Risk and Vulnerability Management

Sven Gabriel, Nikhef, EGI CSIRT

Oct 2023

Introduction to Risk and Vulnerability Management tCSC 2023

Risk and Vulnerability Management

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-

Risk Management

Subsection 1

How decisions are taken

Decision making processes

- Decision making process
  - Slow: Reflecting systems, conscious/controlled.
  - Quick: 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 Reflecting System kicks in, 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?

Subsection 2

Towards Risk Management

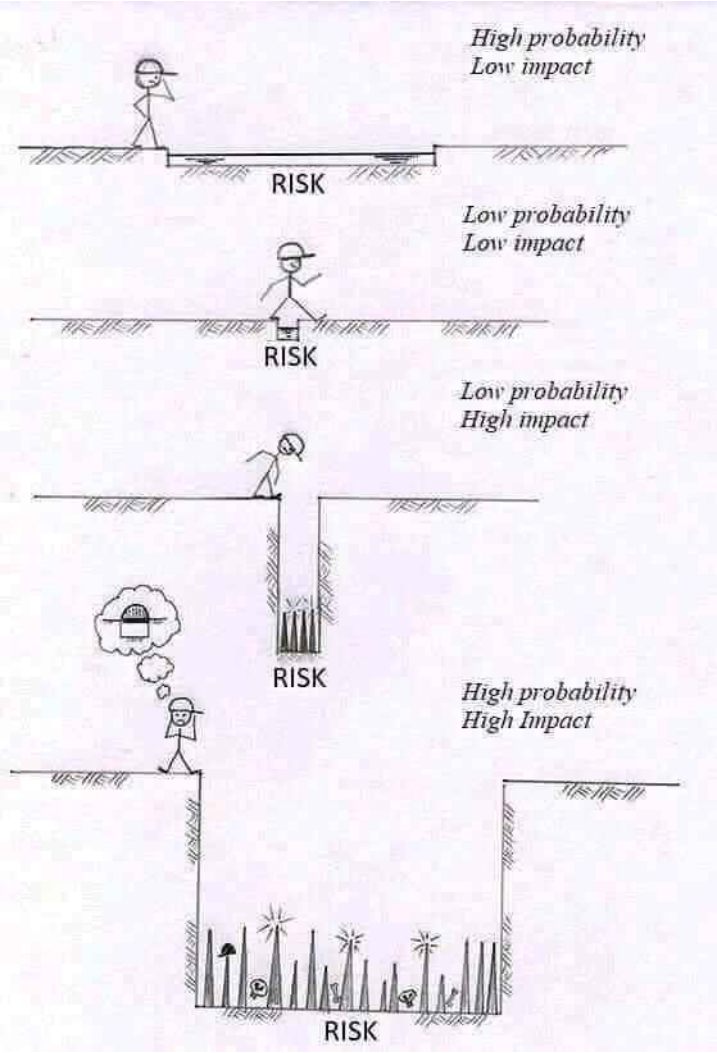
Risk

Definitions of Risk in context of Risk management:

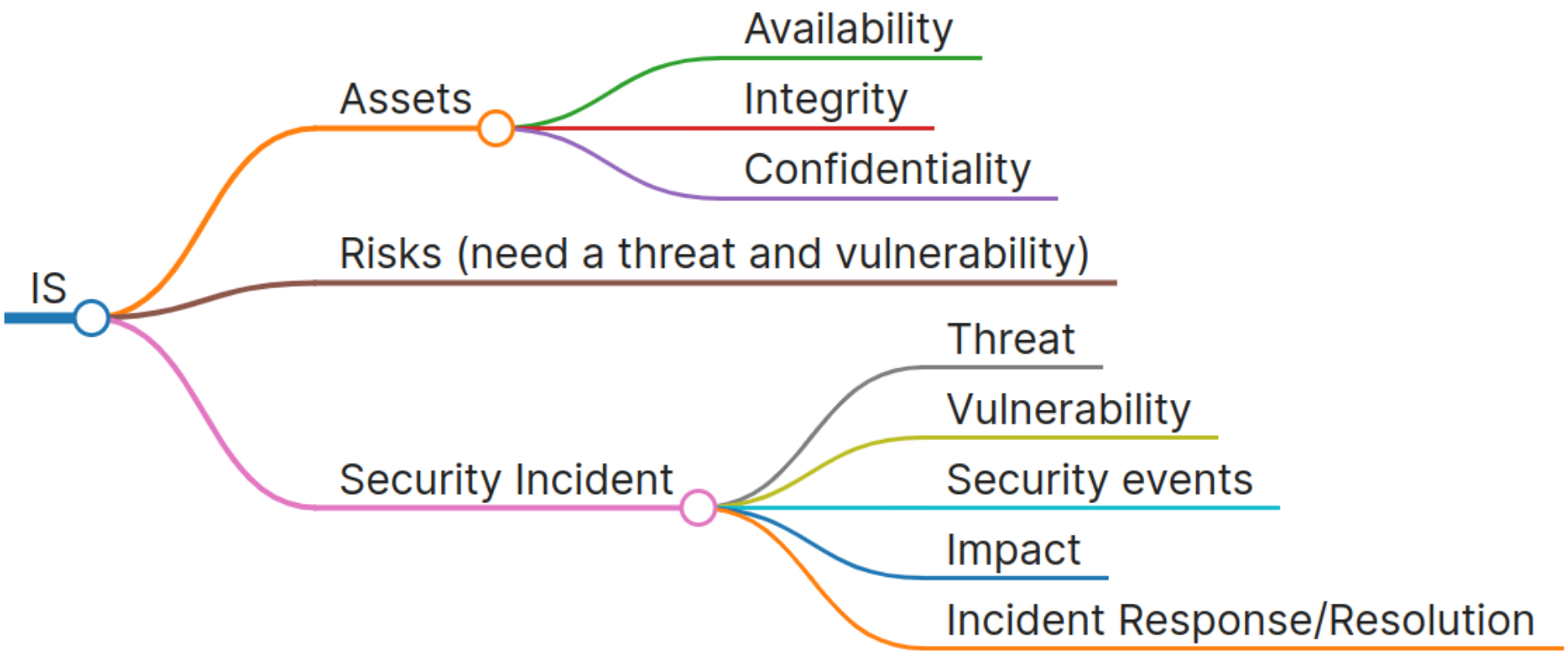
- Old: chance or probability of loss (assets)
- New: effect of uncertainty on (reaching the) objectives (of an organisation) (ISO 31k).

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

Towards Risk management Processs



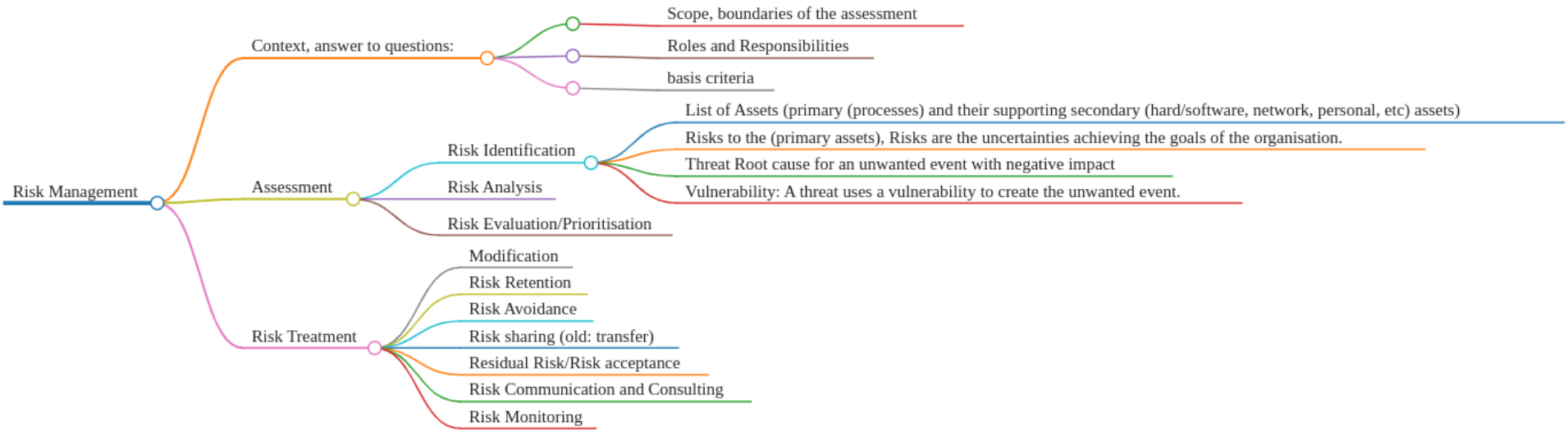
Towards Risk management Processs, add-hoc Information Security



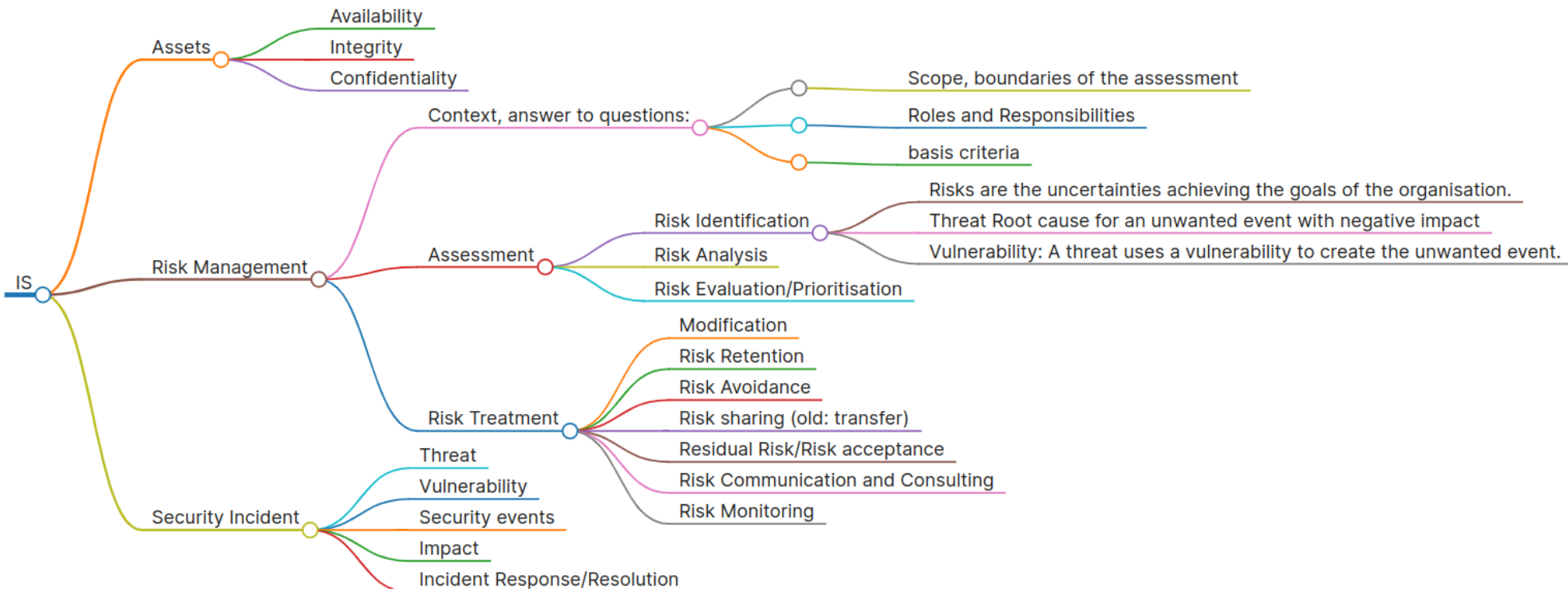
ad-hoc IS management, questions

- 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 ...

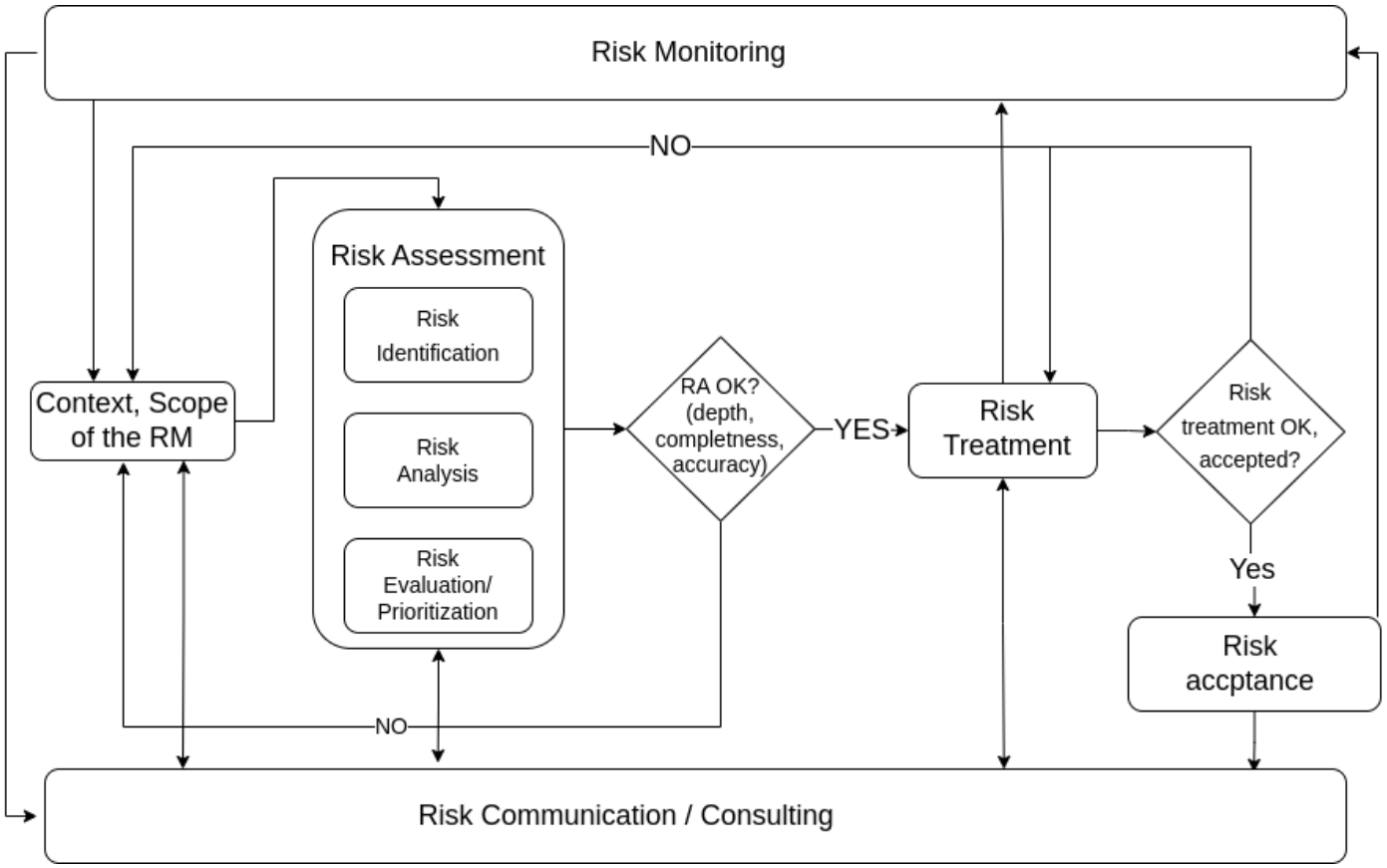
Risk management Process



Information Security Management



Risk management Process



[1]

[1] S. Klipper, Information Security Risk Management

Risk, Threats and all the rest

Risk can be expressed as:

$VxTxI = Risk$[2]

therefore . . . for a Risk to exist a Vulnerability and a Threat needs to exist.

[2] V: Vulnerability, T: Thread, I: Impact

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 . . .

MITRE ATT&CK

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.

Threat Modelling with MITRE ATT&CK

- 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

Incident Response for High impact incident

- 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 3

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. [3]
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.

[3] The Security Risk Assessment Handbook A Complete Guide for Performing Security Risk Assessments, Douglas J. Landoll

Phases/Steps in Risk Analysis

There are multiple methods and frameworks available for Risk Management [4]. 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)

[4] https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-framework

Info Gathering Phase

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 [5].
- identify Critical systems (ex. systems that automate critical business functions)

[5] 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 4

Risk Analysis

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)

Risk mitigation

- 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.

Recommendations, Reporting and Resolution

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.

Finally

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

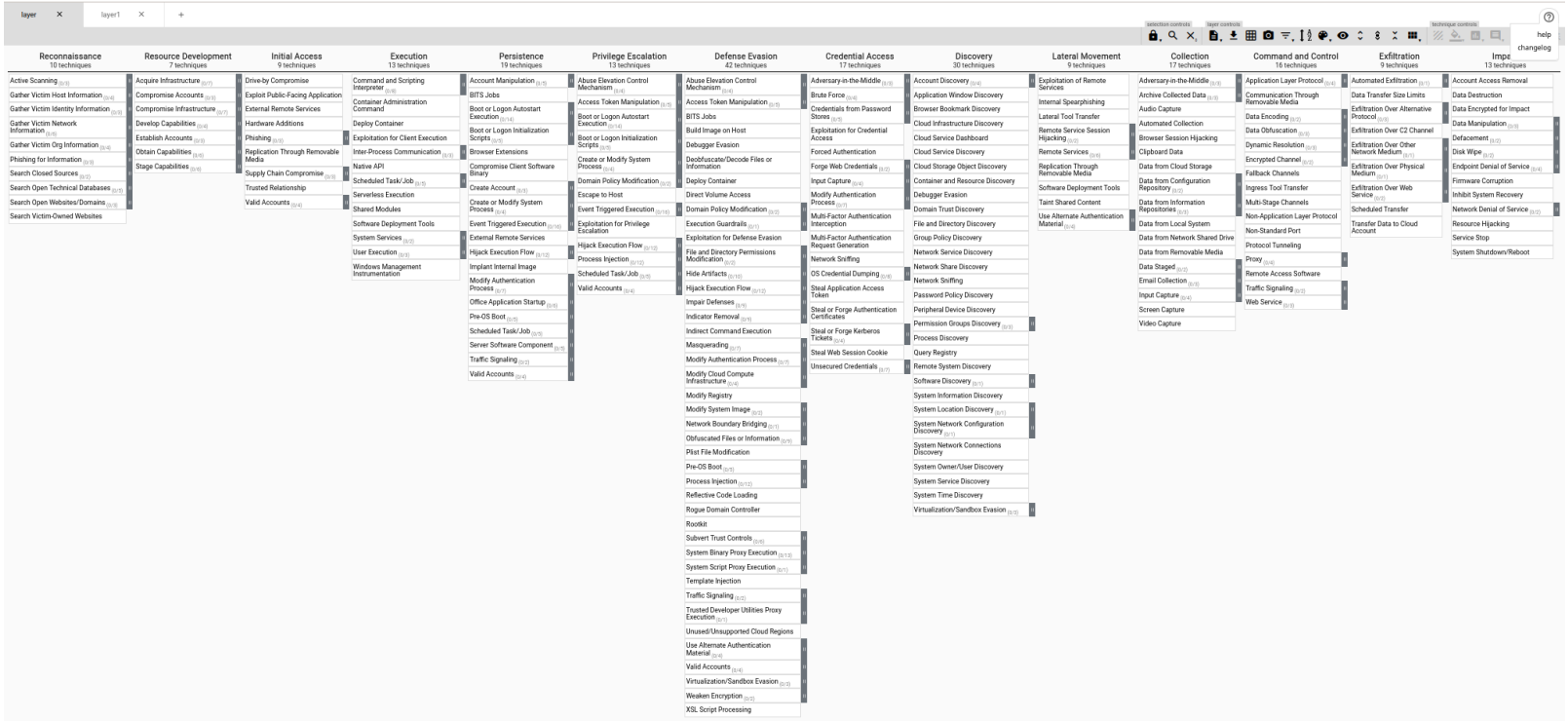
Threat Modelling with MITRE ATT&CK

Subsection 1

MITREATT&CK

MITRE ATT&CK

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

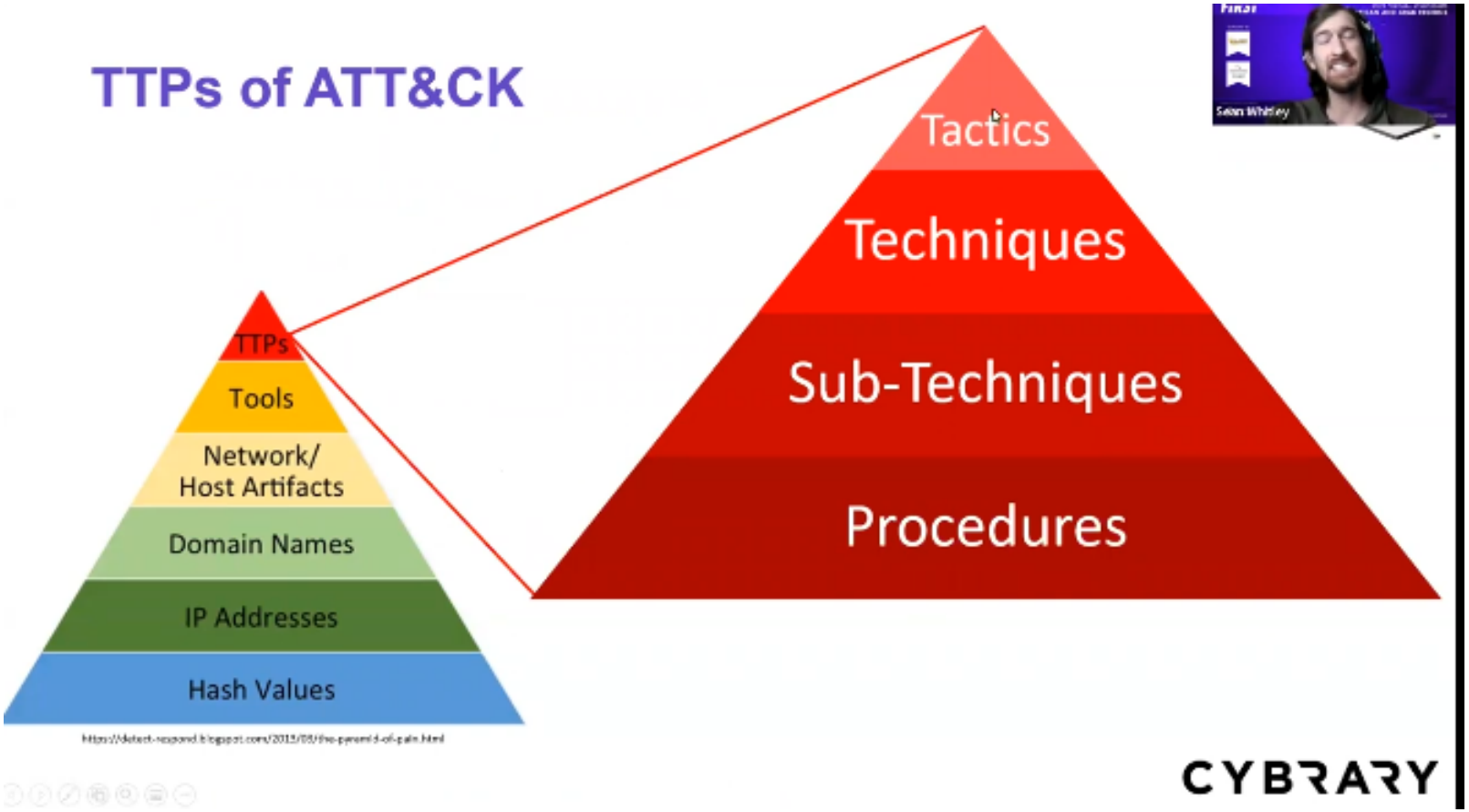


MITRE ATT&CK

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.

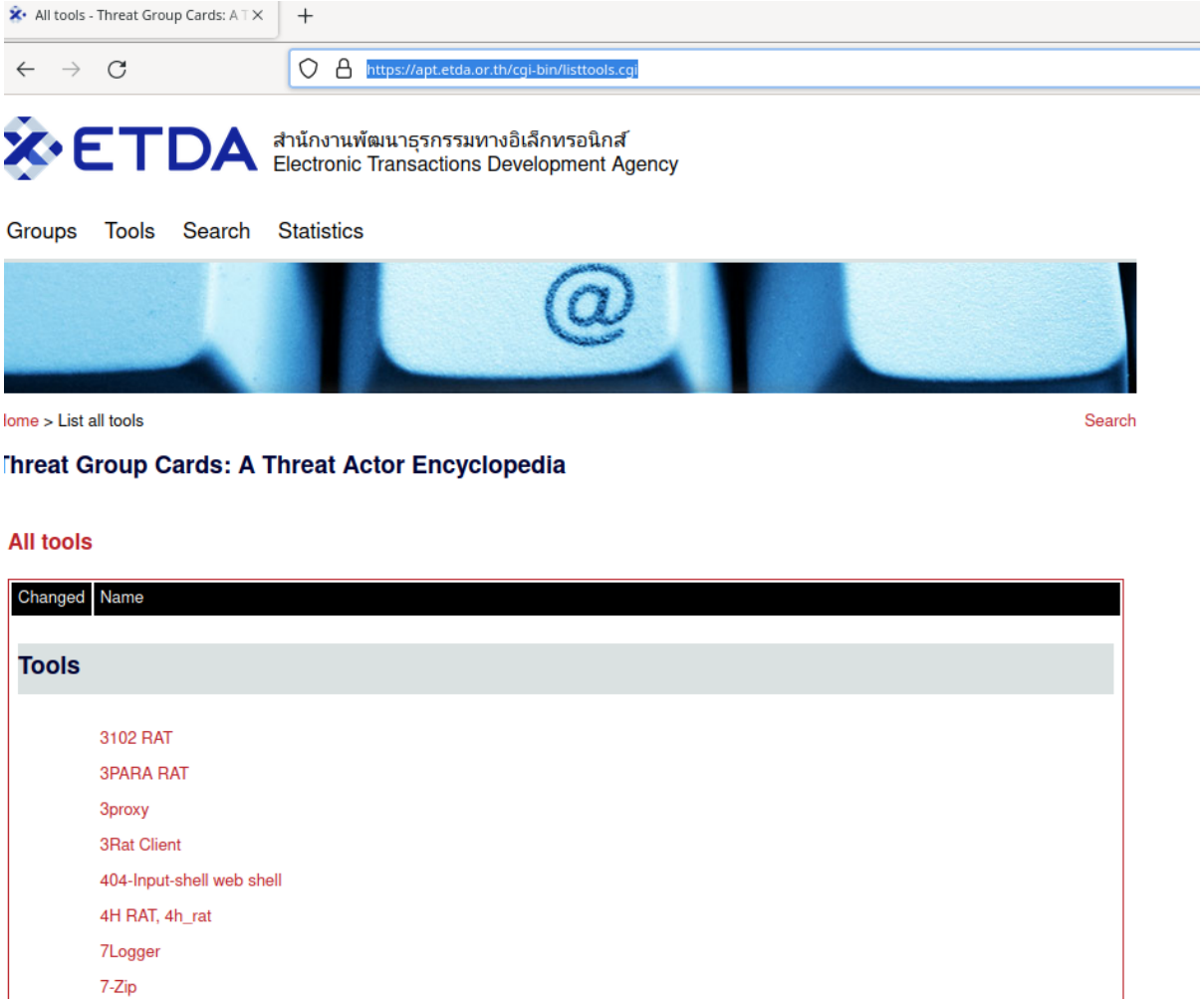
MITREATT&CK



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

OSINT

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



OSINT

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

Database search

Actor	Source country	...
	Victim country	Netherlands ☐ or Worldwide
	Victim sector	Education
	Motivation	...
	Free text search	(can use '*' and '?' wildcards)
		Search!

Tool	Category	...
	Type	...
	Free text search	(can use '*' and '?' wildcards)
		Search!

OSINT

https://apt.etda.or.th/cgi-bin/listgroups.cgi?c=&v=Netherlands&s=Education&m=&x=

Changed	Name	Country	Observed
APT groups			
	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
Other groups			
	Fxmsp		2016-Jul 2020

MITREATT&CK, and OSINT

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

MITREATT&CK, New Layer

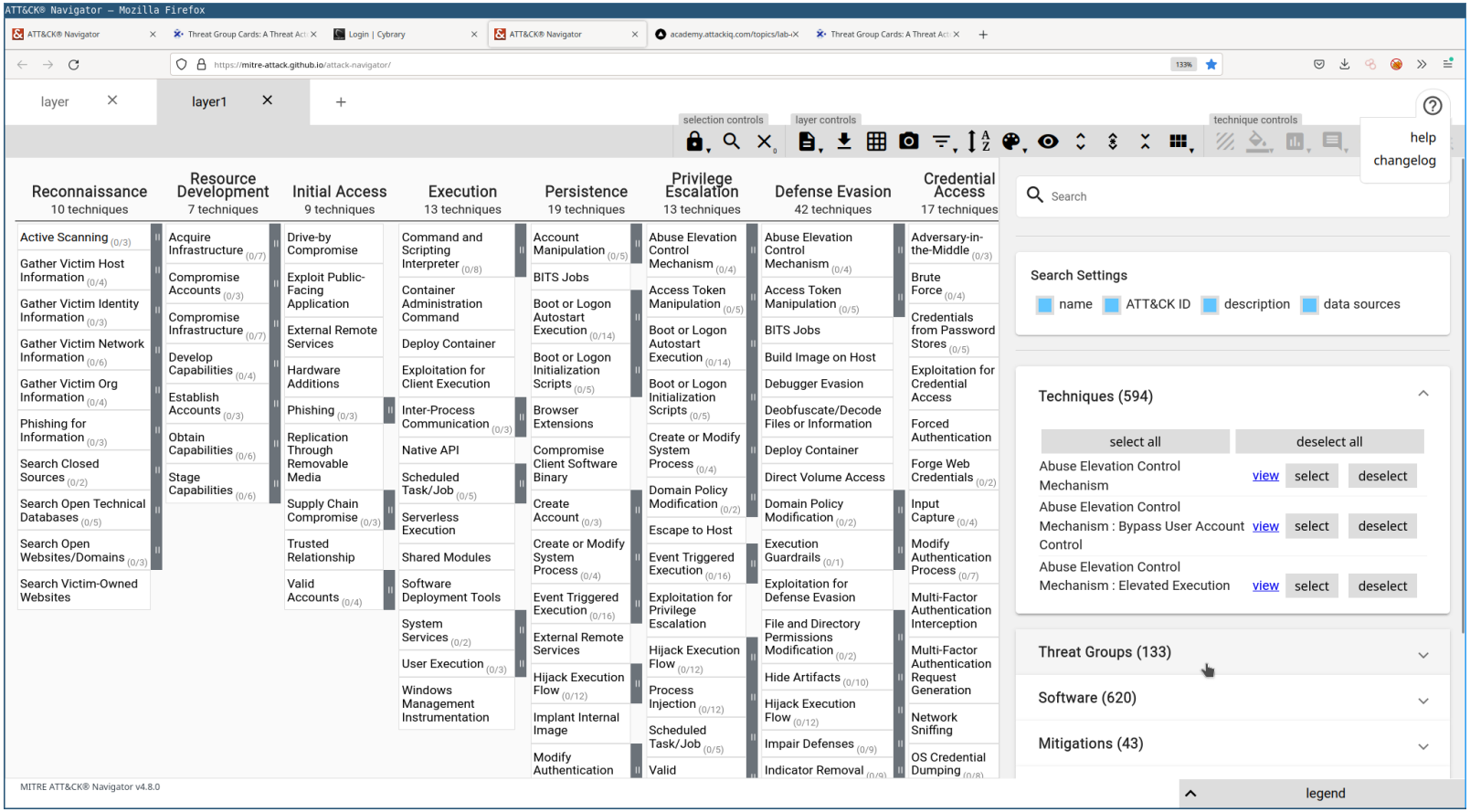
MITRE ATT&CK® Navigator

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.

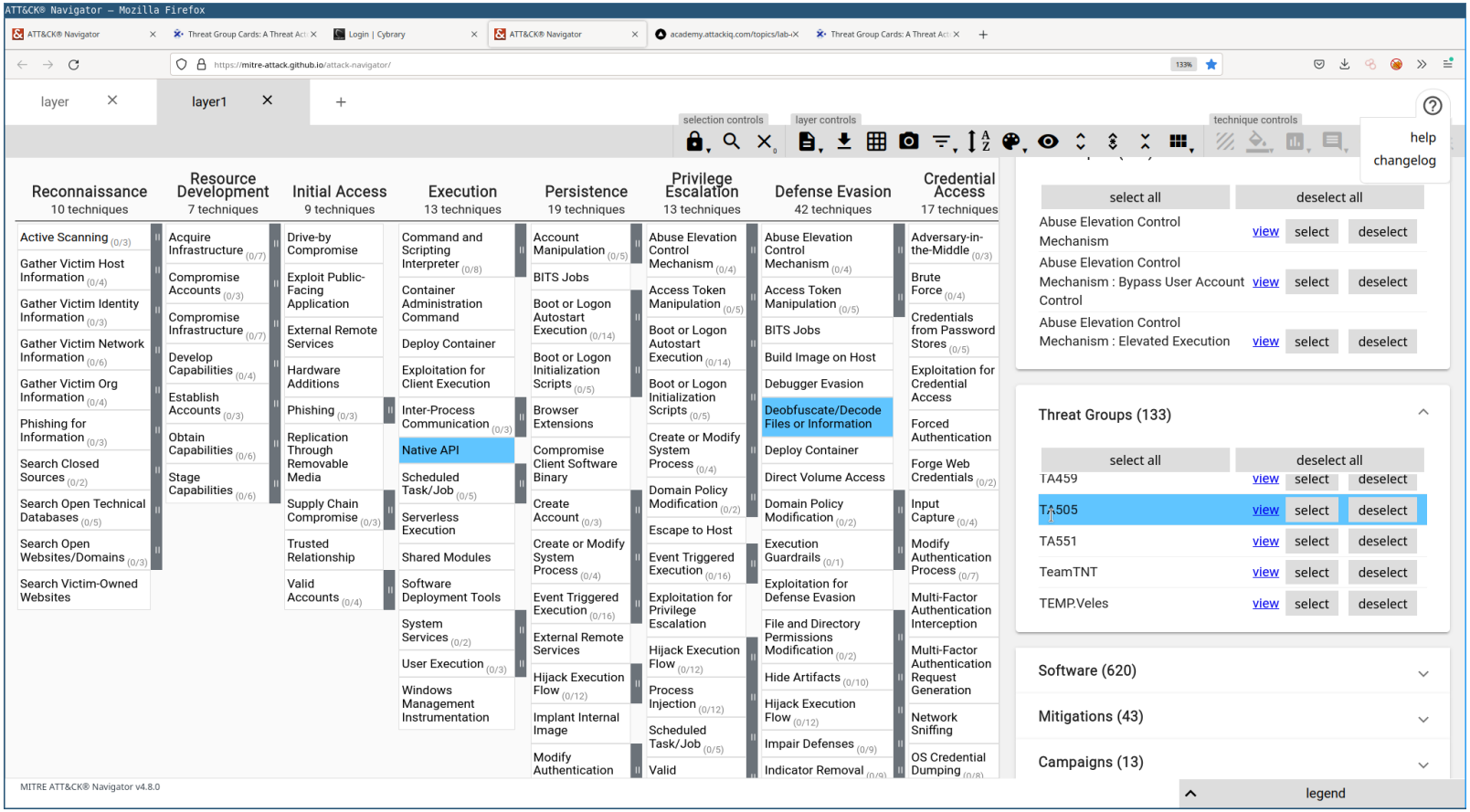
help changelog theme ▾

Create New Layer	Create a new empty layer	^
Enterprise	Mobile	ICS
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	⌄

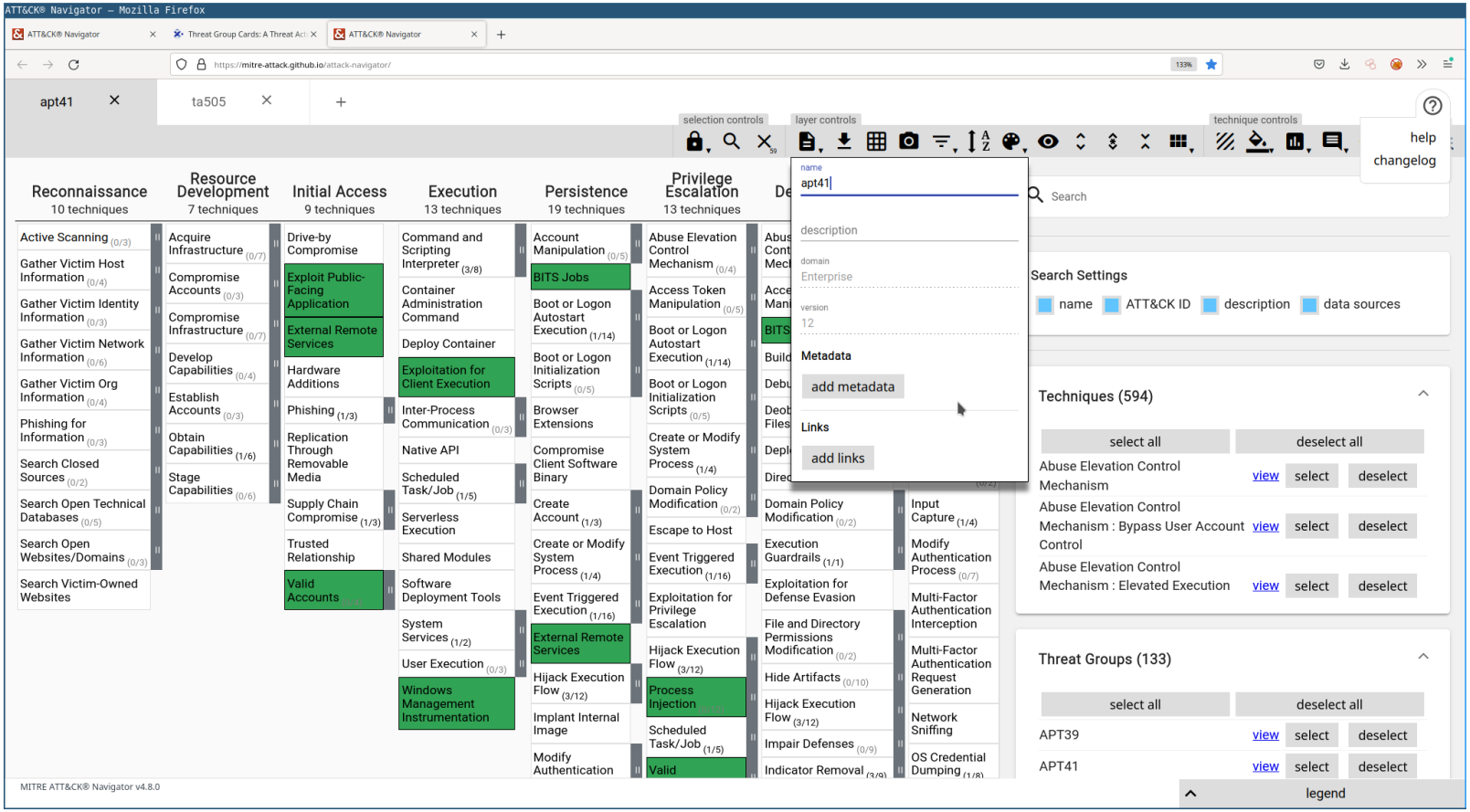
MITREATT&CK, New Layer



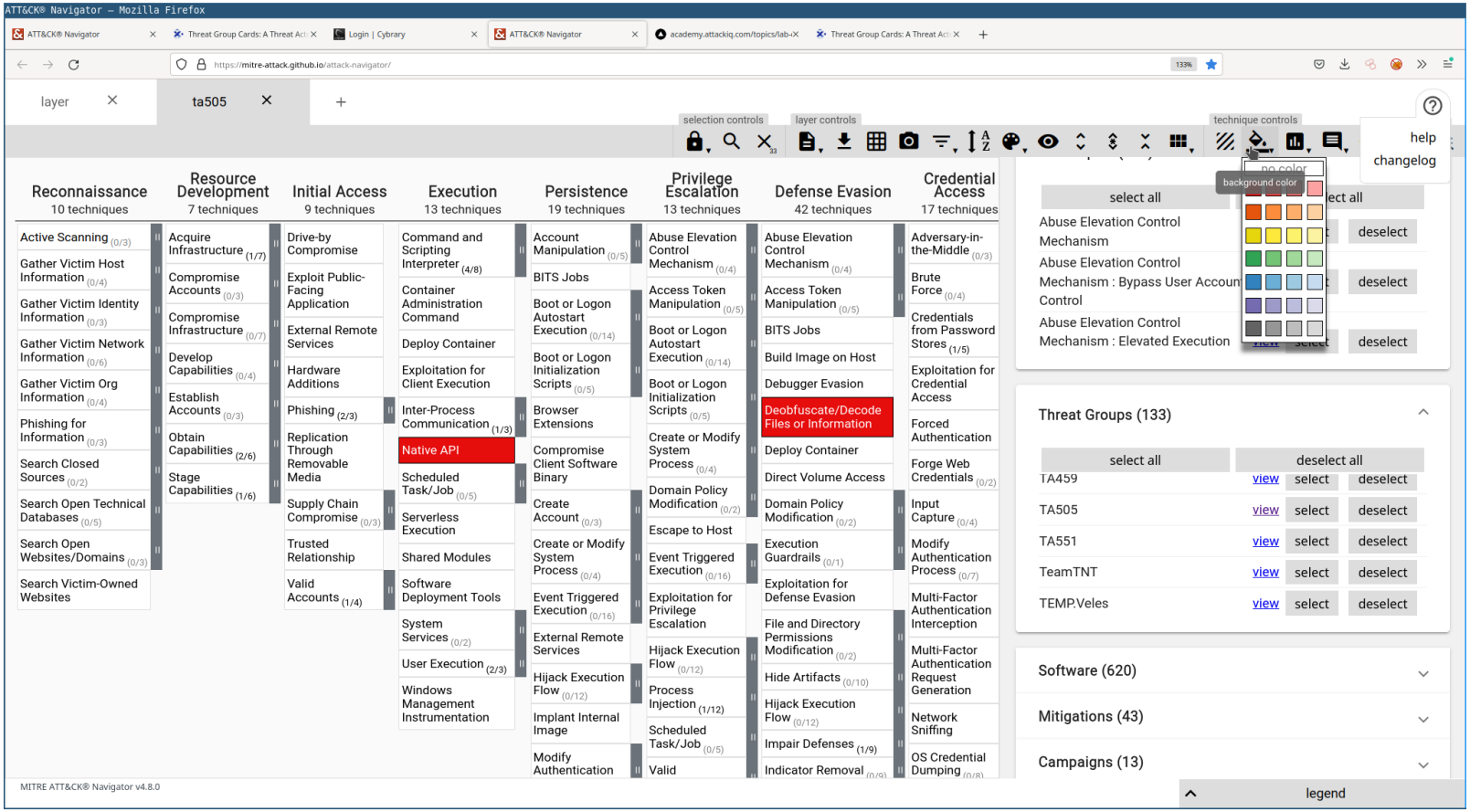
MITREATT&CK, New Layer



MITREATT&CK, New Layer

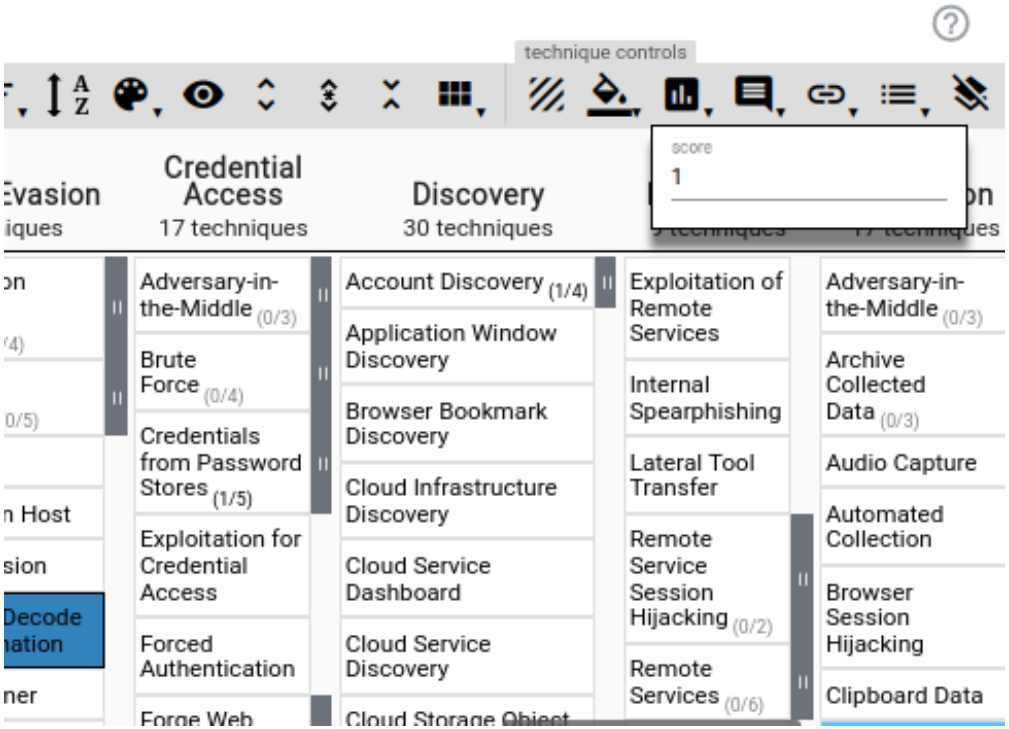


MITREATT&CK, New Layer



MITREATT&CK, New Layer

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



MITREATT&CK, New Layer

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.

score expression

a + b

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:

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

Subsection 2

What to do with MITREATT&CK

Use MITREATT&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 MITREATT&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

QnA

Thanks for your attention, Questions?