Blue Team Level 1 Certification (Standard)

Introduction to BTL1

- ~~Welcome to Blue Team Level 1!~~ — 4 Topics
- ~~Lab and Forum Access~~

SECURITY FUNDAMENTALS DOMAIN

- ~~Introduction to Security Fundamentals~~ — 1 Topic
- ~~Soft Skills~~ — 7 Topics
- ~~Security Controls~~ — 5 Topics | 1 Quiz
- ~~Networking 101~~ — 6 Topics | 1 Quiz
- ~~Management Principles~~ — 4 Topics | 1 Quiz

PHISHING ANALYSIS DOMAIN

- ~~PA1) Introduction to Emails and Phishing~~ — 7 Topics | 1 Quiz
- ~~PA2) Types of Phishing Emails~~ — 10 Topics | 2 Quizzes
- ~~PA3) Tactics and Techniques Used~~ — 12 Topics | 2 Quizzes
- ~~PA4) Investigating a Phishing Email~~ — 8 Topics | 2 Quizzes
- ~~PA5) Analysing URLs, Attachments, and Artifacts~~ — 8 Topics | 1 Quiz
- PA6) Taking Defensive Actions — 12 Topics | 1 Quiz
- PA7) Report Writing — 7 Topics | 1 Quiz
- PA8) Phishing Response Challenge — 3 Topics | 1 Quiz

THREAT INTELLIGENCE DOMAIN

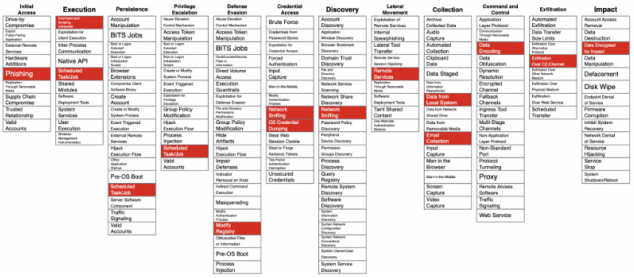
- TI1) Introduction to Threat Intelligence — 7 Topics
- TI2) Threat Actors & APTs — 6 Topics | 2 Quizzes
- TI3) Operational Threat Intelligence — 7 Topics | 1 Quiz
- TI4) Tactical Threat Intelligence — 7 Topics | 1 Quiz
- TI5) Strategic Threat Intelligence — 5 Topics | 1 Quiz
- TI6) Malware and Global Campaigns — 6 Topics | 1 Quiz

DIGITAL FORENSICS DOMAIN

- DF1) Introduction to Digital Forensics — 5 Topics
- DF2) Forensics Fundamentals — 10 Topics | 5 Quizzes
- DF3) Digital Evidence Collection — 8 Topics | 1 Quiz
- DF4) Windows Investigations — 3 Topics | 3 Quizzes
- DF5) Linux Investigations — 4 Topics | 2 Quizzes
- DF6) Volatility — 3 Topics | 1 Quiz

Activity) ATT&CK Navigator

In this activity you're going to become familiar with using ATT&CK Navigator as a tracking tool, and understand how it can be used by blue team and red team members with the ultimate goal of improving an organisation's security posture. At the end of this lesson you'll get hands-on with this tool and answer a number of questions about ATT&CK Navigator.



The above image is a screenshot of the MITRE ATT&CK framework in ATT&CK Navigator. We have specified a number of techniques that were "used" by an adversary in a fictional attack. Can you work out what the attacker did by looking at the coloured items?

In this example the attack scenario would look something like this:

1. An attacker sends a phishing email to an employee at the target organisation including a Microsoft Word document with a malicious macro.
2. PowerShell was executed to download an executable file which initiates a reverse connection to a command-and-control server (C2) and was added as a schedule job to execute at a routine interval on the infected system to provide persistence.
3. The registry was modified to reduce the chance of detection.
4. The attacker then dumped credentials from the OS by retrieving memory from LSASS.exe and then standard sniffing network traffic to identify other online systems and the services they are running.
5. The attacker logged into other systems using the valid credentials obtained from LSASS to perform lateral movement.
6. Emails and local files were collected and prepared for exfiltration.
7. These files were encoded and exfiltrated through a connection to the C2 server, uploading them to an external attacker-owned system.
8. Ransomware was then deployed to cover the attacker's tracks and cause disruption to the target organisation.

While the above image doesn't capture all of the details, it is immediately clear what techniques were used by an adversary in this fictional cyber attack. If you can't already see the value of using ATT&CK Navigator, let's explore some more use cases for this tool!

The Purpose of Threat Hunting:

Threat Hunting is the process of identifying threat actors that have already made it past the perimeter and are now operating inside an environment undetected. It is our job to create a hypothesis, investigate it, and come to a conclusion. An example could include "I believe that malicious actors are utilizing PowerShell within the environment to complete malicious acions". We would then look to audit all PowerShell logs and look for specific commands that are suspicious or malicious, either proving or disproving our hypothesis. Threat Hunting requires a very mature security function as some basic requirements include experienced analysts that understand the ATT&CK framework and cyber kill chain, centralized logging (more than just a SIEM!), and the time to deep-dive into endless logs and events to find the ones that indicate the presence of an adversary.

How ATT&CK Navigator Can Help:

DF7) Autopsy
4 Topics | 1 Quiz

SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN

SI1) Introduction to SIEM
7 Topics | 1 Quiz

SI2) Logging
6 Topics | 2 Quizzes

SI3) Aggregation
2 Topics | 1 Quiz

SI4) Correlation
6 Topics | 1 Quiz

SI5) Using Splunk
5 Topics | 2 Quizzes

INCIDENT RESPONSE DOMAIN

IR1) Introduction to Incident Response
8 Topics | 1 Quiz

IR2) Preparation Phase
10 Topics | 2 Quizzes

IR3) Detection and Analysis Phase
7 Topics | 4 Quizzes

IR4) Containment, Eradication, and Recovery Phase
5 Topics | 1 Quiz

IR5) Lessons Learned and Reporting
7 Topics

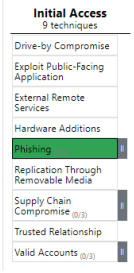
IR6) MITRE ATT&CK
13 Topics | 2 Quizzes

Section Introduction, ATT&CK
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command and Control
Exfiltration
Impact
Activity) ATT&CK Navigator
Activity) End of Section Review, ATT&CK

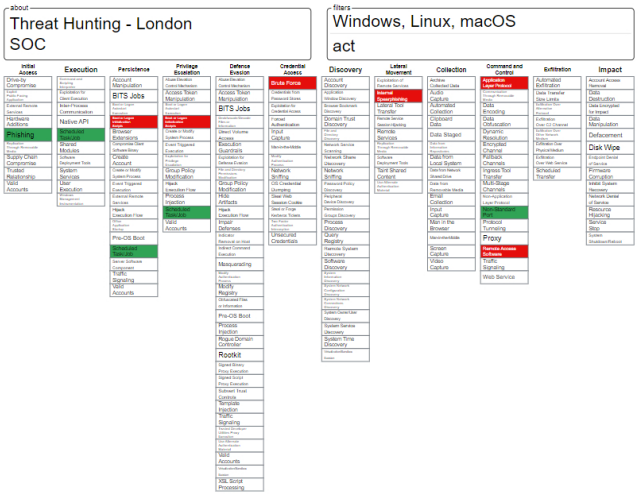
BTL1 EXAM

Exam Preparation
Using RDP and SSH
How to Start Your Exam

A great way that ATT&CK Navigator can be utilized is to keep track of what techniques the threat hunters have tried to discover the presence of. For example, if we wanted to hunt for malicious phishing emails that adversaries have sent that haven't been detected by employees or security controls (such as spear-phishing emails) then we would create an ATT&CK graph and begin our phishing threat hunt. Once this was concluded the team could color in that technique to show that they have conducted a hunt to try and detect it.



Then the hunters would move onto the next technique they want to check, over time building up an image of everything they have manually searched for. Green techniques could be ones that no malicious presence has been discovered during a hunt, while red could show malicious presence has been detected. This all ties in with 'threat detection' which we cover below!

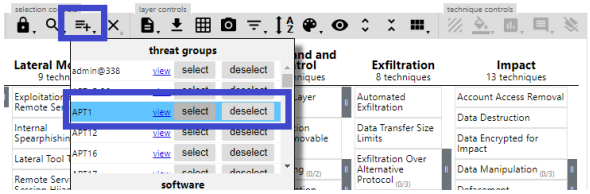


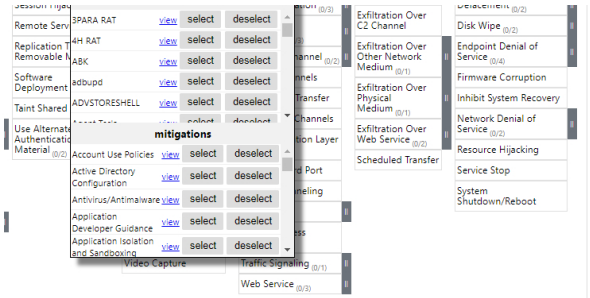
The Purpose of Adversary Emulation:

Adversary Emulation is different from a standard penetration test and requires a lot more time and knowledge. Why? because the aim is to accurately imitate advanced threat actors attacking the organization by copying all of their known tactics and techniques. Organizations with mature security teams would likely conduct these events, and have the red or purple team members imitate the techniques of threat actors that are likely to target the organization based on previous attacks, motives, and industries the actors target. This can help to tune detection rules and ensure that the security team would have visibility if that actor attacked them using the same or similar tactics.

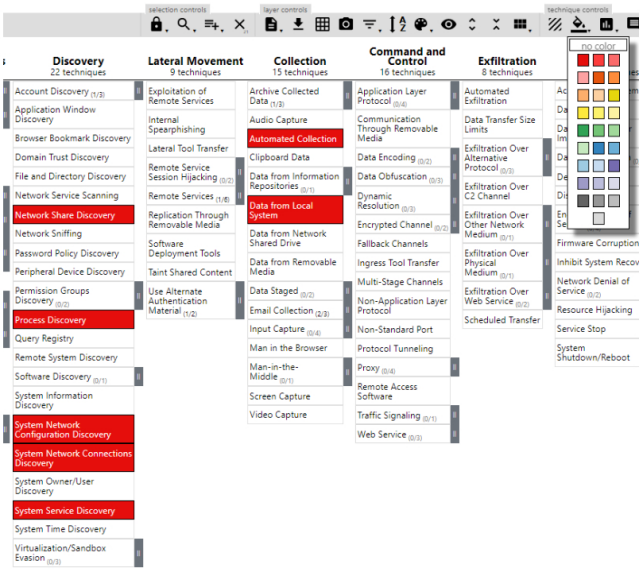
How ATT&CK Navigator Can Help:

On the MITRE ATT&CK page for groups it covers what techniques they have been known to use. From these lists we can create an instance of ATT&CK Navigator to visually map the techniques they have used, and refer to the diagram while conducting the red team engagement, effectively replicating an APT attack. But guess what! This is already built into ATT&CK Navigator! We can simply click on the "multi-select" tool, and then choose the threat actor we want to map.





In the below screenshot you can see that we have mapped the techniques used by APT1 and then used the paint bucket tool to colour them in red. If we were going to start a red team engagement, we would then look to actively use these techniques and once the engagement is over, work with the blue team to see if any of the actions were not detected. If they weren't then rule tuning and additional emphasis on detection rules and monitoring should be raised so that in the future these techniques are properly alerted to security analysts.

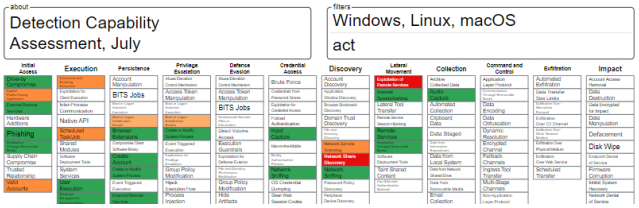


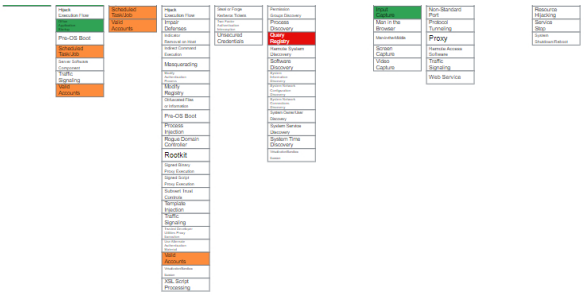
The Purpose of Threat Detection:

Threat Detection is all about ensuring that the monitoring and detection capabilities of the defenders are as accurate as they can be. From tuning false positives to writing new rulesets, security teams are constantly adapting the way they detect malicious actors from a mountain of data.

How ATT&CK Navigator Can Help:

Similar to how we can use ATT&CK Navigator for threat hunting, we can do the same for assessing detection capabilities. One-by-one we would select a technique and review existing detection rules to identify whether the security team would get an alert if that activity was conducted, such as Dumping OS Credentials. One example would be; is the security team monitoring for processes that are interacting with lsass.exe? If not then a rule needs to be created in the SIEM or EDR solution to generate an alert when this activity is observed so analysts can investigate further. Using ATT&CK Navigator we could mark techniques that have been successfully tested against current capabilities and generated an alert (green), techniques that required a rule to be created or tuning of an existing rule (amber), and techniques that are currently not detectable and are pending a new rule or detection method (red).

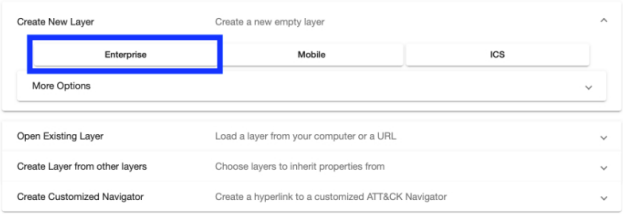




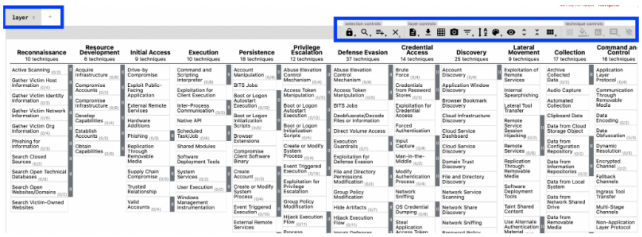
USING ATT&CK NAVIGATOR

Now that you understand why ATT&CK Navigator can be a useful tool for both red and blue teams, let's cover how to use it. You can access the tool online the MITRE Github page here – https://mitre-attack.github.io/attack-navigator/enterprise/

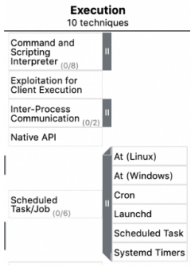
First things first, let's create a new layer for our graph. Click 'Create New Layer' and then select 'Enterprise'.



On the top left we have our current layer and the ability to add additional layers (similar to Photoshop if you've ever used it). On the top right we have all of the controls and tools we'll need to customize our layer.



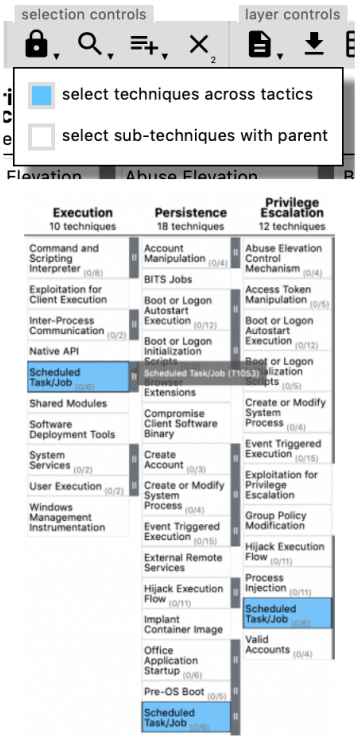
We can see all of the techniques underneath the toolbar. Notice how some of them have grey bars next to them – these are techniques that have sub-techniques. We can expand them by clicking on the grey bar as shown below.



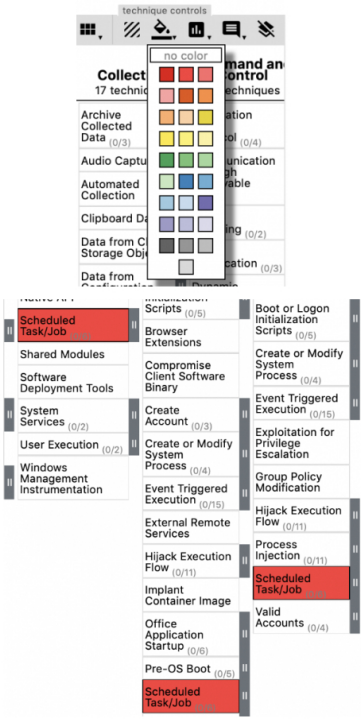
Next let's cover how to colour fill different techniques, this could be used to highlight specific set of techniques for purposes such as:

- Marking off techniques that have been simulated and observed by a security team to see if they can detect the activity (red = not detected, orange = often detected, green = always detected)
- Highlighting which techniques will be emulated during a red team engagement

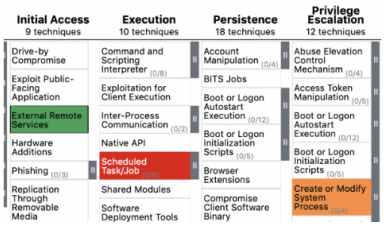
By default the selection control with the padlock icon will have the first option enabled. This will select the same technique across multiple columns, let's demonstrate by selecting a single occurrence of 'Scheduled Task/Job':

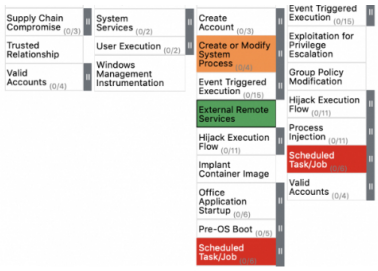


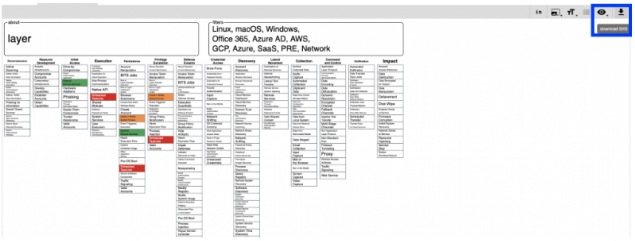
Now that we have these selected lets apply a colour to them. Go to the 'technique controls' section of the toolbar and click the paint bucket tool, then select a fill colour:



In the below example we've coloured a few more techniques so we can show you how to export this layer to an image file, allowing you to use it in presentations, share online, and do whatever else you want!







There you have it – the basics of using ATT&CK Navigator. Ready to complete a short project? Then check out the activity below!

ATT&CK Navigator Activity

For this activity, you work as a Threat Intelligence Analyst and you're presenting to the executive board on a threat group that are likely to target your organisation, a national bank. You are required to map this group's techniques to a layer on ATT&CK Navigator. Visit the MITRE page for different threat groups, locate Carbanak, and map their used techniques using a coloured fill, then export the layer to a SVG file format. To make things a bit neater you should also change the layer name to "Carbanak" by double-clicking it in the top left. **You don't need to submit anything for this activity.**

Want an extra challenge?

Identify another threat group that targets banks/financial institutions and map their tactics to a new layer in Navigator – is there any crossover between the groups? Write a short summary (1-2 paragraphs) on the similarities between these two actors!

When you have finished the activity, you can mark this lesson as complete below.

○ Mark Lesson as Completed

Check

Privacy & Cookies Policy