Risk and Vulnerability Management

Sven $\operatorname{Gabriel}$, Nikhef, EGI CSIRT

Oct 2023



Introduction to Risk and Vulnerability Management tCSC 2023

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

(ロ)、(型)、(E)、(E)、 E) の(()

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?

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ ●の00

Subsection 2

Towards Risk Management

◆□▶ ◆□▶ ◆臣▶ ◆臣▶ 臣 の�?

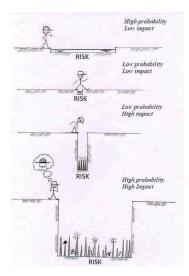
Definitions of Risk in context of Risk management:

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

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ ●の00

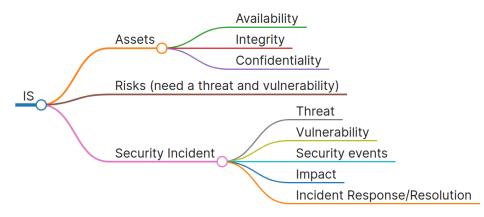
Risk Management is management of an organisation while taking into account the risks.

Towards Risk management Processs



◆□▶ ◆□▶ ◆ □▶ ◆ □▶ ○ □ ○ ○ ○ ○

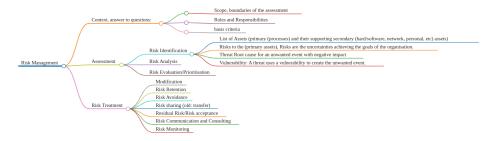
Towards Risk management Processs, add-hoc Information Security



ad-hoc IS management, questions

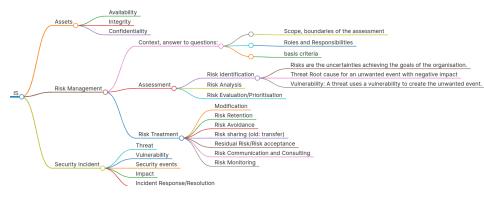
- What was the impact? were you just lucky that not more happened? or ...
- Do you really know your assets?
- Do you really know the risks to your assets?
- Did you know the affected entities in your organisation?
- Could you do proper communications related to the incident?
- If these left a nagging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

Risk management Process



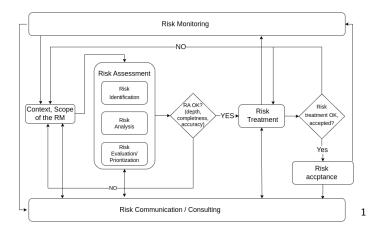


Information Security Management



▲□▶▲□▶▲□▶▲□▶ □ のQの

Risk management Process



¹S. Klipper, Information Security Risk Management \bigcirc \bigcirc \bigcirc \bigcirc \bigcirc \bigcirc \bigcirc \bigcirc \bigcirc

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.

◆□▶ ◆□▶ ◆臣▶ ◆臣▶ □臣 ○のへ⊙

²V: 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

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ ●の00

Threats a card game

Elevation of privilege, threat modelling card game for developers.



(日) (四) (日) (日) (日)

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.

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



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.

³The 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)

⁴https://www.enisa.europa.eu/publications/ interoperable-eu-risk-management-framework (B) (E) (E) (E) (E) (C)

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)

⁵https://www.enisa.europa.eu/topics/

threat-risk-management/threats-and-trends + ()

Get Info on available Controls

- Administrative (policies, procedures)
- Technical (Design, Architecture, Configuration, AuthNZ)

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ ●の00

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.

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ ●の00

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).

▲□▶ ▲□▶ ▲□▶ ▲□▶ □ のQで

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

Finally

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

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ ●の00

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

Threat Modelling with MITRE ATT&CK

◆□▶ ◆□▶ ◆ 臣▶ ◆ 臣▶ ○ 臣 ○ の Q @

Subsection 1

MITREATT&CK

<ロト < 団ト < 団ト < 団ト < 団ト 三 のQの</p>

MITRE ATT&CK

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

Reconnalosance ICherbrigen	Resource Development 7 schrigen	Bittal Access Factoripes	Execution Unerhippen	Pendidbece 15 schriges	Privilege Excatadion 10 schnigen	Defense Evados 42 actrigan	Endential Access ITschrigen	Discorwy 30 schrigen	Lateral Movement 3 techniques	Collection 17 schrigen	Constand and Exertisal 16 sections	Exfitution Stehnpast	anga Urachigan
a haveque	Apple Manhadare (11)	Dively Corporate	Command and Earlying	Accest Metabletien (2.1)	Huse Dealer Carled	Abuse Elevation Excited Rectances	Adversary to the Mulde (11)	Assessed Discoursey, p. 1	Exclusions of Secure	Adverages the Milde page	Aphaton LeyerProtocol.com	Advanted Delivation (171)	Access Access Services
e Veter Box Islamation (14)	Corporate Annatta Ann	Exploit Public Facing Application	Container Administration	and loss	noss fair Meighton	Acces Take Margateter	Ave free per	Application Nindow Discovery	manuf (perphilting	Antibia Collected Data (17)	Communication Through Renno-gourmodo	Into Turole SecUrity	Extra Destruction
"Value Marrie Information	Corporate Inheitrature	Esternal Remote Estatutes	Carenard	Read or Legan Released Execution (2010)	Bet a Loger Adopted	HT.Ms	Casterials from Passaneti District	Brearst Bolimark Darrowy	Land Tel Tanks	Auto Deptere	Des Deodra	Estimator Over Illenative Potent	Esta Encryptet for Impart
r Victor Subaroh	Centry Capiblities	Redeau Johns	Dapley Container	Bod or Logor Indiatation	Langeon and	Ball Propriet for	East-fation for Declarities	Dout Information Discourty	Renda Sensa Seasor	Anonated Solienion	Day Office Ker	Addition Over 12 Channel	Data Maripaletics
	Candida Accounts	Phillip	Exploration to Owner Execution	200 Property and	Bor y Lope Westmon		Acces	Dout Service Subfacerd	machine annual property	Browner Section Marching		Entitudion Over Ether	bdentet
"Nation Dig behavioration (5.1)	Otain Equipilities	Repiretor Trougt Renowship	has been formation	Browse Cransions	Degra (c)	Driveger Transm	Foront Authentication	Elevel Service Discovery	Remote Services	Christellura	Dynamic Resolution	Ealthurine Oper Dirert Network Medium	Dok Nov
reformation (c)	The Designed Law		a 700 a 40	Compression Chert Suffware	Dearson Modily Spream Proceedings	Desisfuenza Gassie Nas or Tribution	Foor the Codemon	Ethel Shines Open Deavers	Backupper Through	Ovarior Oxychospi		Letters Out Placed	Export bend of barries
Donal Engran		Engly Date Desperation (11)	Direkter Tex 20	liney.	- Dense Polos Molforder	Destar Cartainer	Paul Caster	Contenent and Pressourie Descentes		Own from Conference	Adust Owners	Claim	Fernane Canadian
Ren Tethnical Deutscen, J. 1	8	Durret Netrinsky	· broketering	Owner Account	Disease in Fight	Oted Today Assess	Bodh-Auberbuster	Driveer Tunor	Sofware Suphyment Tools	Applies 10	ingen boi hanin	Extinution Over Hab	Intel Super Scores
Epo Wester Conaix (c)		THE ROUTLAN	Description	Cash-y Weby Symmetry	Intel Transmillanation	B Dense Polici Ballintina		Domain Trad Documery	Fairt Shared Current	Ous for Advantor	Wuts-Stope Channels	Scheduled Transfer	National Denial of Denine
ug h (sockwar Katas			Settage Galageer Task	from Viggered Execution	Textubering ing Deciment	fancier bactula	NUS Factor Authonisation	The and Electron Electrony	the Ahmura Asheroceton	Data from Land Tenters	Non-Application Law Proposil	Danate Baters Grad	Boners Nacion
			Datien Genting	Drama Sense Gentres	Examples	- Industries for Defense Dunion	Bull Faster Suffernisation	Drag Date Denny		Data from National Datas Drive	No-Bardelling	Room	Gentre Sea
			Har families	Hart Capita Creater	Pipels Demokra Fire	The set literate forminizes	Repurci Gerenation	Schenk Sening Chemany		Cara fron Removal a Media	Pretonal Turneling		Server Shattan Balan
			Notice Measured		Property and	Budhaten	Antonia Stating				No.		Speen Skitcowymetod
			Windows Recupited	higher his mail trope	Distant Selection	Not A View,	OS Desienta/Damping	Monet Stat Decovy		Cos Stape	Remain Assess Dollarge	-	
				Droves	Tale Accusts	Next Incodes Top.	Stad Application Across				Tatle Spaing		
				Office Association Dantas		insuit Johnson		Passed Pully 200493		Tel Deter (1)	the Service		
				Delline		indicator ferminal	End or herps haltertowine	Perginana Deniar Discovery	_	Same Capture			
				Scheduler Task / All		ndvertonment becater	Test in Forge Redwood	Permanan Group Dalaway		Video Copium			
				See Stree Corporat		Norperading	Talana pro	Press Dancey					
				Torth Tarativa		Rods Automatics Proves	freed that Season Cookie	bas figins					
				NOLAMORE		Notify Class Compare	Sheerand Dedentials	Networks Spetiers Discovery					
				And Constant and		readurary		Software Bacovers	1				
						No.01x Tegetty		Network Strengton Doctorery					
						Rody Jumn map		hypers/, postor Beapery	1				
						Selarah Engelan Bridging		Destro Televit Carbonites					
						Obtained Titles or Information		Parenas					
						Phy Fite Modification		System/Reburk (procedure Descent)					
						Paddan		Sectors Committee Electrony					
						Proceedigation	1	Senery Service Biocoway					
						Referrise Costs Loading		Anton True Jacoury					
						Rogue Bumain Controller		Virtualization Section Learning					
						Kopa Sunai Coltuna Kopis		What show handlow the sole (2.1)					
						New11vd Come							
							1						
						Spring Bray Prog Secular (1991)							
						Apriam Script Prog Execution (21)							
						Template Injustion							
						Tartic Spraing 20							
						Euclid Develope Stilles Prov							
						Unued Druggortal Dout Regions	-						
						Use Operate Automization							
						Retarial							
						Yeld Accounts over							
						Weindows Carolina Leaster (11)							
						Weaker Everyption							

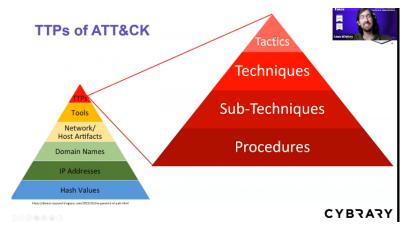
▲□▶ ▲□▶ ▲ 三▶ ▲ 三▶ 三三 - のへぐ

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

▲ロ ▶ ▲周 ▶ ▲ 国 ▶ ▲ 国 ▶ ● の Q @

OSINT

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



Groups Tools Search Statistics



lome > List all tools

Search

Threat Group Cards: A Threat Actor Encyclopedia

All tools

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

◆□▶ ◆□▶ ◆臣▶ ◆臣▶ □臣 ○のへ⊙

OSINT

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

Actor	Source country	v
	Victim country	Netherlands v or Worldwide
	Victim sector	Education
	Motivation	v
	Free text search	(can use ** and '?' wildcards)
		Searchl

Tool	Category	v	
	Туре	v	
	Free text search		(can use "" and '?' wildcards)
		Searchl	

OSINT

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

Changed	Name	Country	Observed	
APT g	roups			
	APT 17, Deputy Dog, Elderwood, Sneaky Panda	•2	2009-Sep 2017	
	APT 29, Cozy Bear, The Dukes		2008-Oct 2022	Q
	APT 41	•0	2012-Aug 2022	4
	Circus Spider	[Unknown]	2019-Feb 2022	q
	Cutting Kitten, TG-2889	٠	2012-Mar 2016	G
	Dark Caracal		2007-2020	
	Desert Falcons	[Gaza]	2011-Nov 2021	4
	Equation Group		2001-Aug 2016	٩
	FIN11	[Unknown]	2016-Dec 2022 💧	٩
	MuddyWater, Seedworm, TEMP.Zagros, Static Kitten	٠	2017-Late 2021	0
	Shadow Network	•0	2010-2010	4
	Sofacy, APT 28, Fancy Bear, Sednit		2004-Sep 2022	4
	TeamSpy Crew		2010-Feb 2017	
	Turla, Waterbug, Venomous Bear		1996-Sep 2022	
Other	groups			
	Fxmsp		2016-Jul 2020	4

▲□▶ ▲□▶ ▲ 三▶ ▲ 三▶ 三 のへぐ

MITREATT&CK, and OSINT

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

◆□▶ ◆□▶ ◆臣▶ ◆臣▶ □臣 ○のへ⊙

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	~

◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 - のへで

ATTROX8 Nevigetor X	Thread Group Cards: A T	erst. Ici - X 🛛 📓 Logie Cyle	wy × 🛃 A	T&CKB Navigator	 academy allackie som 	Apples/Jab.X 🔒 Threat Group Con	ACATHONIACIX +	
C	O A topolimized	ick.gkthub.lo/astack-nev/patoc/						🚥 \star 🛛 🗄 👋 🖗 »
layer ×	layer1 ×	+			selection confi		0 ₹ .12 (P. O ≎ ŝ ≭ III. Mechnique controla Mechnique controla Mech
Reconnaissance	Resource Development 7 techniques	Initial Access 9 techniques	Execution 13 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion	Credential Access 17 techniques	Q, Search
Active Scanning (3/2)	Acquire Infrastructure (0/7)	Drive-by Compromise Exploit Public-	Command and Scripting Interpreter	Account Manipulation (1/3) BITS Jobs	Abuse Elevation Control Mechanism ₍₀₁₄₎	Abuse Elevation Control Mechanism (1/4)	Adversary-in- the-Middle (1/2) Brute	Search Settings
Sather Victim Identity	Accounts (0/7)	Facing Application	Container Administration Command	Boot or Logon	Access Token Manipulation	Access Token Manipulation	Credentials	name ATT&CK ID description data sources
Sather Victim Network	Develop Capabilities (3-0)	External Remote Services	Deploy Container Exploitation for	Execution (0/14) Boot or Logon	Boot or Logon Autostart Execution (3/14)	BITS Jobs Build Image on Host	from Password Stores (1/5) Exploitation for	
ather Victim Org	Establish Accounts	Additions Phishing (22)	Client Execution	Scripts (0/5) Browser	Boot or Logon Initialization Scripts 2019	Debugger Evasion Deobfuscate/Decode	Credential Access	Techniques (594)
Phishing for Information (1/2)	Obtain Capabilities (200)	Replication Through	Communication (323) Native API	Extensions	Create or Modify System	Files or Information	Forced Authentication	select all deselect all
earch Closed ources (3/2)	\$1440	Removable Media	Scheduled Task/Job	Client Software Binary	Process (3-4)	Direct Volume Access	Forge Web Credentials (1/2)	Abuse Elevation Control view select deselect
earch Open Technical atabases (1/3)	Capabilities (3.16)	Supply Chain Compromise (1/3)	Serverless Execution	Create Account (1/7)	Domain Policy Modification (3/2) Escape to Host	Domain Policy Modification (1/2)	Input Capture (1/4)	Abuse Elevation Control Mechanism : Bypass User Account view select deselect
earch Open febsites/Domains (0/2)		Trusted Relationship	Shared Modules	Create or Modify System Process (2010)	Event Triggered Execution 12/16	Guardralis (0/1)	Modify Authentication Process (1/7)	Control Abuse Elevation Control
earch Victim-Owned febsites		Accounts (I/I)	Software Deployment Tools System	Event Triggered Execution (0.116)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion File and Directory	Multi-Factor Authentication	Mechanism : Elevated Execution yiew select deselect
			Services (1/2)	External Remote Services	Hijack Execution	Modification (1/2)	Multi-Factor	Threat Groups (133)
			Windows Management	Hijack Execution Flow (3/12)	Process Injection (2012)	Hide Artifacts (3/10) Hijack Execution	Request Generation	Software (620)
			Instrumentation	Implant Internal Image Modify	Scheduled Task/Job (3/5)	Flow (0/12) Impair Defenses (1/9)	Network Sniffing OS Credential	Mitigations (43) 🗸
ITRE ATT&CKIP Navigator +4.0.0				Authentication	Valid	Indicator Removal and	Dumping	

⇒ C	O A separative-ato	ok.gkhub.lo/stack-nevipeter/						1306. ★	0	🗄 🍕 🤗 »
layer ×	layer1 ×	+			selection cont			. ⊙ ≎ ŝ X II , ///	pe controls	(
						^, ∎, ≚ ⊞		, u , , , … , ///	<u>.</u> , <u>.</u> , .	changelo
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	select all	dese	lect all
the Scanning $_{(\lambda^{\prime}2)}$	Acquire Infrastructure (8/7)	Drive-by Compromise	Command and Scripting	Account Manipulation	Abuse Elevation Control	Abuse Elevation Control	Adversary-in- the-Middle	Abuse Elevation Control Mechanism	view selec	t deselect
formation (1/4)	Compromise Accounts	Exploit Public- Facing	Interpreter (1.18) Container	BITS Jobs	Mechanism (0/4)	Mechanism (3/4) Access Token	Brute Force (1/4)	Abuse Elevation Control Mechanism : Bypass User Account Control	view selec	t deselect
ther Victim Identity ormation (1/3)	Compromise Infrastructure (0/7)	Application External Remote	Administration Command	Boot or Logon Autostart Execution	Manipulation (011) Boot or Logon	Manipulation (315) BITS Jobs	Credentials from Password	Abuse Elevation Control Mechanism : Elevated Execution		t deselect
her Victim Network semation (1/5)	Develop Capabilities (3.40	Services Hardware	Deploy Container Exploitation for	Boot or Logon Initialization	Autostart Execution (3/14)	Build Image on Host	Stores (3/5) Exploitation for	Mechanism : Elevated Execution	view selec	c deselect
nmation (1-4)	Establish Accounts (0/2)	Additions Phishing (3/2)	Client Execution	Scripts (0,5) Browser	Boot or Logon Initialization Scripts	Debugger Evasion Deobfuscate/Decode	Credential Access	Threat Groups (133)		,
shing for emation (1/2)	Obtain Capabilities (200)	Replication Through	Communication (0/3) Native API	Extensions Compromise	Create or Modify System	Files or Information Deploy Container	Forced Authentication			
rch Closed rces (3/2)	Stage Capabilities	Removable Media	Scheduled Task/Job	Client Software Binary	Process (1-4) Domain Policy	Direct Volume Access	Forge Web Credentials (5/2)	select all TA459	view selec	lect all t deselect
rch Open Technical Ibases (1/3)	Capabilities (3/4)	Supply Chain Compromise (1/3)	Serverless Execution	Create Account (5/7)	Modification (3/2)	Domain Policy Modification (1/2)	Input Capture (1/4)	TĄ505	view selec	t deselect
rch Open sites/Domains		Trusted Relationship	Shared Modules	Create or Modify System	Escape to Host Event Triggered	Execution Guardralis (pro)	Modify Authentication	TA551	view selec	
rch Victim-Owned isites		Valid Accounts (pro)	Software Deployment Tools	Process (0/4) Event Triggered	Execution (2/16)	Exploitation for Defense Evasion	Process (1/7) Multi-Factor	TeamTNT	view selec	
			System Services (177)	Execution (3/16) External Remote	Privilege Escalation	File and Directory Permissions	Authentication Interception	Tallit, Yorka	in seat	Geselect
			User Execution (3/3)	II Hijack Execution	Hijack Execution Flow (1/12)	Hide Artifacts (1/2)	Multi-Factor Authentication Request	Software (620)		
			Windows Management Instrumentation	Flow (3/12) Implant Internal	Process Injection (1/12) Scheduled	Hijack Execution Flow (0/12)	Generation Network Spiffing	Mitigations (43)		
				Modify Authentication	Task/Job (0/5)	Impair Defenses (1/9) Indicator Removal (1/9)	OS Credential Dumping	Campaigns (13)		

◆□▶ ◆□▶ ◆ □▶ ◆ □▶ ● □ ● ● ●

ATT&OOB Neviptor X	Thread Group Carety A T	west Act X	niptor × +							
→ C	O A topoleterat	ek.gkhub.le/stack-navigator/						137A 🔮	0 1	< 🔒 »
apt41 ×	ta505 ×	+					⊞© ≂.12¢	P. ⊕ ≎ ŝ ≭ Ⅲ,	ingua controla	(? help
Reconnaissance	Resource Development 7 techniques	Initial Access 9 techniques	Execution 13 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	De app41		Q. Search		changelog
ctive Scanning (0.2) lather Victim Host rformation (0.4) lather Victim Identity rformation (0.5) lather Victim Network rformation (0.5)	Acquire Infrastructure (0/7) Compromise Accounts (0/7) Compromise Infrastructure (0/7) Develop	Drive-by Compromise Exploit Public- Facing Application External Remote Services	Command and Scripting Interpreter (5/16) Container Administration Command Deploy Container	Account Menipulation (205) BITS Jobs Boot or Logon Autostart Execution (1/14) Boot or Logon	Abuse Elevation Control Mechanism (())() Access Token Manipulation (()) Boot or Logon Autostart Execution ()/14)	Abur description Cont Mect Enterprise Acco Man BITS 12 Bullo Metadata		Search Settings	escription 📕 data	I SOURCES
ather Victim Org formation (144) hishing for formation (142) earch Closed ources (142)	Capabilities (3.4) Establish Accounts (3.4) Obtain Capabilities (1.4) Stage	Hardware Additions Phishing (1/2) Replication Through Removable Media	Exploitation for Client Execution Inter-Process Communication (2018) Native API Scheduled	Initialization Scripts ((c)S) Browser Extensions Compromise Client Software Binary	Boot or Logon Initialization Scripts (2015) Create or Modify System Process (314)	Debt add metac Dect Files Depl add links	data 🍋	Techniques (594) select all Abuse Elevation Control	deselect	all deselect
earch Open Technical stabases (5/5) earch Open febsites/Domains (5/7) earch Victim-Owned	Capabilities (344)	Supply Chain Compromise (1.0) Trusted Relationship	Task/Job (1/8) Serverless Execution Shared Modules Software	Create Account (1/3) Create or Modify System Process (1/4)	Domain Policy Modification (1/2) Escape to Host Event Triggered Execution (1/16)	Domain Policy Modification (5/2) Execution Guardralis (1/1) Exploitation for	Modify Authentication Process (1/7)	Mechanism Abuse Elevation Control Mechanism : Bypass User Accou Control Abuse Elevation Control Mechanism : Elevated Execution		deselect
iebsites		Accounts	Deployment Tools System Services (1/2) User Execution (3/3) Windows	Event Triggered Execution (1/16) External Remote Services	Exploitation for Privilege Escalation Hijack Execution Flow (1/12) Process	Permission File and Directory Permissions Modification (1/2) Hide Artifacts (1/10)	Multi-Factor Authentication Interception Multi-Factor Authentication Dequest Generation	Threat Groups (133)	<u>view</u> select	deselect
			Management Instrumentation	Flow (3/12) Implant Internal Image	Injection (2012) Scherholart	Hijack Execution Flow (3/12)	Network Spiffing	select all	deselect	
				Modify Authentication	Task/Job (1/5)	Impair Defenses (1/) Indicator Removal	OS Credential	APT39 APT41	view select	deselect deselect
TRE ATT&CKIP Navigator v4.0.1	0							^	legend	

⇒ C	O A Hourset	edegithabile/etack-newpeter/						100a 🚖	Θ	¥ 🗟 😣 »
layer ×	ta505 ×	+			selection cont		$\mathbf{o} = \mathbf{i} \mathbf{A} \mathbf{a}$		ique controles	C hele
						∧. ∎, ≚ ⊞		•, • • • • • •, <i>•</i> , <i>•</i> , <i>•</i> ,	<u>.</u>	changelog
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	select all Abuse Elevation Control	epound color ec	t all
tive Scanning (3/2) ther Victim Host	Acquire Infrastructure (1/7)	Drive-by Compromise	Command and Scripting Interpreter (ant)	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism (1991)	Adversary-in- the-Middle (1/3)	Abuse Elevation Control Mechanism Abuse Elevation Control		deselect
ormation (1/1) ther Victim Identity	Accounts (0/7)	Exploit Public- Facing Application	Container Administration	BITS Jobs Boot or Logon	Access Token Manipulation	Access Token Manipulation	Brute Force (1)/4)	Mechanism : Bypass User Accoun Control		deselect
ormation (1/3) ther Victim Network ormation (1/3)	Compromise Infrastructure (0/7)	External Remote Services	Command Deploy Container	Autostart Execution	Boot or Logon Autostart	BITS Jobs Build Image on Host	Credentials from Password Stores (1/5)	Abuse Elevation Control Mechanism : Elevated Execution		deselect
her Victim Org	Capabilities (3/4) Establish	Hardware Additions	Exploitation for Client Execution	Initialization Scripts (0.5)	Execution (3/14) Boot or Logon Initialization	Debugger Evasion	Exploitation for Credential Access			
shing for smation (1/2)	Accounts (0/2)	Phishing (2/2) Replication	Inter-Process Communication (1/3)	Browser Extensions	Scripts (0,1) Create or Modify	Deobfuscate/Decode Files or Information	Forced	Threat Groups (133)		
Irch Closed	Capabilities (2.%)	Through Removable	Native API	Compromise Client Software	System Process (340)	Deploy Container	Forge Web	select all	deselec	
rces (1/2) rch Open Technical	Stage Capabilities (1/6)	Media Supply Chain	Scheduled Task/Job (3/5)	Binary Create	Domain Policy Modification	Direct Volume Access	Credentials (1/2)	TA459	view select	deselect
ibases (1/3)		Compromise (1/3)	Serverless Execution	Account (5/7)	Escape to Host	Modification (1/2)	Capture (1/4)	TA505 TA551	view select	deselect deselect
rch Open isites/Domains (0/2)		Trusted Relationship	Shared Modules	Create or Modify System Process (2010)	Event Triggered Execution (2/16)	Guardraits (Dr1)	Modify Authentication Process (1/7)	TeamTNT	view select	deselect
rch Victim-Owned osites		Valid Accounts (1/0	Software Deployment Tools	Event Triggered Execution	Exploitation for Privilege	Exploitation for Defense Evasion	Multi-Factor Authentication	TEMP.Veles	view select	deselect
			System Services (1/2)	External Remote Services	Escelation Hijack Execution	File and Directory Permissions Modification (1/2)	Multi-Factor			
			User Execution (2/3) Windows	Hijack Execution Flow (3/12)	Flow _(1/12) Process	Hide Artifacts (3/10)	Authentication Request Generation	Software (620)		
			Management Instrumentation	Implant Internal Image	Injection (1/12) Scheduled	Hijack Execution Flow (0/12)	Network Sniffing	Mitigations (43)		
				Modify	Task/Job (0,15)	Impair Defenses (1/8)	OS Credential Dumping	Campaigns (13)		

◆□▶ ◆□▶ ◆ □▶ ◆ □▶ ● □ ● ● ●

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

6

▲□▶ ▲□▶ ▲三▶ ▲三▶ 三三 のへで

		technique controls	(?)
, 1 ^A z	₽,	; X Ⅲ, <i>∅</i> , <u>№,</u> <u>0, ۹,</u>	⊝,≡, 🕅
Evasion iques	Credential Access	Discovery 30 techniques	n
on II	Adversary-in- the-Middle (0/3)	Account Discovery (1/4)	Adversary-in- the-Middle (0/3)
(4)	Brute Force (0/4)	Discovery Browser Bookmark Browser Bookmark Browser Bookmark	Archive Collected Data (0/3)
0/5)	Credentials from Password Stores (1/5)	Discovery Cloud Infrastructure	Audio Capture
n Host	Exploitation for	Discovery Remote	Automated Collection
sion	Credential Access	Cloud Service Service Dashboard Session	Browser
Decode nation	Forced Authentication	Cloud Service Discovery Remote	Session Hijacking
ner	Forge Web	Cloud Storage Object	Clipboard Data



◆□▶ ◆□▶ ◆□▶ ◆□▶ □ のQ@

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.

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ ●の00

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

▲□▶ ▲□▶ ▲□▶ ▲□▶ □ のQで

Thanks for your attention, Questions?