

# COS30015 Lab 1: MITRE ATT&CK

## 1. Basic Concepts

- What is the MITRE ATT&CK Matrix?

The MITRE ATT&CK (Adversarial Tactics, Techniques and Common Knowledge) Matrix is a framework for understanding and categorising the various tactics, techniques and procedures (TTPs) used by attackers during a cyber attack. MITRE, a non-profit organisation that works with government and industry to improve cyber security, developed the ATT&CK Matrix.

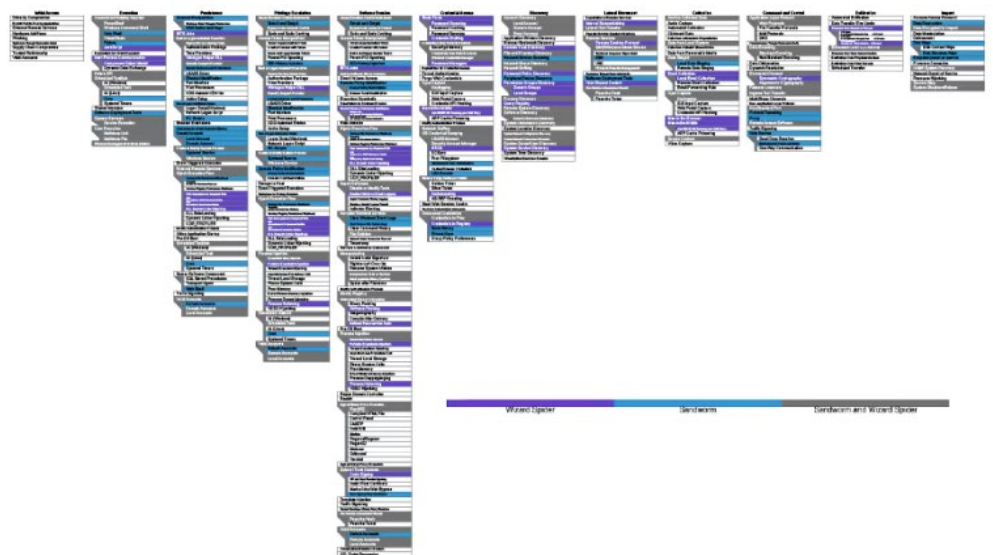
The MITRE ATT&CK Matrix is widely used in the cyber security community as a reference for identifying and responding to cyber threats. It is used by security analysts, incident responders and other cyber security professionals to better understand the tactics and techniques used by attackers to develop more effective defence strategies and to improve overall security posture.

The ATT&CK Matrix consists of two main components: tactics, techniques and procedures. Tactics represent the goals of an attacker, while techniques represent the specific methods used to achieve those goals. The ATT&CK Matrix is organised into several categories, each of which represents a different stage of a cyber attack.

- How Are the ATT&CK Matrix and the ATT&CK Framework Different?

The MITRE ATT&CK framework and the MITRE ATT&CK Matrix are two related but distinct tools developed by MITRE Corporation to help organisations improve their cyber security posture. The MITRE ATT&CK framework is a comprehensive knowledge base of tactics, techniques and procedures used by attackers during different stages of a cyber attack. It categorises the tactics and techniques based on the stage of the cyber attack (e.g., initial access, execution, persistence) and the objectives of the attacker (e.g., data theft). The framework serves as a common language that enables organisations to understand and describe the different steps that attackers take during a cyber attack and to assess their own defences against those steps.

The MITRE ATT&CK Matrix, on the other hand, is a visualisation of the tactics and techniques in the ATT&CK framework. It presents the same information in a condensed format, using a matrix that lists the tactics along the top and the techniques along the side. Each cell of the ATT&CK Matrix represents a specific technique within a specific tactic.



Example of color-coding: The MITRE ATT&CK framework: Wizard Spider & Sandworm

Reference: <https://www.paloaltonetworks.com.au/cyberpedia/what-is-mitre-attack-matrix>

## Tactics, Techniques and Procedures (TTPs)

- **Tactics** are high-level goals that an attacker might have when attempting to compromise a system or network. There are 11 tactics in the framework, such as *Initial Access*, *Execution*, *Persistence* etc. Each category includes multiple techniques, which are further broken down into sub-techniques. These techniques and sub-techniques are assigned unique identifiers and are described in detail with procedural examples, including how they work, what tools and tactics they use, and how they can be detected and mitigated.
- Each tactic is further broken down into a number of specific **techniques** (e.g., Content Injection (T1659) under Initial Access Tactic Session), which are the specific methods used to achieve the goals of the tactic. There are currently over 250 techniques documented in the framework.

For each tactic, the framework also includes information on the procedures or sub-techniques used by attackers to carry out the technique. At a high level, this means the 11 tactics above are broken down like this:

**Initial Access** — techniques used to gain access to a target system or network.

**Execution** — techniques used to run malicious code on a target system or network.

**Persistence** — techniques used to maintain a foothold on a target system or network.

**Privilege Escalation** — techniques used to gain higher levels of access on a target system or network.

**Defence Evasion** — techniques used to avoid detection by security tools and systems.

**Credential Access** — techniques used to steal user credentials or other sensitive information.

**Discovery** — techniques used to gather information about a target system or network.

**Lateral Movement** — techniques used to move from one system or network to another within a target environment.

**Collection** — techniques used to gather data or other valuable information from a target system or network.

**Exfiltration** — techniques used to remove stolen data or other valuable information from a target system or network.

**Command and Control** — techniques used to establish and maintain communication with an attacker's command and control infrastructure.

By organising attacks into TTPs, the MITRE ATT&CK framework provides a comprehensive view of the cyber threat landscape and allows organisations to better understand how attackers operate. This, in turn, can help organisations develop more effective defence strategies and improve their overall security posture.

- **Procedures** are the specific implementations the adversaries use for techniques or sub-techniques. For example, a procedure could be an adversary using PowerShell to inject into lsass.exe to dump credentials by scraping LSASS memory on a victim. Procedures are categorised in ATT&CK as the observed in the wild use of techniques in the "Procedure Examples" section of technique pages.

## 2. Three Threat Actor Cases

This document provides a walkthrough of how to use the ATT&CK Navigator (<https://mitre-attack.github.io/attack-navigator/enterprise/>) to create a matrix for a threat actor and compare different layers to analyse and conclude from cyber threat cases. (Navigator source code is available at <https://github.com/mitre-attack/attack-navigator>). This comparison method is useful if you want to compare techniques used by two different groups for example.

For this Exercise, you'll create matrices for three threat actors (e.g., APT29 techniques) and compare them. To do this, you will:

1. Find the page of the threat actor and get the table of MITRE ATT&CK Tactics and Techniques involved in the case
2. Create a layer and assign a score to techniques used by an actor in one layer
3. Create layers for other layers for different actors and assign a different score to techniques used in the cases
4. Combine these layers using "Create Layer from other layers" using the expression "a + b + c"

## 5. Export the layer in the format of your choice

- Get the TTPs information from the threat actor page

Go to the cyber actor page (<https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/svr-cyber-actors-adapt-tactics-initial-cloud-access>), scroll down and find the table compiled from the report (usually shown in the Appendix part of the page). Let's take "APT29" for the first example and you can follow these steps to create layers for other cyber actors.

### MITRE ATT&CK®

This report has been compiled with respect to the MITRE ATT&CK® framework, a globally accessible knowledge base of adversary tactics and techniques based on real-world observations.

Tactic	ID	Technique	Procedure
Credential Access	<a href="#">T1110</a>	Brute forcing	The SVR use password spraying and brute forcing as an initial infection vector.
Initial Access	<a href="#">T1078.004</a>	Valid Accounts: Cloud Accounts	The SVR use compromised credentials to gain access to accounts for cloud services, including system and dormant accounts.
Credential Access	<a href="#">T1528</a>	Steal Application Access Token	The SVR use stolen access tokens to login to accounts without the need for passwords.
Credential Access	<a href="#">T1621</a>	Multi-Factor Authentication Request Generation	The SVR repeatedly push MFA requests to a victim's device until the victim accepts the notification, providing SVR access to the account.
Command and Control	<a href="#">T1090.002</a>	Proxy: External Proxy	The SVR use open proxies in residential IP ranges to blend in with expected IP address pools in access logs.
Persistence	<a href="#">T1098.005</a>	Account Manipulation: Device Registration	The SVR attempt to register their own device on the cloud tenant after acquiring access to accounts.

### Mitigation and Detection

A number of mitigations will be useful in defending against the activity described in this advisory:

Reference: <https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/svr-cyber-actors-adapt-tactics-initial-cloud-access>

- Create a layer and assign a score to techniques used by threat actor (APT29 in this example)

Go to the ATT&CK Navigator (<https://mitre-attack.github.io/attack-navigator/enterprise/>). By default, Navigator will start with a new layer called "layer," so you'll work with that. To help keep yourself organised, you will rename the layer to "APT29" by clicking on the name at the top.

## MITRE ATT&amp;CK® Navigator

The ATT&CK Navigator is a web-based tool for annotating and exploring ATT&CK matrices. It can be used to visualize defensive coverage, red/blue team planning, the frequency of detected techniques, and more.

[help](#) [changelog](#) [theme ▼](#)

Create New Layer	Create a new empty layer	▼
Open Existing Layer	Load a layer from your computer or a URL	▼
Create Layer from Other Layers	Select layers to inherit properties from	▼
Create Customized Navigator	Create a hyperlink to a customized ATT&CK Navigator	▼

## MITRE ATT&amp;CK® Navigator

The ATT&CK Navigator is a web-based tool for annotating and exploring ATT&CK matrices. It can be used to visualize defensive coverage, red/blue team planning, the frequency of detected techniques, and more.

[help](#) [changelog](#) [theme](#) ▾

Create New Layer Create a new empty layer

Enterprise ATT&CK Mobile ATT&CK ICS ATT&CK

More Options

Open Existing Layer Load a layer from your computer or a URL

Create Layer from Other Layers Select layers to inherit properties from

Create Customized Navigator Create a hyperlink to a customized ATT&CK Navigator

Click on the button and choose the Enterprise ATT&CK, which we

**Click the layer name and change the name.**

**Rename to APT29.**

The screenshot displays the MITRE ATT&CK framework interface. The top navigation bar includes the MITRE logo (circled in red), a search icon, and a list of icons representing different attack categories. Below the navigation bar, the main content area is divided into 14 columns, each representing a category of attack techniques. The categories and their associated technique counts are: Reconnaissance (8), Resource Development (8), Initial Access (10), Execution (14), Persistence (20), Privilege Escalation (42), Defense Evasion (34), Credential Access (22), Discovery (22), Command and Control (9), Exfiltration (14), and Impact (14). The 'Reconnaissance' column is highlighted with a red circle. The 'MITRE' logo is also circled in red in the top right corner.

First, you will manually select the 6 techniques used by APT29 from this list (you may find it helpful to print this list or bring it up on a second screen as you select the techniques):

## MITRE ATT&CK®

This report has been compiled with respect to the MITRE ATT&CK® framework, a globally accessible knowledge base of adversary tactics and techniques based on real-world observations.

Tactic	ID	Technique	Procedure
Credential Access	<a href="#">T1110</a>	Brute forcing	The SVR use password spraying and brute forcing as an initial infection vector.
Initial Access	<a href="#">T1078.004</a>	Valid Accounts: Cloud Accounts	The SVR use compromised credentials to gain access to accounts for cloud services, including system and dormant accounts.
Credential Access	<a href="#">T1528</a>	Steal Application Access Token	The SVR use stolen access tokens to login to accounts without the need for passwords.
Credential Access	<a href="#">T1621</a>	Multi-Factor Authentication Request Generation	The SVR repeatedly push MFA requests to a victim's device until the victim accepts the notification, providing SVR access to the account.
Command and Control	<a href="#">T1090.002</a>	Proxy: External Proxy	The SVR use open proxies in residential IP ranges to blend in with expected IP address pools in access logs.
Persistence	<a href="#">T1098.005</a>	Account Manipulation: Device Registration	The SVR attempt to register their own device on the cloud tenant after acquiring access to accounts.

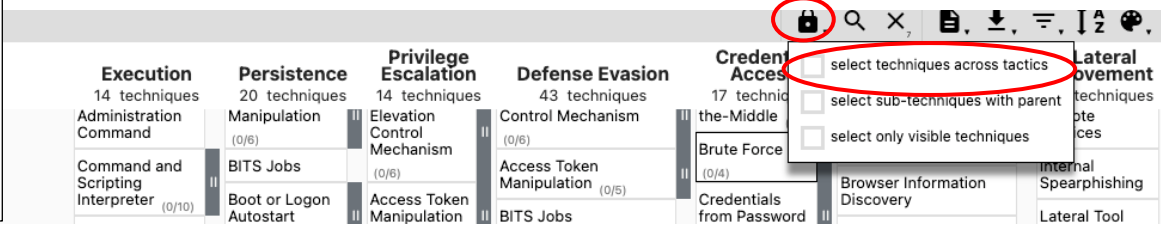
## Mitigation and Detection

A number of mitigations will be useful in defending against the activity described in this advisory:

Reference: <https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/svr-cyber-actors-adapt-tactics-initial-cloud-access>

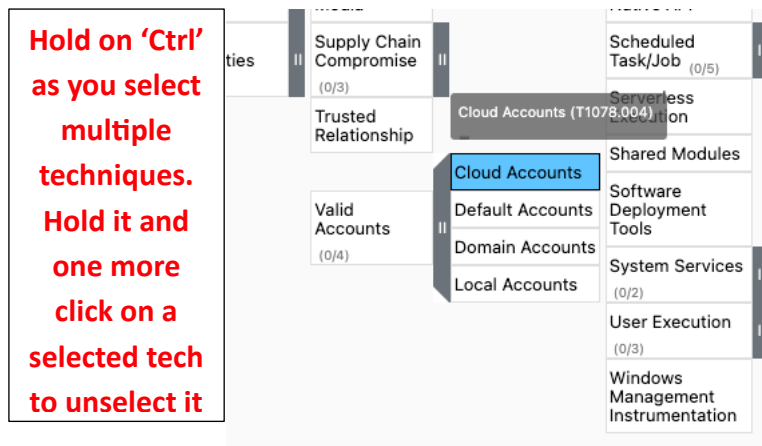
**NOTE:** By default, Navigator will select all instances of the same technique if it falls under multiple tactics. For example, Scheduled Task falls under the Execution, Persistence, and Privilege Escalation tactics, so it will be selected under all of the tactics. To turn this functionality off and only select a single tactic for a technique, click on the “lock multi-tactic technique selection” button until it appears in the unlocked position as shown below. (Alternately, you can leave it on and proceed with the exercise in a similar way.)

Click off to allow you to select a technique under a single tactic

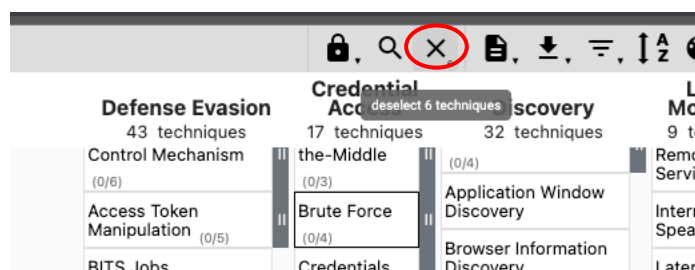


The screenshot shows the MITRE ATT&CK Navigator interface. It features a grid of tactics and techniques. The tactics listed are Execution (14 techniques), Persistence (20 techniques), Privilege Escalation (14 techniques), Defense Evasion (43 techniques), Credential Access (17 techniques), and Lateral Movement (techniques). The techniques listed under these tactics are: Administration Command, Command and Scripting Interpreter, BITS Jobs, Boot or Logon Autostart, Elevation Control Mechanism, Access Token Manipulation, Control Mechanism, Access Token Manipulation, Brute Force, Credentials from Password, Browser Information Discovery, and Internal Spearphishing. A red circle highlights the 'lock multi-tactic technique selection' button (a padlock icon) in the top right corner. A red oval highlights the dropdown menu options: 'select techniques across tactics' (selected), 'select sub-techniques with parent', and 'select only visible techniques'.

Click on the first technique to select it. To select multiple techniques, hold down the “Ctrl” key (Win)(Command Key for Mac OS) as you select additional techniques. Proceed through the matrix until all 6 of the above techniques are selected.

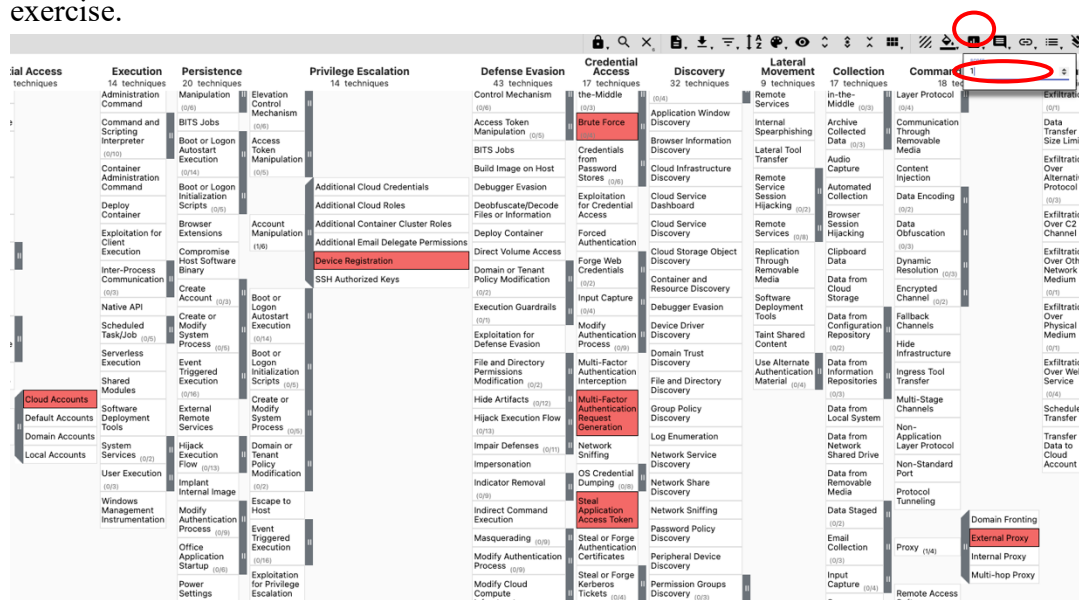


You can verify you have 6 techniques selected by hovering over the “deselect” option by not clicking it.



Hover over “deselect” button to check the number of selected

Next, you will assign a score to these highlighted techniques. You do this by clicking the “Scoring” button and choosing a score. Make the score 1 for this exercise.

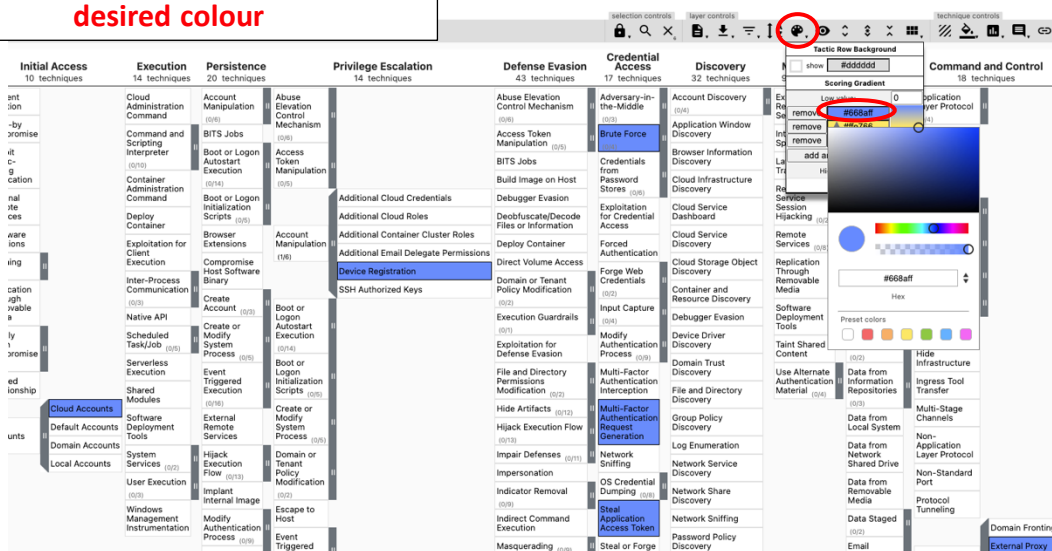


Click Scoring button and enter score of your

You may choose to give your techniques a different colour, such as blue in this example, by clicking on the “colour setup” button, selecting each value, and making each value blue. This will change all your techniques to the selected colour.



Click colour setup button and choose your colours by clicking in the value sections and selecting the desired colour



- Create layers for other layers and assign a different score to techniques used in the cases

Please follow the steps above and create for another two cyber threat actors, named *Ivanti* and *Infamous Chisel*.

**Infamous Chisel:** <https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/infamous-chisel> ;

## Threat Actors Exploit Multiple Vulnerabilities in Ivanti Connect Secure and Policy

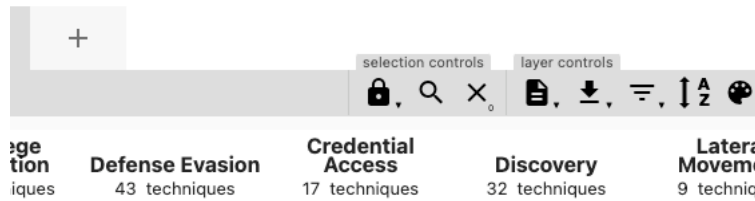
**Secure Gateways:** <https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/threat-actors-exploit-multiple-vulnerabilities-ivanti-connect-secure-and-policy-secure-gateways>

**NOTE:** Give your techniques a **different** score than you did in the APT29 layer (use 2 for Ivanti for example), and then colour them as you choose.

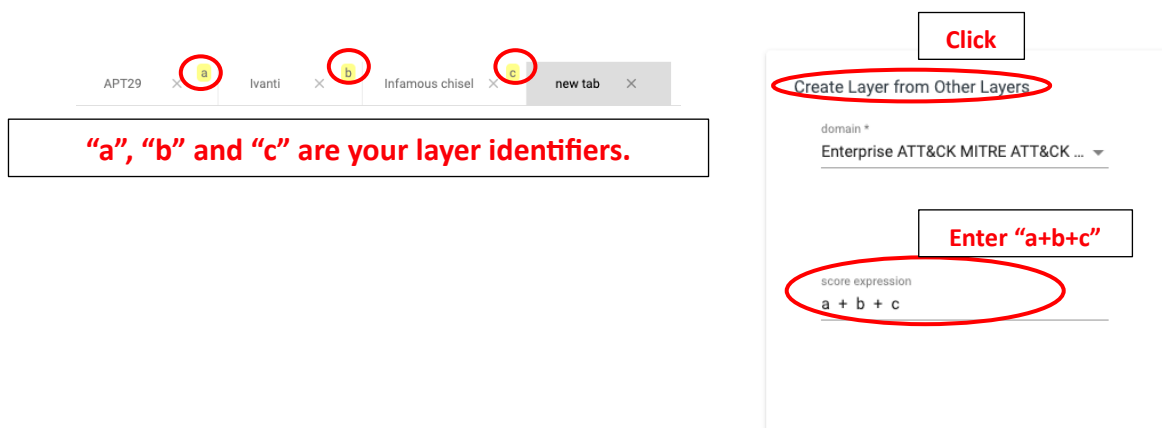
- Combine these layers using “Create Layer from other layers” using the expression “a + b + c”

Now that you have three layers, you want to combine them. You will again click the plus sign to create a new layer

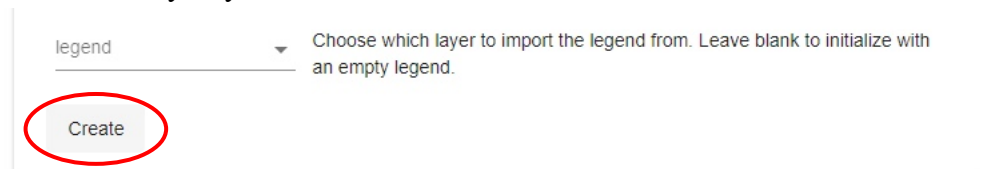




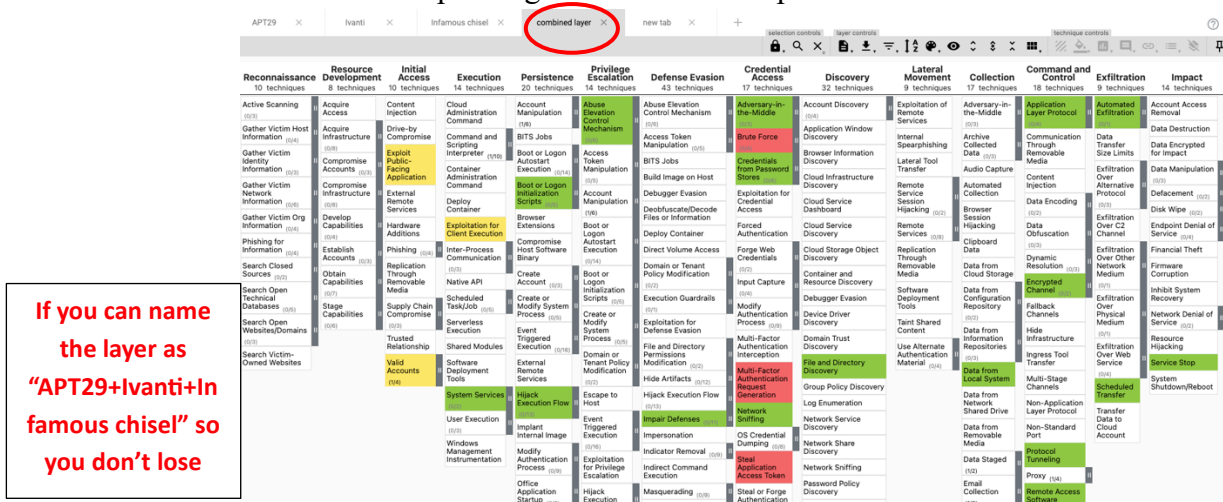
But this time you will select the option to “Create Layer from other layers” to expand the dropdown. When you expand the dropdown, Navigator helpfully gives letter names for each of your existing layers in yellow. So, you know that Navigator identifies your APT29 layer as “a” and your Ivanti layer as “b” and “Infamous chisel” as “c”. You want to combine the scores you have in your three layers, so you choose addition and enter the expression “a + b + c” into the score expression field.



To create the layer, you’ll click the “Create” button at the bottom of the section.



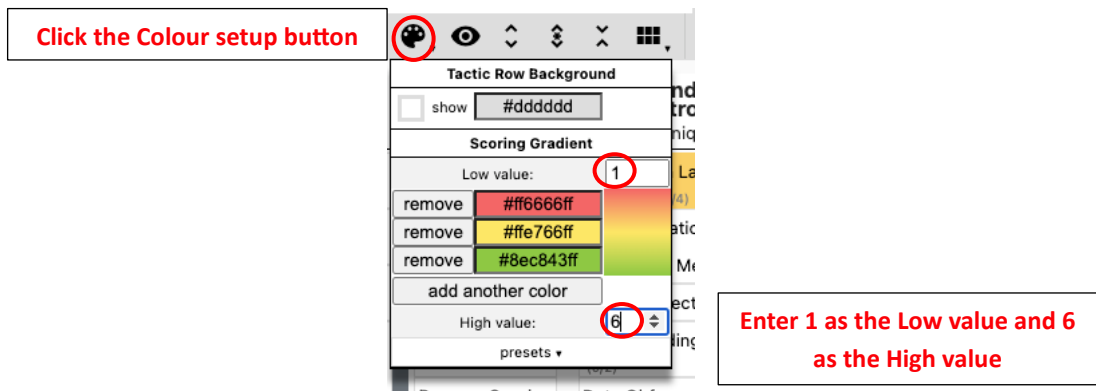
Now you have the combined layer. Initially, all the techniques may appear as various colours depending on the colour setup.



However, if you scroll over techniques, you’ll see that some techniques have a score of 1 (these are the ones used by APT29 only), some have a score of 2 (these are the

ones used by Ivanti only), and some of have a score of 3 (these are the ones only used by Infamous Chisel). While in some cases, they may have overlapped techniques (say the ones used by both APT29 and Ivanti).

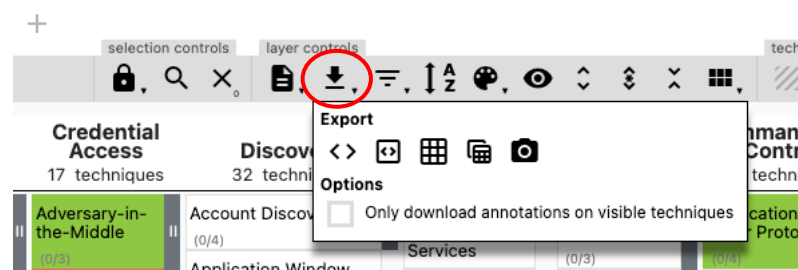
You can change the colours that appear for each score by clicking the “Colour setup” button. You know the values are 1, 2, and 3, so make the low value 1 and the high value 3. Navigator knows 2 is halfway between 1 and 3 so will automatically use the middle colour for the value of 2.



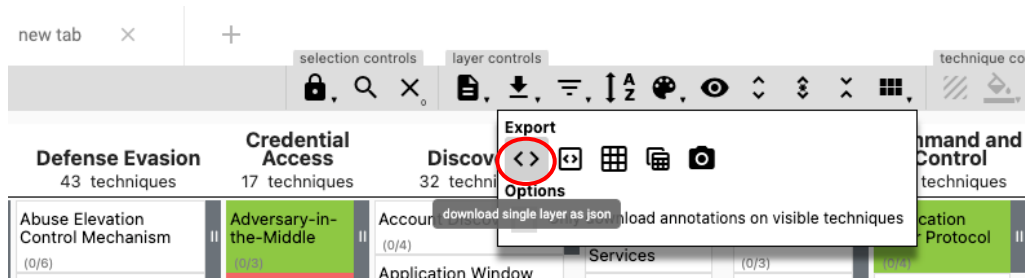
Now you can choose the colours you want for each layer. For instance, you can choose to make APT29 techniques (score = 1) yellow, Ivanti techniques (score = 2) blue, and Infamous Chisel (score = 3) red and their overlapped items like APT29 + Ivanti (score= 5) as green in order to convey that yellow plus blue makes green. You can use the default colours in Navigator or specify your own hex values/choose your own custom colours if you’d like.

- Export the layer in the format of your choice

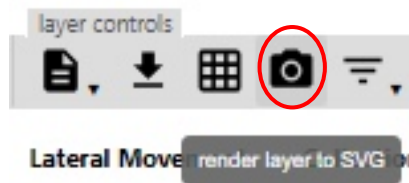
You have a couple options for how you can export the Navigator layer, and which one you choose will depend on how you want to work with it. You can export to Excel (arguably the best analyst tool of all time). This option will just export colours, not scores.



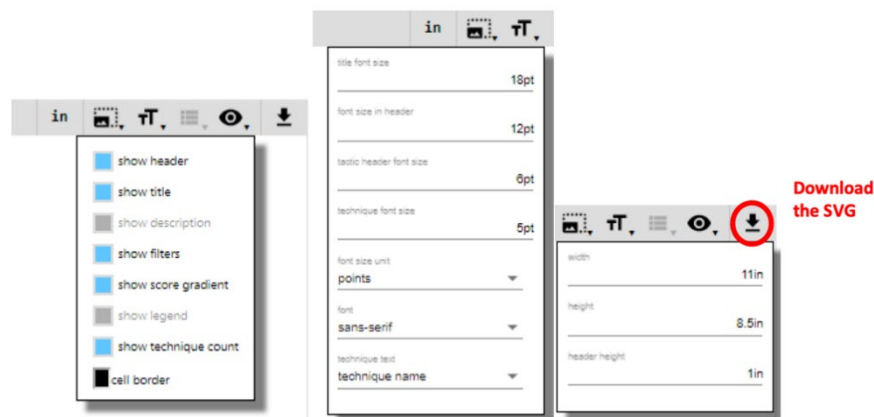
You can also download the layer as JSON, which might be useful if you want to script a layers ingest into another tool or save it for later manipulation in the Navigator.



Maybe you want to download it as an image for a PowerPoint so you can show off what you know about adversary groups. You can export the layer as an SVG image file.



As you export to SVG, you have lots of options on what you want to include as well as the format, text, size, etc. Click the download button to get a copy of your SVG to use however you see fit.



#### Questions:

1. What are the most common TTPs in three attack actors? If not, why?
2. What are the unique TTPs for each attack actors?
3. What procedures are utilised for the unique techniques in each case (listing 3 procedures with one procedure for each technique, in other words, 3 techniques for one attack actor)?
4. Following the above question (Q3), what might be the mitigation and detection methods? (List 2-3 techniques for each technique)

### 3. Ransomware Cases Study

In this part, we are going to further analyse the TTPs involved in ransomware. Ransomware is a common and dangerous type of malware. It works by locking up or encrypting your files so you can no longer access them. A ransom, usually in the form of cryptocurrency, is demanded to restore access to the files. Cyber criminals might also demand a ransom to prevent data and intellectual property from being leaked or sold online.

Similar to the procedure introduced in the previous sections, we will create three layers for the ransomware cases and further compare and analyse them. The links of the cases are provided as:

**LockBit:** <https://www.cyber.gov.au/about-us/advisories/understanding-ransomware-threat-actors-lockbit>

**Play Ransomware:** <https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/stopransomware-play-ransomware>

**BianLian:** <https://www.cyber.gov.au/about-us/advisories/stopransomware-bianlian-ransomware-group>

#### Questions:

5. What are the most common TTPs in ransomware attacks?
6. What are the unique TTPs for each ransomware attack case?
7. What procedures are utilised for the unique techniques in each case (listing 3 procedures with one procedure for each technique, in other words, 3 techniques for one attack actor)?
8. Following the above question (Q3), what might be the mitigation and detection methods? (List 2-3 techniques for each technique)

### 4. Summary of TTPs used to Target Australian Networks

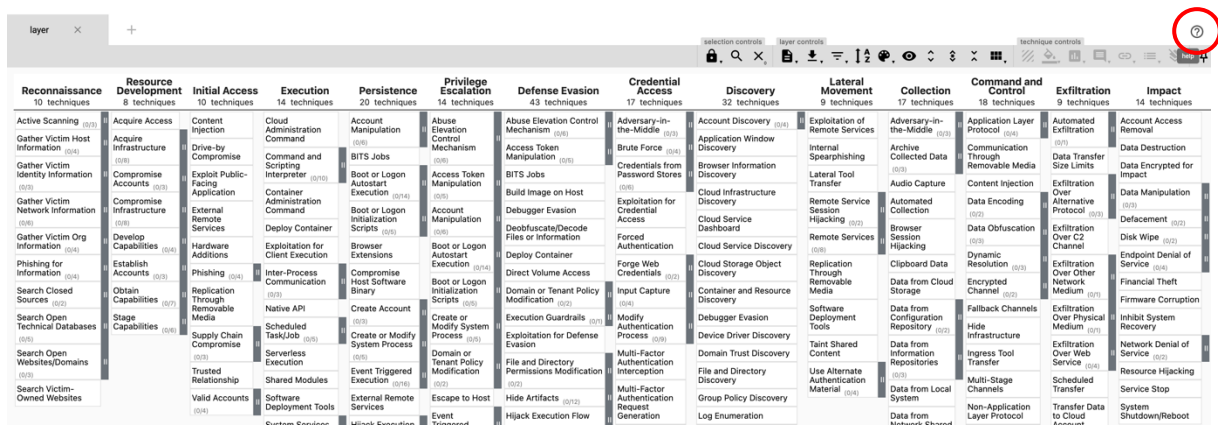
In this part, we are going to look into the summary of TTPs used to target Australian networks. The ACSC strongly recommends implementing ASD's Essential Eight. A review of investigations performed by the ACSC has shown that implementation of ASD's Essential Eight on victim networks would substantially reduce the risk of compromise by the adversary TTPs identified in this advisory <https://www.cyber.gov.au/about-us/advisories/summary-tactics-techniques-and-procedures-used-target-australian-networks>. Please generate a layer (named summary\_AUNet) for the TTPs involved in this advisory and trying to answer the questions below.

## Questions:

9. Comparing it with the previous two combined layers, what techniques are also listed in the layer we just created for the summary?
10. What procedures are utilised to implement these techniques, if possible, list with procedure examples?
11. Following the above question, what might be the mitigation and detection methods? (List 2-3 defence techniques for each)

Need more help with ATT&CK Navigator?

Just click the ? button in the upper right corner of the Navigator, and it will bring up much more detail on the above controls and more.



layer	Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Active Scanning	Active Scanning	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Adversary-in-the-Middle	Account Discovery	Exploitation of Remote Services	Adversary-in-the-Middle	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Gather Victim Host Information	Gather Victim Host Information	Acquire Infrastructure	Drive-by Compromise	Command and Scripting Interpreter	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Brute Force	Application Window Discovery	Internal Spearphishing	Archive Collected Data	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information	Gather Victim Identity Information	Compromise Accounts	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution	Access Token Manipulation	Access Token Manipulation	Credentials from Password Stores	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Gather Victim Network Information	Gather Victim Network Information	Compromise Infrastructure	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts	Account Manipulation	Account Manipulation	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking	Automated Collection	Data Encoding	Exfiltration Over C2 Channel	Data Manipulation
Gather Victim Org Information	Gather Victim Org Information	Develop Capabilities	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	Forged Authentication	Cloud Service Dashboard	Remote Services	Browser Session Hijacking	Data Obfuscation	Exfiltration Over Other Network	Defacement
Phishing for Information	Phishing for Information	Establish Accounts	Phishing	Inter-Process Communication	Compromise Host Software Binary	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Input Capture	Cloud Storage Object Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution	Exfiltration Over Other Network	Disk Wipe
Search Closed Sources	Search Closed Sources	Obtain Capabilities	Replication Through Removable Media	Native API	Create Account	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Domain or Tenant Policy Modification	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel	Exfiltration Over Physical Medium	Endpoint Denial of Service
Search Open Technical Databases	Search Open Technical Databases	Stage Capabilities	Scheduled Task/Job	Serverless Execution	Create or Modify System Process	Domain or Tenant Policy Modification	Domain or Tenant Policy Modification	Execution Guardrails	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository	Fallback Channels	Exfiltration Over Physical Medium	Firmware Corruption
Search Open Websites/Domains	Search Open Websites/Domains	Supply Chain Compromise	Serverless Execution	Shared Modules	Event Triggered Execution	File and Directory Permissions Modification	File and Directory Permissions Modification	Exploitation for Defense Evasion	Device Driver Discovery	Use Alternate Authentication Material	Data from Information Repositories	Hide Infrastructure	Exfiltration Over Web Service	Network Denial of Service
Search Victim-Owned Websites	Search Victim-Owned Websites	Trusted Relationship	Software Deployment Tools	Valid Accounts	External Remote Services	Hide Artifacts	Hide Artifacts	Multi-Factor Authentication Request Generation	File and Directory Discovery	Data from Local System	Multi-Stage Channels	Scheduled Transfer	Resource Hijacking	Service Stop
									Log Enumeration	Data from Network Channel	Non-Application Layer Protocol	Transfer Data to Cloud	System Shutdown/Reboot	