event is correct.

A best practices approach includes options for deciding whether to execute actions automatically or queuing them up for immediate execution pending approval by customer security analysts or other personnel. Any automation action can also be executed on an ad hoc basis within any case via an embedded CLI.

This delivers the most flexible means of reducing resolution times without violating policy.

Security analysts are able to significantly reduce mean time to resolution (MTTR) for MITRE-defined attacks.

How Devo Delivers:

SOCs need to equip their security teams with rich, correlated data and automate repeatable tasks so their analysts have the time and energy they need for incident resolution. Devo SOAR offers multiple options for rapid response that can all be mapped to recommendations in the MITRE ATT&CK matrix. Although any action can be fully automated, they can also be configured to require one-click authorization allowing you to review the case details first, while immediately executing the action when you're ready. You retain complete control, but no longer have to bounce between platforms to execute necessary containment actions to stop an attack. It includes:

- Fully automated response on any action for immediate execution
- Simple, one-click authorization for speed and control
- Embedded CLI for rapid ad hoc execution of any action
- Simple toggle to switch between fully automated and one-click response

How Devo SOAR Works with MITRE ATT&CK

Devo has refined and automated hundreds of threat hunting detection patterns and techniques and mapped them to the MITRE ATT&CK framework, a globally accessible knowledge base of adversary Tactics and Techniques based on real-world observations and maintained by the MITRE Corporation. Some major capabilities in the Devo SOAR playbooks include:

IDENTIFY MALICIOUS PROCESS CHAINS

By baselining your environment and recognizing patterns in thousands of known malicious examples, Devo can automatically identify anomalous and suspected malicious parent/child process relationships.

AUTOMATED POWERSHELL COMMAND TRIAGE

The playbook de-obfuscates and analyzes Powershell commands, factoring in hundreds of patterns and a machine learning classifier trained on your organization's data.

"LIVING OFF THE LAND" ATTACK TECHNIQUE SIMILARITY

Devo has identified numerous patterns of attack techniques, drawing on the MITRE ATT&CK framework. Devo playbooks can find new attacks through fuzzy text similarity matching on thousands of known attack examples and by matching known patterns manually created by domain experts.

CUT ANALYST TIME WITH AUTOMATED SUSPICIOUS URL TRIAGE

Integration of a URL analysis engine allows Devo SOAR to automatically retrieve the content behind suspicious URLs, hash the downloaded files, and scan files with a custom set of YARA file analysis rules.

AUTOMATION-DRIVEN DETECTION AND RESPONSE

Combining automatic false positive reduction with a composite risk-ranked view of threats from the various analysis and enrichment engines, Devo SOAR provides truly advanced threat detection capabilities, while acting as a force multiplier for your analysts.

How Devo Delivers:

Having access to detailed information about relevant nation state threat actors and threat groups will better equip security teams to be informed as they proactively hunt for pertinent threat actors targeting the organization.
Get the complete MITRE ATT&CK "story" as it unfolds, without any gaps:

- KPI-based dashboards to quickly understand the big picture
- Continuous detection and response
- Contextualized cases so your team can focus only on real threats
- Full transparency into hundreds of out-of-the-box threat detection playbooks mapped to MITRE ATT&CK Framework

About Devo

Devo is the only cloud-native logging and security analytics platform that releases the full potential of your data to empower bold, confident action. With unrivaled scale to collect all of your data without compromise, speed to give you immediate access and answers, and clarity to focus on the signals that matter most, Devo is your ally in protecting your organization today and tomorrow. Headquartered in Cambridge, Massachusetts, with operations in North America, Europe and Asia-Pacific, Devo is backed by Insight Partners, Georgian, TCV, General Atlantic, Bessemer Venture Partners, Kibo Ventures and Eurazeo. Learn more at **www.devo.com**.

Intelligence at the Speed of Decision Automation

TRANSFORM YOUR SOC

As you shift to the cloud, join leading organizations transforming their SOCs with Devo to streamline security operations and defend against the expanding threat landscape.

SHIFT LOGGING TO THE CLOUD

Eliminate the constraints and compromises imposed by legacy logging and get the speed, scale, and clarity your organization needs.

EMPOWER YOUR ANALYSTS

Improve your team's effectiveness with a next-gen SIEM that provides the data, context, and workflow they need to triage, investigate, and hunt.

Devo
255 Main Street
Suite 702
Cambridge, MA 02142

Devo is the only cloud-native logging and security analytics platform that releases the full potential of your data to empower bold, confident action. With unrivaled scale to collect all of your data without compromise, speed to give you immediate access and answers, and clarity to focus on the signals that matter most, Devo is your ally in protecting your organization today and tomorrow. Devo is headquartered in Cambridge, Mass. Learn more at **www.devo.com**.