IMMERSIVELABS

ALIGNING CYBER SKILLS TO THE MITRE ATT&CK® FRAMEWORK

WHAT IS MITRE ATT&CK?

ATT&CK STANDS FOR ADVERSARIAL TACTICS TECHNIQUES & COMMON KNOWLEDGE

The MITRE ATT&CK® framework is a comprehensive matrix of tactics and techniques used by threat hunters, red teamers and defenders to help identify attack types and define risk.

It began life as an internal project but has since developed into a comprehensive public knowledge base adopted by numerous security vendors and consultants.

As a knowledge base of cyber-attack tactics, techniques and procedures, MITRE ATT&CK brings structure to the understanding of adversarial behavior.

Its organized approach means you can select the attack required to validate your security strategy, and then analyze your defense in order to expand your security controls rationally.

It also helps security management to identify critical problems for remediation quickly. This objective assessment is a data-driven approach to prioritizing and scaling your cybersecurity program and budget.

THE BEAUTY OF AN EFFECTIVE FRAMEWORK

A COMMON LANGUAGE THAT THOSE IN EVERY SECURITY ROLE CAN UNDERSTAND

MITRE ATT&CK has brought a well-matured taxonomy of tactics and techniques that an attacker could deploy. For the first time there exists a common terminology that enables stakeholders, cyber defenders and vendors to communicate on the exact nature of threats and conduct objective evaluations of defensive capability. The precision of this common lexicon, which describes attacker procedures, tools and techniques, enables accurate assessments of threats and a faster, more targeted response.

BREADTH AND DEPTH OF ADVERSARY BEHAVIOR

Conceptual frameworks like the Cyber Kill Chain, the Diamond Model, and NIST's CSF have tried to bring clarity to cyber-attack definitions. They have proved useful to those leading security and risk teams when defining a broad security strategy, but they lack the details required for more operational security work, such as threat modeling efforts and incident response.

MITRE ATT&CK adds a key component: complete explanations of the tactical needs of security operations teams. This makes it a multi-faceted tool and a crucial addition in the maturing of cybersecurity strategies.

CONTINUALLY UPDATED WITH EMERGING THREATS

New tactics and techniques can be added to align with the evolving threat landscape, which means the ATT&CK framework lives and breathes. MITRE does some of this work through regular updates to its website, but as the framework uses a matrix-style format, it can be easily customized using a spreadsheet (or one of many GitHub projects and visualization tools).

A GUIDED TOUR OF THE FRAMEWORK

The MITRE ATT&CK framework presents a well-organized taxonomy of a threat actor's tactics and techniques. It aims to improve post-compromise detection in enterprises by illustrating the actions an attacker may have taken. How did the attacker get in? How are they moving around? These are the questions that the knowledge base answers, helping to define an organization's security posture at the perimeter and beyond.

Organizations can use the framework to identify defensive frailties — and then prioritize them based on risk.

WHAT ARE TACTICS?

A **TACTIC** is a high-level description of attacker behavior, and it represents a class of a certain type of behavior.

WHAT ARE TECHNIQUES?

A **TECHNIQUE** provides a more detailed description of specific types of behavior within that TACTIC class.

THE ATT&CK MATRIX

MITRE presents five different matrices to organize and present the attacker tactics and techniques:

- PRE-ATT&CK
- Enterprise – Linux
- Enterprise – macOS
- Enterprise – Windows
- Mobile

PRE-ATT&CK is organized around an adversary's activity prior to launching an attack. The remaining matrices align with the execution of the specific attacks by computing platform.

Threat hunters can leverage the ATT&CK framework to look for specific techniques that adversaries may use in conjunction with others. The framework is extremely useful for gauging an organization's visibility against targeted attacks with the existing tools deployed across their endpoints and perimeter.

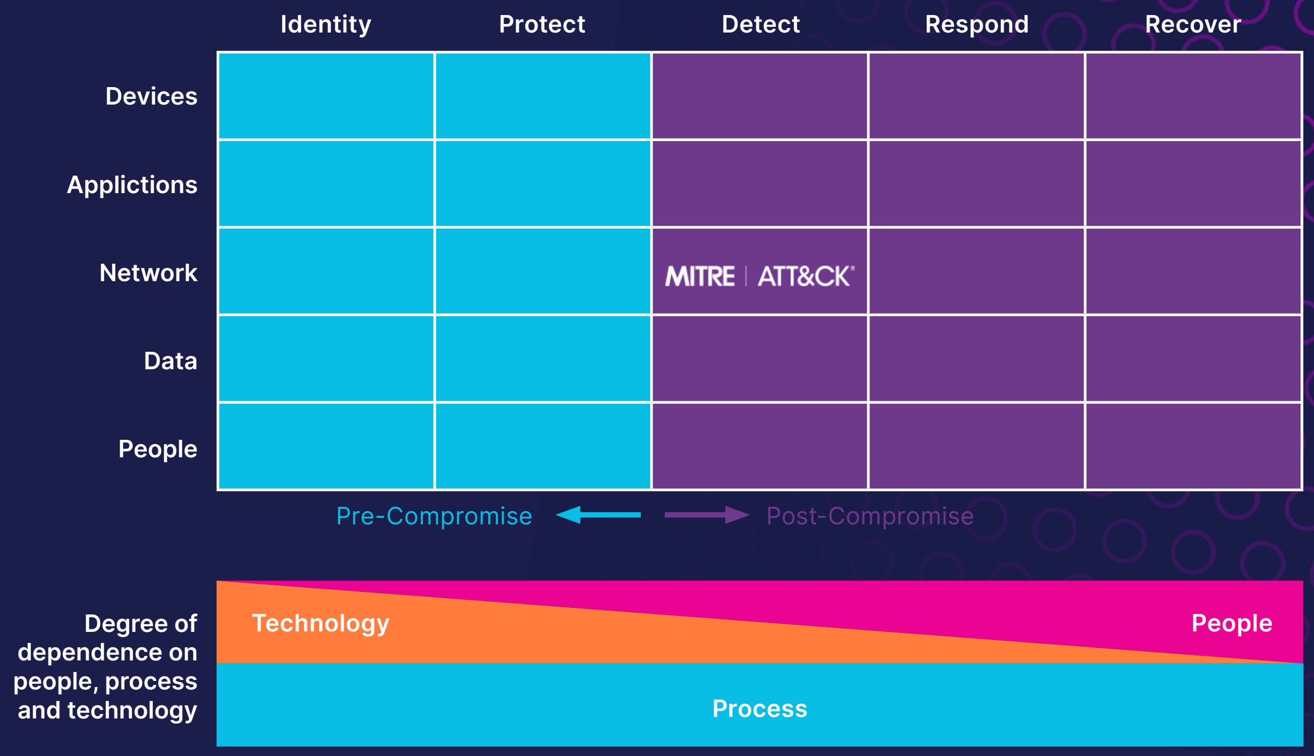
SECURITY EVALUATION USE CASES FOR MITRE FOCUS SOLELY ON TECHNOLOGY

MITRE recently introduced a program for evaluating the threat detection capability of security technology. This open methodology for highlighting potential gaps and even significant overlaps in deployed solutions is a valuable and practical addition to ATT&CK's use cases.

WHY THE HUMAN ELEMENT IS SO IMPORTANT

Human capabilities are clearly a vital element in an effective security strategy. Although techniques applied by threat actors are technical in nature (as defined in ATT&CK), understanding the motivation behind tactics and identifying potential techniques isn't always a job for technology alone. The way humans contextualize information makes their role as important as implemented security technology — if not more.

ATT&CK occupies the intersection between technology and people, so when applying the framework, it makes sense to also evaluate the capabilities of individuals in relevant roles.



UPSKILLING PEOPLE SHOULD AUGMENT THE BENEFITS OF TECHNOLOGY

MAKING UPSKILLING RELEVANT AND RAPID

One potential pitfall of implementing ATT&CK as a framework for cybersecurity is its sheer size. To get the most from it, you should focus on relevant tactics and ensure effective security to counter the techniques most applicable to the risks your business faces. For each tactic and technique, ensure you've considered the impact of human capabilities in your organization; and where you see gaps, deploy techniques that allow for rapid upskilling.

ON-DEMAND AND GAMIFIED SKILLS DEVELOPMENT

Practical, gamified and on-demand exercises such as simulations and capture the flags (CTFs) can get security professionals hands on with specific techniques, helping to build a culture of continuous skills development. Going beyond static, classroom training is essential.

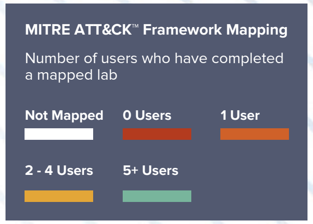
Ensuring security teams develop skills that make them more effective is just one aspect of efficient training. It's just as important to measure and visualize skills as they're acquired and to understand how those skills best align your people to your security strategy.

MAPPING AND MEASURING SKILLS ALIGNED TO MITRE ATT&CK WITH IMMERSIVE LABS

Immersive Labs is packed with cyber skills content mapped directly to tactics and techniques in the ATT&CK framework. As individuals complete relevant exercises, our ATT&CK heat map will show you where coverage is strong and where improvement is needed.

An understanding of skill levels across all security functions brings invaluable insights in some key areas:

01 In the event of an incident, you'll be able to identify individuals with the right skills to respond as the situation unfolds.

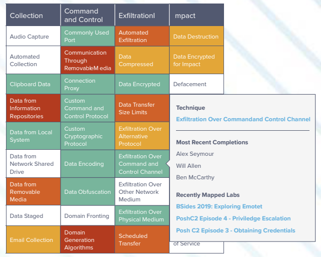


MITRE ATT&CK™ Framework Mapping

Number of users who have completed a mapped lab

Not Mapped	0 Users	1 User
⬜	🟥	🟧
2 - 4 Users	**5+ Users**	
🟨	🟩	

02 Visualizing skill levels will help you measure and communicate improving areas of coverage as well as those that require investment.



Collection	Command and Control	Exfiltrationl	mpact
Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Automated Collection	Communication Through RemovableM edia	Data Compressed	Data Encrypted for Impact
Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	
Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	
Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	
Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	
Data Staged	Domain Fronting	Exfiltration Over Physical Medium	
Email Collection	Domain Generation Algorithms	Scheduled Transfer	of Service

Technique

Exfiltration Over Commandand Control Channel

Most Recent Completions

Alex Seymour

Will Allen

Ben McCarthy

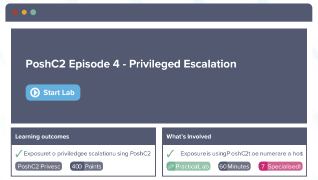
Recently Mapped Labs

BSides 2019: Exploring Emotet

PoshC2 Episode 4 - Priviledge Escalation

Posh C2 Episode 3 - Obtaining Credentials

03 Gamified learning experiences will see teams and individuals competing for points and badges to prove their skills.



PoshC2 Episode 4 - Privileged Escalation

Learning outcomes

✓ Exposuret o priviledgee scalationu sing PoshC2

PoshC2 Privesc 400 Points

What's Involved

✓ Exposureis usingP oshC2t oe numerare a host

PracticalL ab 60 Minutes 7 Specialisedl

ABOUT IMMERSIVE LABS

Immersive Labs is the world's first fully interactive, gamified and on-demand cyber skills platform. Our technology delivers challenge-based assessments and upskilling exercises which are developed by cyber experts with access to the latest threat intelligence. Our unique approach engages users of every level, so all employees can be equipped with critical skills and practical experience in real time.

IMMERSIVELABS

www.immersivelabs.com | enquiries@immersivelabs.com