



# Security workshop ISGC 2023

**Sven GABRIEL, Nikhef, EGI CSIRT**



# Introduction to the Security Workshop ISGC-2023

- Risk Management
- Security Service Challenge
- Forensics exercise (Remote)
- Threat Intelligence and Security Operations Centers

# Risk Management

## Subsection 1

# Introduction to the introduction

# Security Teams, ... a look back <sup>1</sup>



Communications on security related matters require trust between the communication endpoints. Trust is in organizations and in peers (individuals)

- Trust groups
  - Higher base trust.
  - Fragile, maintenance depends on individuals.
  - Limited in growth.
- Organisations, Network of CERTs/CSIRTs
  - Lower base trust, communicating to groups you do not personally know.
  - Endpoint description in official templates (RFC-2350)
  - (Checked) Canonical contact addresses like [abuse@](#), [security@](#), [postmaster@](#), [rfc2142](#)
  - Maintained contact information available in directories

Until 1973 no standardized emergency phone numbers existed.

- Response times unnecessarily slow.
- Deadly traffic accident of a 8 year old kid in 1969 triggered an initiative to standardise it.
- Instead of checking a phone book to find the local emergency number, just call 112.

Since Feb. 1991 the same emergency number 112 is in place in all EU member states, EFTA, ...

You usually don't call a colleague and ask for an introduction to one of the local firefighters, you call 112.



# Emergency contacts, use the system

Translated to the situation in IT emergency response ...

- Use the standard contact addresses.
- If they do not meet the standards wrt response times, confidentiality, report it to coordinating bodies (TF-CSIRT, FIRST, NREN-CERTs).
- ... as you would in case that calling 112 does not lead to the expected result.

# Subsection 2

## **Introduction**

- Decision making process
  - Reflecting systems, conscious/controlled.
  - Automatic system/gut feeling, interpretations, auto correction.
- Decision making and Information Security Projects
  - Information systems are complex, to get to quick results often "gut feeling" approaches, "drive-by risk assessment" is used.
  - Doing incident response activates the "reflecting system". (*Oh look, this log file entry looks interesting ...*).
  - Implementing a Risk management system requires you to reflect on your security posture.

# Incident Response, Reflecting system, and all the Rest

When doing incident response, you usually ask:

- Why could this incident happen? (Status of your security controls).
- Why wasn't it detected? (Status of your sensors)
- How can we prevent the same incident from happening again?

Risk and Vulnerability Management is a wide area. We will only have a generic view on Risk Management and some hints why this would be very helpful for the organisations Operational Security team. As for vulnerability management we will take a look on how its done in EGI.

A much more complete online training on Vulnerability Management is available at GÉANT:

[https://learning.geant.org/  
domain-name-system-dns-protection-operational-network-](https://learning.geant.org/domain-name-system-dns-protection-operational-network-)

A lot material from: S. Klipper, Information Security Risk Management: Risikomanagement mit ISO/IEC 27001, 27005 und 31010 (2015).

## Subsection 3

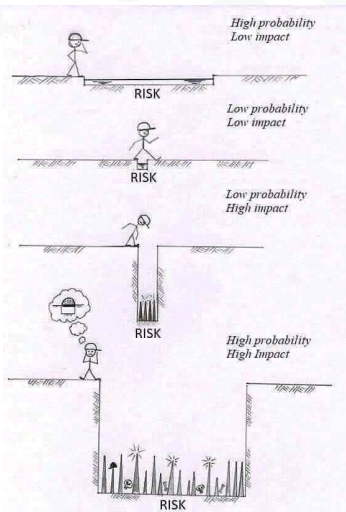
# Towards Risk Management

Definitions of Risk in context of Risk management:

- Old: chance or probability of loss (assets)
- New: effect of uncertainty on (reaching the) objectives (of an organisation) (ISO 31k).

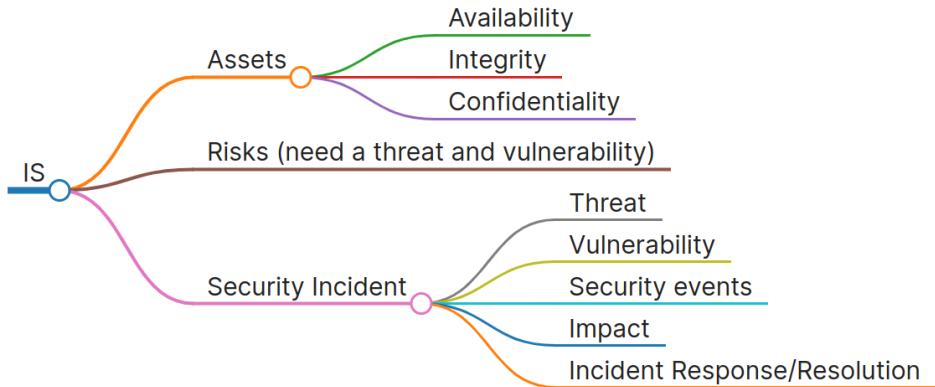
Risk Management is management of an organisation while taking into account the risks.

# Towards Risk management Process





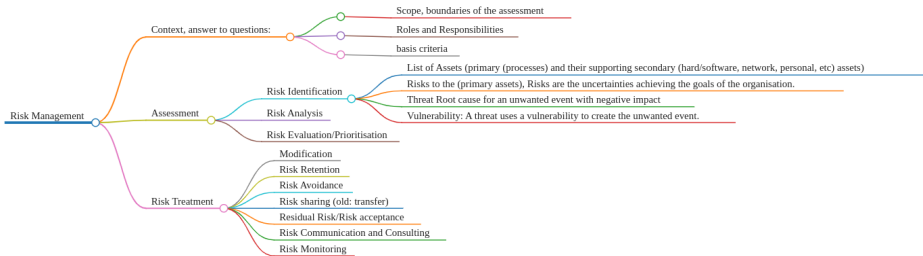
# Towards Risk management Process, add-hoc Information Security

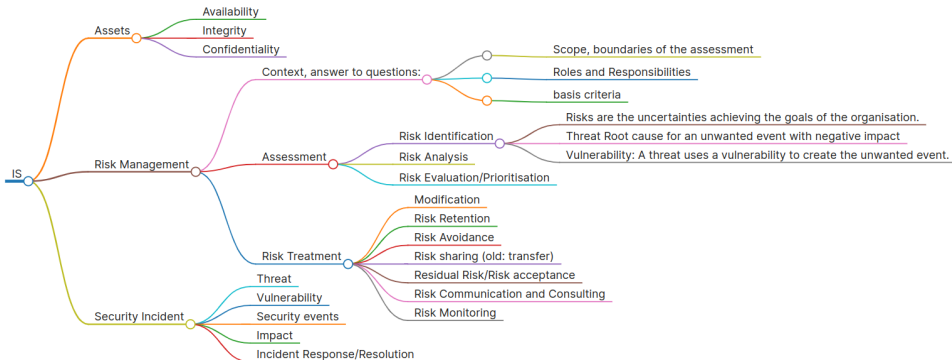


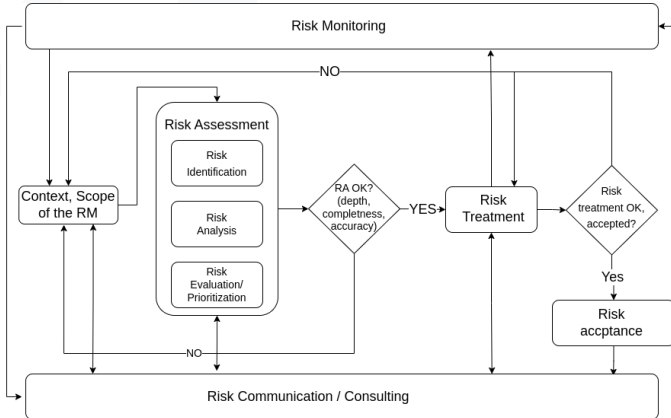
# ad-hoc IS management, questions

- What was the impact? were you just lucky that not more happened? or ...
- Do you really know your assets?
- Do you really know the risks to your assets?
- Did you know the affected entities in your organisation?
- Could you do proper communications related to the incident?
- If these left a nagging feeling with you, continue ...

# Risk management Process







2

# Risk, Threats and all the rest

When entering the Risk Assessment, one needs to identify risks. Threats are a component of Risks, therefore

...

## Oh Dear, a lot input needed

To implement a Risk Management Process a lot of information is needed, good thing ISO 2700{1,2,5} and 31010 can help. .

- 27005 Information Security Risk Management (Annex on Threats, Vulnerabilities.)
- ENISA ThreatLandscape
- SANS YYYY Top New Attacks and Threat Report (also Controls)
- <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

Monitoring of the Risk Management Process requires current input on threats and security controls.

# Risk, Threats and all the rest

- STRIDE: A model of what can go wrong:
- Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege.
- Is used in threat modelling, see Adam Shostack's book Threat Modeling: Designing for Security  
<https://shostack.org> or  
<https://www.youtube.com/watch?v=DMFF8zQqEVQ>



# Threats a card game

Elevation of privilege, threat modelling card game for developers.



Not prepared yet, please come back later this year . . .

<https://attack.mitre.org/> MITRE ATT&CK is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. From here you get information on:

- Which APT group is focusing on your sector?
- What is their motivation?
- What are the typical attacks, tools (threats) they use to exploit the resp. vulnerabilities.

- Pick an organisation,
- Set up context,
- Find Threats to this organisations Assets.
- **Threat modeling in security operations**

A first version in the Hands-On, please come back next year for a more complete versio . . .

# Why Risk management?

Leverage the outcome of a Risk Assessment, examples

- To get started, . . . lets look at the debriefing of a successful ransom attack and the problems you may run into, like:
- How to prioritize what systems to bring back first. (Business Continuity Plan)
- What is lost? GDPR relevant data loses need to be reported to the authorities.
- do useable back-ups of **important** (for business continuity) datasets exist?
- Note, at this stage its not about what security controls failed.
- Risk analysis helps to know your assets and protective measures in place

## Subsection 4

# Preparation for Risk Analysis

# What is Risk Analysis?

Risk Analysis is a process. An objective analysis of the effectiveness of the current security controls that protect an organization's assets and a determination of the probability of losses to those assets. <sup>3</sup>

When doing it for an organisation, this is rather a project with involvement of senior management and other key-personal.

At the end of this project the Risk Management Process should be started.

---

<sup>3</sup>The Security Risk Assessment Handbook A Complete Guide for Performing Security Risk Assessments, Douglas J. Landoll  
Security workshop ISGC 2023

# Phases/Steps in Risk Analysis

There are multiple methods and frameworks available for Risk Management <sup>4</sup>. Remember, this is a project which requires the usual project management (with senior management contribution/support). The methods differ in details/organisation of the following phases. Which method to use is also subject to the goal of the Risk assessment (Compliance with security regulations, ISO-27K, NIST-800, etc)

---

<sup>4</sup><https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-framework>



Large parts of the info gathering is already done in the project planning part. Information Gathering, Identify:

- Assets, Primary Assets (Business Processes), Secondary Assets (Hardware, Software, Personal/Experts, Data Sets/Bases) supporting the primary Assets, are used in the processes.
- Threats, use OSINT, see also the hands-on <sup>5</sup>.
- identify Critical systems (ex. systems that automate critical business functions)

---

<sup>5</sup><https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends>

## Get Info on available Controls

- Administrative (policies, procedures)
- Technical (Design, Architecture, Configuration, AuthNZ)
- Physical (physical access control, CCTV etc)

# Subsection 5

## **Risk Analysis**

Bringing together the gathered data/information.

- Asset valuation, example: Low (little to no impact), Medium, High, Critical (Indicates that compromise of the asset would have grave consequences). Various valuation approaches.
- Threat and Vulnerability mapping,
- Risk Calculation. (Here the above information is used to get a qualitative (low, moderate, high) or quantitative value)
- Risk Mitigation: Safeguard selection, Safeguard effectiveness(cost-value ratio)

- Safeguard/Control selection
- Safeguard/Control effectiveness (cost-value ratio)
- Risk reduction (improve existing controls, apply additional controls)
- Result: Residual security risk (that remains after implementation of recommended safeguards). This will be treated in the next step.

Senior manager must decide to reduce the security risk, accept the residual security risk, or delegate the security risk to someone else (example: insurance).

- Risk transfer.
- Risk acceptance.
- Risk assignment.

The Risk assessment report will help the Operational Security team to prioritize the available resources to:

- Security Monitoring (ex. access control)
- System audits, log processing, alerting
- Back-up Strategy

# Threat Modelling with MITRE ATT&CK



# Subsection 1

## **MITREATT&CK**

<https://mitre-attack.github.io/attack-navigator/>

The screenshot displays the MITRE ATT&CK Navigator tool interface. The tool is organized into a grid of columns representing different attack phases and sub-phases. The columns include:

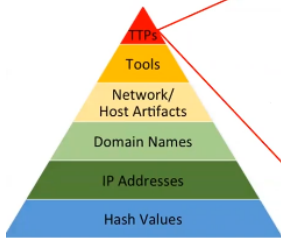
- Reconnaissance (Discovery, Active Directory Enumeration, etc.)
- Resource Development (Compromise Account, etc.)
- Initial Access (Exploit Public-Facing Application, etc.)
- Execution (Command and Control, etc.)
- Persistence (Account Manipulation, etc.)
- Privilege Escalation (Exploit Vulnerability, etc.)
- Defense Evasion (Application Whitelisting, etc.)
- Credential Access (Adversary Infiltration, etc.)
- Discovery (Network Discovery, etc.)
- Lateral Movement (Network Discovery, etc.)
- Collection (Active Directory Enumeration, etc.)
- Command and Control (Command and Control, etc.)
- Exfiltration (Data Exfiltration, etc.)

Each cell in the grid contains a list of specific attack techniques with their corresponding MITRE IDs. The interface also includes a search bar at the top right and a sidebar on the right for filtering and navigation.

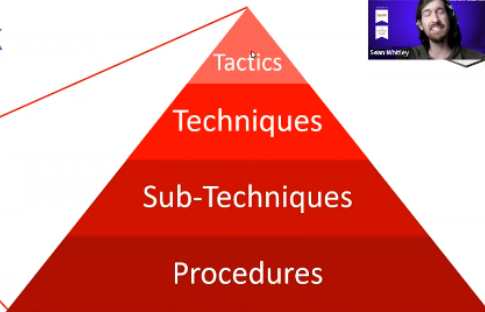
MITRE ATT&CK Matrices capture the relationship between:

- Tactics (Column headers), Represent (intermediate) goals of an adversary, for example lateral movement.
- Techniques (Column entries)
  - are the means/tools how the adversary achieve their goals/tactics
  - are written/used by the adversaries, entries describe and capture how an adversary performs each action or behaviour.
  - Subtechniques describe adversary behaviour at a lower level then the resp. technique.
  - are often platform specific, Example: Technique = Command + Scripting Interpreter, the Subtechniques are: Powershell . . . Windows; Unix shell . . . Unix; python, Javascript . . . Cross platform.

## TTPs of ATT&CK



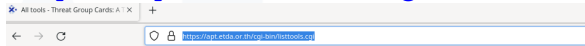
<https://advent-response.blogspot.com/2015/03/no-parent-of-gain.html>



CYBRARY

<https://www.youtube.com/watch?v=1cCt2XZr2ms>

<https://apt.etda.or.th/cgi-bin/listtools.cgi>



**ETDA** สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์  
Electronic Transactions Development Agency

Groups Tools Search Statistics



home > List all tools

Search

## Threat Group Cards: A Threat Actor Encyclopedia

### All tools

Changed	Name
<b>Tools</b>	
	3102 RAT
	3PARA RAT
	3proxy
	3Rat Client
	404-Input-shell web shell
	4H RAT, 4h_rat
	7Logger
	7-Zip













<https://apt.eta.dor.th/cgi-bin/listtools.cgi>

### Database search

<b>Actor</b>	Source country	...
	Victim country	Netherlands <input type="checkbox"/> or Worldwide
	Victim sector	Education
	Motivation	...
	Free text search	<input type="text"/> (can use '*' and '?' wildcards)
		<input type="button" value="Search!"/>

<b>Tool</b>	Category	...
	Type	...
	Free text search	<input type="text"/> (can use '*' and '?' wildcards)
		<input type="button" value="Search!"/>

<https://apt.eta.dor.th/cgi-bin/listgroups.cgi?c=&v=Netherlands&s=Education&m=&x=>

Changed	Name	Country	Observed
<b>APT groups</b>			
	APT 17, Deputy Dog, Elderwood, Sneaky Panda		2009-Sep 2017
	APT 29, Cozy Bear, The Dukes		2008-Oct 2022 ●
	APT 41		2012-Aug 2022 ●
	Circus Spider	[Unknown]	2019-Feb 2022 ●
	Cutting Kitten, TG-2889		2012-Mar 2016 ●
	Dark Caracal		2007-2020
	Desert Falcons	[Gaza]	2011-Nov 2021 ●
	Equation Group		2001-Aug 2016 ●
	FIN11	[Unknown]	2016-Dec 2022 🔥 ●
	MuddyWater, Seedworm, TEMP.Zagros, Static Kitten		2017-Late 2021 ●
	Shadow Network		2010-2010 ●
	Sofacy, APT 28, Fancy Bear, Sednit		2004-Sep 2022 ●
	TeamSpy Crew		2010-Feb 2017
	Turla, Waterbug, Venomous Bear		1996-Sep 2022
<b>Other groups</b>			
	Fxmosp		2016-Jul 2020 ●

# MITREATT&CK, and OSINT

Use the APT group information from the previous step in MITREATT&CK ...



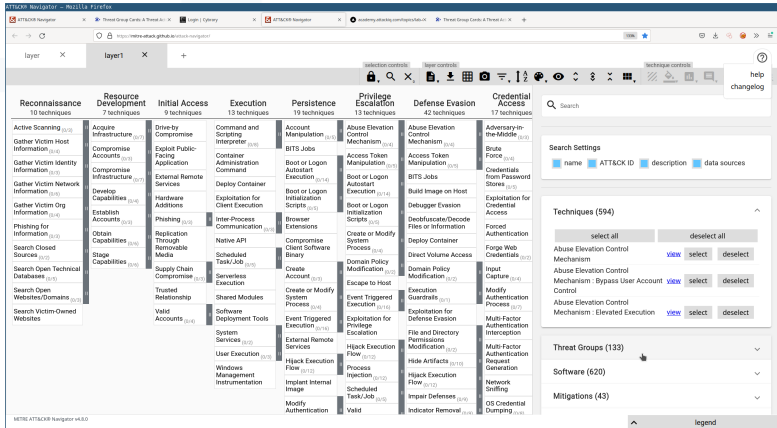
## MITRE ATT&CK® Navigator

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	^
<input type="button" value="Enterprise"/>	<input type="button" value="Mobile"/>	<input type="button" value="ICS"/>
<input type="button" value="More Options"/>		▼
Open Existing Layer	Load a layer from your computer or a URL	▼
Create Layer from other layers	Choose layers to inherit properties from	▼
Create Customized Navigator	Create a hyperlink to a customized ATT&CK Navigator	▼

# MITRE ATT&CK, New Layer



The screenshot displays the MITRE ATT&CK Navigator v4.8.0 interface. The main area shows a grid of technique categories, each with a count of techniques:

- Reconnaissance: 10 techniques
- Resource Development: 7 techniques
- Initial Access: 9 techniques
- Execution: 13 techniques
- Persistence: 19 techniques
- Privilege Escalation: 13 techniques
- Defense Evasion: 42 techniques
- Credential Access: 17 techniques

The 'layer1' view is active, showing a grid of techniques. The sidebar on the right includes:

- Search Settings: name, ATT&CK ID, description, data sources
- Techniques (594): select all, deselect all
- Threat Groups (133)
- Software (620)
- Mitigations (43)
- Legend

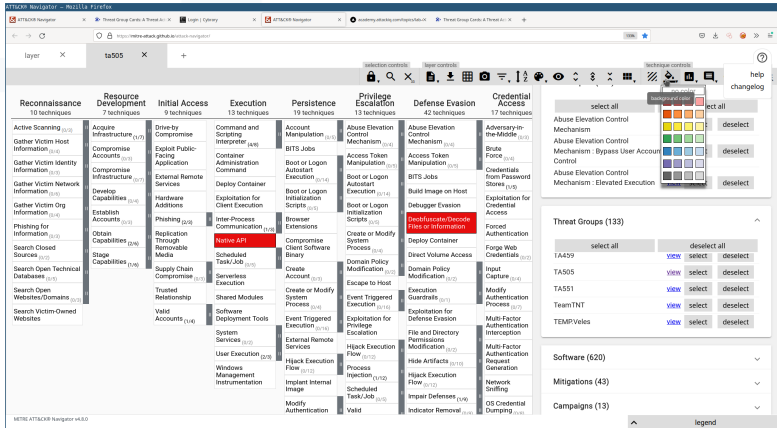
At the bottom of the interface, the text "MITRE ATT&CK Navigator v4.8.0" is visible.

# MITRE ATT&CK, New Layer

Screenshot of the MITRE ATT&CK Navigator v4.8.0 interface. The browser address bar shows the URL: <https://mitre-attack.github.io/mitre-attack-navigator/>. The interface displays a grid of attack techniques categorized into groups: Reconnaissance (10), Resource Development (7), Initial Access (9), Execution (13), Persistence (19), Privilege Escalation (13), Defense Evasion (42), and Credential Access (17). The 'Native API' technique under Persistence is highlighted in blue. On the right side, there are two panels: 'Threat Groups (133)' with a list of groups including TA459, TA505 (highlighted), TA551, TeamTNT, and TEMP/Veas; and 'Software (620)', 'Mitigations (43)', and 'Campaigns (13)'. A legend is visible at the bottom right of the right-hand panels.

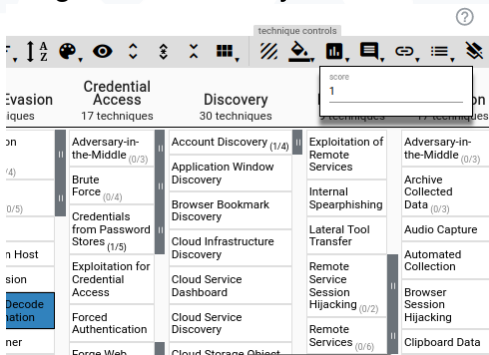
The screenshot displays the MITRE ATT&CK Navigator v4.8.0 interface. The main view is a grid of techniques categorized into columns: Reconnaissance (10), Resource Development (7), Initial Access (9), Execution (13), Persistence (19), and Privilege Escalation (13). A context menu is open over the 'appt1' technique, showing options like 'description', 'domain', 'Enterprise', 'version', 'add metadata', 'add links', 'Input Capture', 'Multi-Factor Authentication Interception', and 'OS Credential Dumping'. The right sidebar shows search settings and a list of techniques (594) and threat groups (133).

Category	Technique Name	Version	
Reconnaissance	Active Scanning	(3,10)	
	Gather Victim Host Information	(3,4)	
	Compromise Accounts	(3,11)	
	Gather Victim Identity Information	(3,12)	
	Compromise Infrastructure	(3,7)	
	Gather Victim Network Information	(3,14)	
	Gather Victim Org Information	(3,4)	
	Phishing for Information	(3,1)	
	Search Closed Sources	(3,7)	
	Search Open Technical Databases	(3,7)	
Resource Development	Acquire Infrastructure	(3,7)	
	Drive-by Compromise	(3,7)	
	Exploit Public-Facing Application	(3,11)	
	Develop Capabilities	(3,4)	
	Establish Accounts	(3,1)	
	Obtain Capabilities	(3,14)	
	Stage Capabilities	(3,4)	
Initial Access	External Remote Services	(3,7)	
	Hardware Additions	(3,14)	
	Phishing	(1,10)	
	Replication Through Removable Media	(3,10)	
	Supply Chain Compromise	(1,7)	
	Trusted Relationship	(3,10)	
	Valid Accounts	(3,10)	
	Software Deployment Tools	(3,10)	
	User Execution	(3,10)	
Execution	Command and Scripting Interpreter	(3,10)	
	Container Administration Command	(3,10)	
	Deploy Container	(3,10)	
	Exploitation for Client Execution	(3,11)	
	Browser Extensions	(3,10)	
	Native API	(3,10)	
	Scheduled Task/Job	(1,10)	
	Serverless Execution	(3,10)	
	Shared Modules	(3,10)	
	System Services	(1,10)	
	User Execution	(3,10)	
	Windows Management Instrumentation	(3,12)	
	Persistence	Account Manipulation	(3,10)
NTS Jobs		(3,10)	
Boot or Logon Autostart Execution		(1,14)	
Boot or Logon Initialization Scripts		(3,11)	
Browser Extensions		(3,10)	
Compromise Client Software Binary		(3,10)	
Create Account		(3,10)	
Create or Modify System Process		(1,14)	
Event Triggered Execution		(1,14)	
External Remote Services		(3,10)	
Hijack Execution Flow		(3,12)	
Implant Internal Image		(3,10)	
Modify Authentication		(3,10)	
Privilege Escalation		Abuse Elevation Control Mechanism	(3,4)
		Access Token Manipulation	(3,7)
		Boot or Logon Autostart Execution	(1,14)
		Boot or Logon Initialization Scripts	(3,11)
		Create or Modify System Process	(1,14)
		Domain Policy Modification	(3,11)
	Escape to Host	(3,10)	
	Event Triggered Execution	(1,14)	
	Exploitation for Privilege Escalation	(3,10)	
	Hijack Execution Flow	(3,12)	
	Process Injection	(3,10)	
	Scheduled Task/Job	(1,10)	
	Indicator Removal	(1,14)	



The screenshot displays the MITRE ATT&CK Navigator v4.8.0 interface. The main area is a grid of attack techniques, organized into columns representing different stages of an attack: Reconnaissance (10 techniques), Resource Development (7 techniques), Initial Access (9 techniques), Execution (13 techniques), Persistence (19 techniques), Privilege Escalation (13 techniques), Defense Evasion (42 techniques), and Credential Access (17 techniques). A technique named 'Native API' is highlighted in red. On the right side, there is a 'Threat Groups (133)' section with a list of groups including TA459, TA505, TeamTNT, and TEMP/Veles. A color selection tool is also visible, allowing users to choose colors for different techniques.

Add a score value, for example 1 for all layers for equal weight in the overlay.



The screenshot shows the MITRE ATT&CK interface with a 'technique controls' toolbar at the top. A 'score' input field is highlighted, containing the value '1'. Below the toolbar, the interface is organized into columns representing different categories of techniques:

- Evasion** (17 techniques)
- Credential Access** (17 techniques)
- Discovery** (30 techniques)
- Exploitation of Remote Services** (17 techniques)

Techniques listed include:

- Adversary-in-the-Middle (0/3)
- Brute Force (0/4)
- Credentials from Password Stores (1/5)
- Exploitation for Credential Access
- Forced Authentication
- Force Web
- Account Discovery (1/4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object
- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (0/2)
- Remote Services (0/6)
- Adversary-in-the-Middle (0/3)
- Archive Collected Data (0/3)
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data

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

Choose layers to inherit properties from

domain \*

Enterprise ATT&CK v12

Choose the domain and version for the new layer. Only layers of the same domain and version can be merged.

Use constants (numbers) and layer variables (yellow, above) to write an expression for the initial value of scores in the new layer. A full list of supported operations can be found [here](#). Leave blank to initialize scores to 0. Here's a list of available layer variables:

score expression

a + b

- **a** (layer)
- **b** (layer1)
- **c** (layer)
- **d** (layer by operation)

## Subsection 2

# What to do with MITRE ATT&CK



## Use MITRE ATT&CK, for...

- Threat modelling with MITRE ATT&CK is certainly not complete.
- It depends on your (time consuming) OSINT, to get the groups that could possibly be interested in your assets.
- Still it will give you a pretty good start on ...

## Use MITRE ATT&CK, for...

- Data Sources (do you have the logs for the threats identified).
- Detection/analysis (sensors, where to place them)
- Mitigation (security controls)

As a result you get a good indication of your security posture against the groups, techniques in scope. Map it against your SOC settings/capabilities

Thanks for your attention, Questions?