PRELUDE

Before going through the notes of the actual course I want to make a prelude with important definitions and knowledge which are usefull to understand the course content

WHAT'S ATT&CK?

Adversarial **T**actics **T**echniques **& C**ommon **K**nowledge (ATT&CK) is a gideline for classifying and describe cyberattacks. Is created by MITRE and provide usefulls matrix (actually 3 type of matrices ICS, Enterprise and Mobile).

In the course we focus using the Enterprise one but same things can be applied to other matrix

MITRE Enterprise ATT&CK™ Framework

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Image File Execution Options Injection			Forced Authentication	Network Share Discovery	AppleScript		Man in the Browser	Exfiltration Over Physical Medium	Multi-hop Proxy
Plist Modification			Hooking	System Time Discovery	Third-party Software		Browser Extensions		Domain Fronting
Valid Accounts			Password Filter DLL	Peripheral Device Discovery	Windows Remote Management		Video Capture	Exfiltration Over Command and Control Channel	Data Encoding
DLL Search Order Hijacking			LLMNR/NBT-NS Poisoning	Account Discovery	SSH Hijacking	LSASS Driver	Audio Capture		Remote File Copy
AppCert DLLs		Process Doppelgänging	Securityd Memory	File and Directory Discovery	Distributed Component Object Model	Dynamic Data Exchange	Automated Collection	Scheduled Transfer	Multi-Stage Channels
Hooking		Mshta	Private Keys	System Information Discovery	Pass the Ticket	Mshta	Clipboard Data	Data Encrypted	Web Service
Startup Items		Hidden Files and Directories	Keychain	Security Software Discovery	Replication Through Removable Media	Local Job Scheduling	Email Collection	Automated Exfiltration	Standard Non-Application Layer Protocol
Launch Daemon		Launchctl	Input Prompt	System Network Connections Discovery	Remote Desktop Protocol	Trap	Screen Capture	Exfiltration Over Other Network Medium	Communication Through Removable Media
Dylib Hijacking		Space after Filename	Bash History	System Owner/User Discovery	Pass the Hash	Source	Data Staged	Exfiltration Over Alternative Protocol	Multilayer Encryption
Application Shimming		LC_MAIN Hijacking	Two-Factor Authentication Interception	System Network Configuration Discovery	Exploitation of Vulnerability	Space after Filename	Input Capture	Data Transfer Size Limits	Standard Application Layer Protocol
AppInit DLLs		HISTCONTROL	Account Manipulation	Application Window Discovery	Shared Webroot	Execution through Module Load	Data from Network Shared Drive	Data Compressed	Commonly Used Port
Web Shell		Hidden Users	Replication Through Removable Media	Network Service Scanning	Logon Scripts	Regsvcs/Regasm	Data from Local System		Standard Cryptographic Protocol
Service Registry Permissions Weakness		Clear Command History	Input Capture	Query Registry	Remote Services	InstallUtil	Data from Removable Media		Custom Cryptographic Protocol
Scheduled Task		Gatekeeper Bypass	Network Sniffing	Remote System Discovery	Application Deployment Software	Regsvr32			Data Obfuscation
New Service		Hidden Window	Credential Dumping	Permission Groups Discovery	Remote File Copy	Execution through API			Custom Command and Control Protocol
File System Permissions Weakness		Deobfuscate/Decode Files or Information	Brute Force	Process Discovery	Taint Shared Content	PowerShell			Connection Proxy
Path Interception		Trusted Developer Utilities	Credentials in Files	System Service Discovery		Rundll32			Uncommonly Used Port
Accessibility Features		Regsvcs/Regasm				Scripting			Multiband Communication
Port Monitors		Exploitation of Vulnerability				Graphical User Interface			Fallback Channels
Screensaver		Extra Window Memory Injection				Command-Line Interface			
LSASS Driver		Access Token Manipulation				Scheduled Task			
Browser Extensions		Bypass User Account Control				Windows Management Instrumentation			
Local Job Scheduling		Process Injection				Trusted Developer Utilities			
Re-opened Applications		Component Object Model Hijacking				Service Execution			
Rc.common	SID-History Injection	InstallUtil							
Login Item	Sudo	Regsvr32							
LC_LOAD_DYLIB Addition	Setuid and Setgid	Code Signing							
Launch Agent		Modify Registry							
Hidden Files and Directories		Component Firmware							
.bash_profile and .bashrc		Redundant Access							
Trap		File Deletion							
Launchctl		Timestomp							
Office Application Startup		NTFS Extended Attributes							
Create Account		Process Hollowing							
External Remote Services		Disabling Security Tools							
Authentication Package		Rundll32							
Netsh Helper DLL		DLL Side-Loading							
Component Object Model Hijacking		Indicator Removal on Host							
Redundant Access		Indicator Removal from Tools							
Security Support Provider		Indicator Blocking							
Windows Management Instrumentation Event Subscription		Software Packing							
Registry Run Keys / Start Folder		Masquerading							
Change Default File Association		Obfuscated Files or Information							
Component Firmware		Binary Padding							
Bootkit		Install Root Certificate							
Hypervisor		Network Share Connection Removal							
Logon Scripts		Rootkit							
Modify Existing Service		Scripting							

attack.mitre.org

The whole framework is based on 4 main components :

1. TECHNIQUES = how an adversary achieves a goal performing and action (**T1134 - Access Token Manipulation**)
2. SUB-TECHNIQUES = like techniques but more specific, they are part of a technique (**T1134.001 - Token Impersonation**)
3. DATA SOURCES = subject information which can be collected by sensors/logs (**Logon Session**)
4. **TACTIC** = The adversary tactical objective

There are various ways you can use this framework but for the purpose of the course we will use it as **heatmap** (we will explain it later)

WHAT'S A SOC?

Security Operation center is a team of IT professionals which purpose is to monitor 24/7 the entire IT infrastructure of a organization (can be in house or outsourced) and choose technology and methodologies to improve and mantain security. Planning, monitor/detection and recovery (if needed) are all covered by SOCs

WHAT'S A SOC ASSESSMENT The assessment is a full procedure created in order to analyze, improve and mature the SOC team helping to fit the organization goals and business model. Need to keep in mind that an assessment is a snapshot in time determine the efficiency of the SOC and their services
In this course I learned how to fit an assessment with the ATT&CK framework or we better call it an **ATT&CK based SOC assessment**.

ATT&CK SOC ASSESSMENTS

```
assessment team + SOC enviroment = detection heatmap
```

Assessment Phases

1. Map SOC technologies to ATT&CK matrix
2. Interview SOC staff

3. Communicate thefindings (with ATT&CK)
4. Suggest changes to align with ATT&CK

WHY ATT&CK ASESSMENTS?

In this type of assessments we focus on confidence detection which is a pretty neat and understandable type of scoring. The ATT&CK give a good explanation on **Threat Intelligence** and **Adversary Emulation**.

The assessment is used, in first place, to discover **confidence detection gaps** and fix it through :

- Communicate capabilities
- Tooling purchase (based on ROI)
- Data sources for detection
- Analytics on high impact threats

IDENTIFY DETECTION GAPS

1. **Hands On** → pentest/read team
   Usefull for small scope or when pinpoint accuracy is needed but is **time consuming and really invasive**
2. **Hands Off** → overview + analysis (assessments!)
   Paint broad strokes, can be used for a fast turn around. Minimal invasive and variable time investment

METHODOLOGY FOR ASSESSMENTS

```
discuss -> analyze -> interview -> process -> heatmap
```

Usually assessments take 1-4 months with an analytic develop programs, where the assessment team need to **map SOC to ATT&CK**

- **SET THE STAGE** → interview preview, expectation, timeline
- **ANALYZE** → tools/sensors, analytics in SIEM, log collection, other documentation 9red team, incident report...)

- **INTERVIEW SOC STAFF** → standard questions, clarify documentation, known gaps/strength
- **DELIVER RESULTS** → incorporate feedback, heatmap compilation, outbrief, report

The ingredients for a full SOC ASSESSMENTS are **heatmap + summary report (with key finding) + reccomendations**

The phases are :

1. **Frame Assessment** = coverage & definitions
2. **Set Rubric** = definition of "coverage"
3. **Analyze Components** = from SOC tech to ATT&CK
4. **Interview Staff** = how things actually work
5. **Compile Results** = analysis, heat map and report
6. **Propose Changes** = "how to get better" after the assessments

(1.1) FRAMING ASSESSMENTS

This is the first step and you need to decide if the organization should or not run an assessments and help the SOC understand and want the assessments

The real gold here should make **clear to the clients the right expectations and resize the existing ones** :

- ATT&CK is not a silver bullet, it just give a glimpse inside the framework coverage
- Assessments are a snapshot of the current situation when the assessments is made
- The real security improving need a following up after the assessment (not the assessment itself)
- Hands off assessments return broad strokes and suggestion on where gaps (can) lie

Also here a list of organizations that are **not suitable** for an ATT&CK assessments

- Who are **not interested** in assessments or in the follow up
- Organizations **without SOC staff**
- Organizations **without visibility in key data sources** (ex:/ email managed by another org)

- Organizations which want a **turn-key** (is not an ATT&CK solutions)
- Organizations with a **stable and good understand** of ATT&CK

The **right target** for this type of assessments are organization which are looking to improve and start branching into **threat-informed defense**

The final thing to note in this first part is that usually your role can be defined as **antagonist** and not an ally here a few tips to avoid this and makes your position clear from the start

- **Feedback =/= wordsmiths**, staff can be worried on how the reports/final results will be used (like a personal attack)
- Staff might exagerate/misrepresent real capabilities which lead to innacurate results
- Staff (especially leadership) may overreact to results making damage and ignore the point of your job
- Find **alternative phrase** to use **instead of "assessment"**
- Make sure leadership understand the assessments and viceversa (your assessments should help the business model and organization goals)

If you are described as enemy from the **SOC** they **might not comply to the process adding effort and time** to your schedule, this is why is important to set yourself as an ally from the start and that the is not a staff evaluation but a gauge performance

(1.2) SCOPING AN ASSESSMENTS

Last part of **framing the assessment** is to identifythe relavant parts of the ATT&CK framework for the specific SOC. Also decide if use **ICS, Mobile or Enterprise platform.**

To achieve this you need to make yourself some questions to adjust your scope :

- Which tech are available in the SOC enviroment?
- What are they suppoed to protect?
- Can they see it?
- Do they want to protect it?

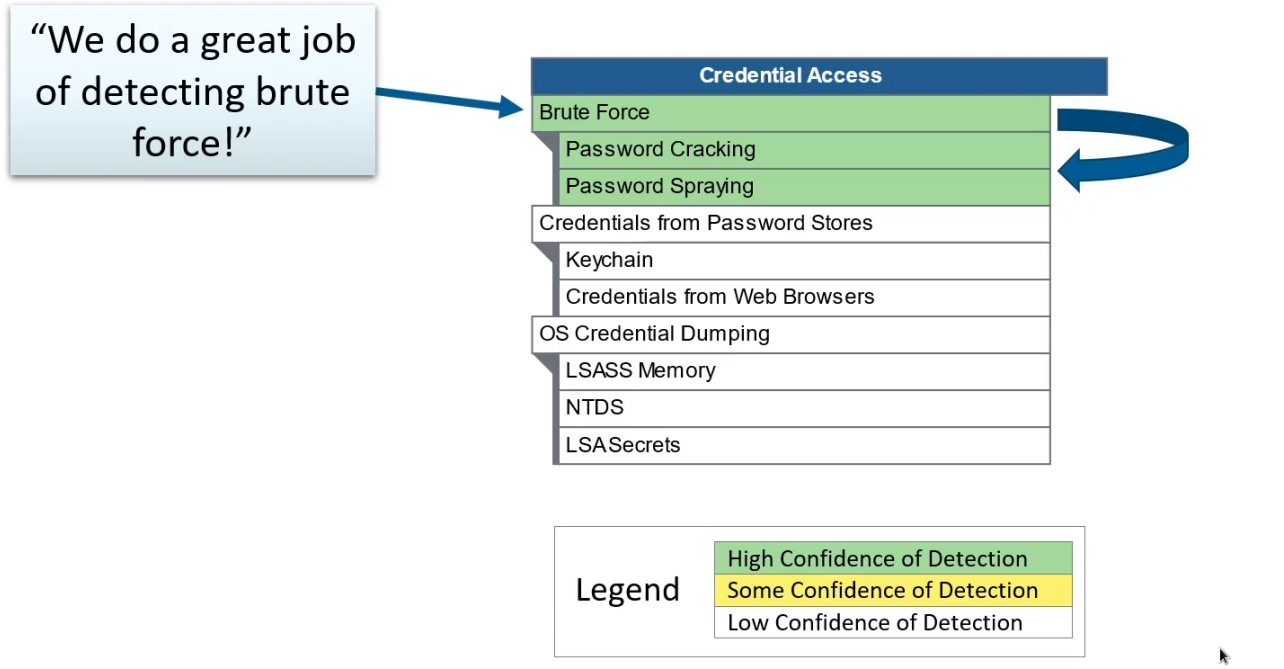
Usually the PRE-ATT&CK matrix is not included but it depend from the context

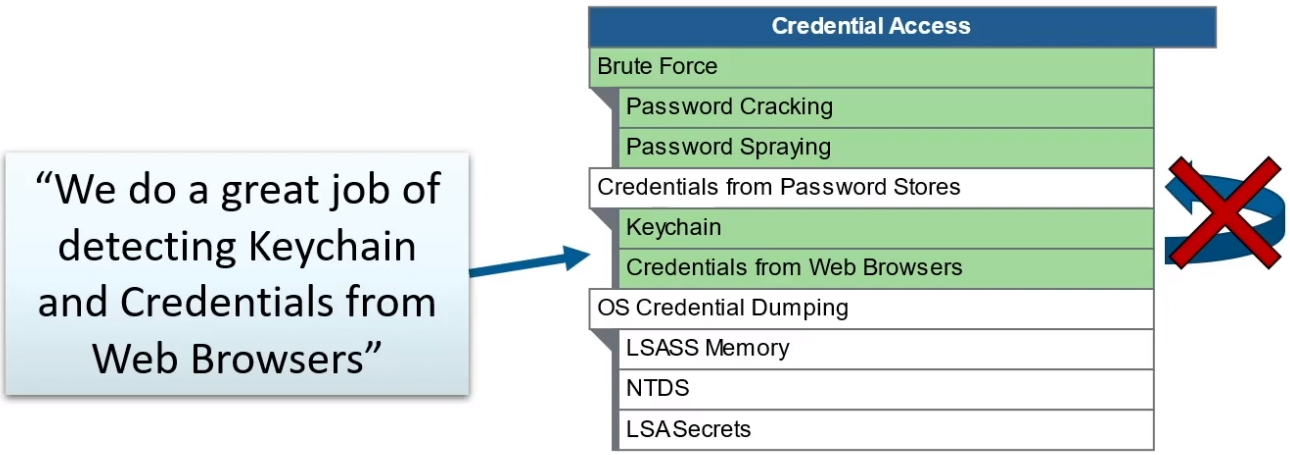
(2) COVERAGE RUBRIC

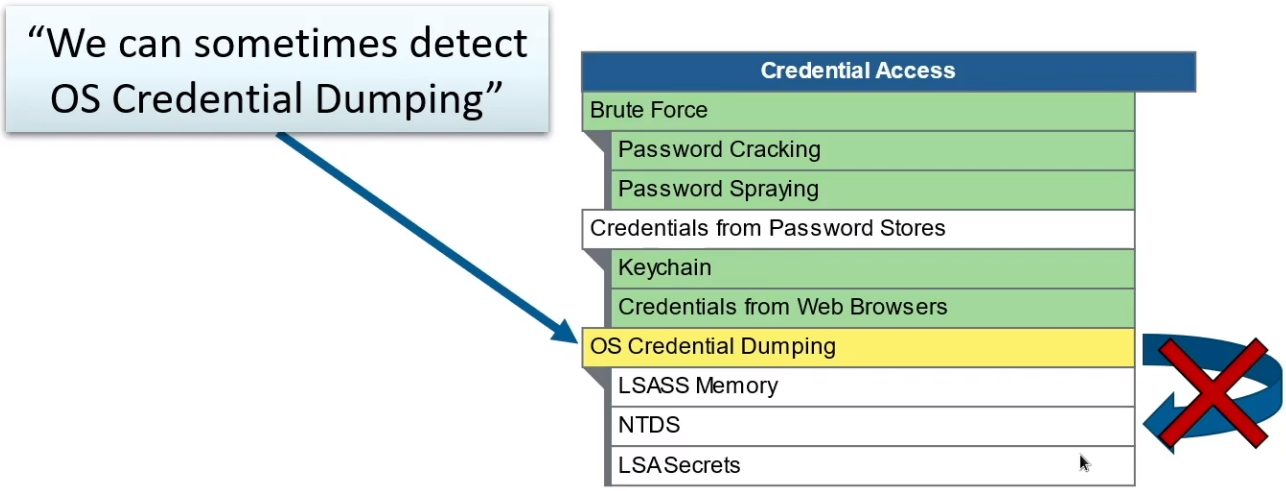
In the second step we need to decide the coverage scheme and how to cover technique and sub-technique. We can decide from 3 components (ordered to the most abstract from the most specific) :

1. TACTIC (ex:/ exfiltrate file should be hard on air-gapped network)
2. TECHNIQUE (ex:/ apply isolation/sandbox)
3. SUB-TECHNIQUE (ex:/ enable auit kerberos to log kerberos TGS request in order to detect kerberoasting)

In particular **technique and sub-technique inference** is an important topic to understand to gain a good view on the SOC environment







TIPS

- Be specific as possible
- Keep attention with infered accuracy (if unsure be skeptical!)
- Perfect/good ATT&CK matche isn't always possible....is totally fine

Take some time to decide (and explain) what you mean by **"coverage"**, what are you measuring and what is your method?

- **SIMPLE**
  "Can we detect it?" yes/no
- **DETECTION + MITIGATION**
  "Are we confident to detect it?" no/partially/mostly/yes
- **HYBRID**
  "Will execution of this technique cause problems?" score 1 to 100

Start with **simple** method to gain a first image and don't worry about accuracy, experience and maturity will define your final metric over- time

(3.1) ANALYZE COMPONENTS

Data sources are really variegated (they also include "Persona" as data surces) and every of that is linked with 1 or more technique

Persona

A malicious online profile representing a user commonly used by adversaries to social engineer or otherwise target victims

ID: DS0021

Platform: PRE

Collection Layer: OSINT

Version: 1.0

Created: 20 October 2021

Last Modified: 20 October 2021

Version Permalink

Data Components

Persona: Social Media

Established, compromised, or otherwise acquired social media personas

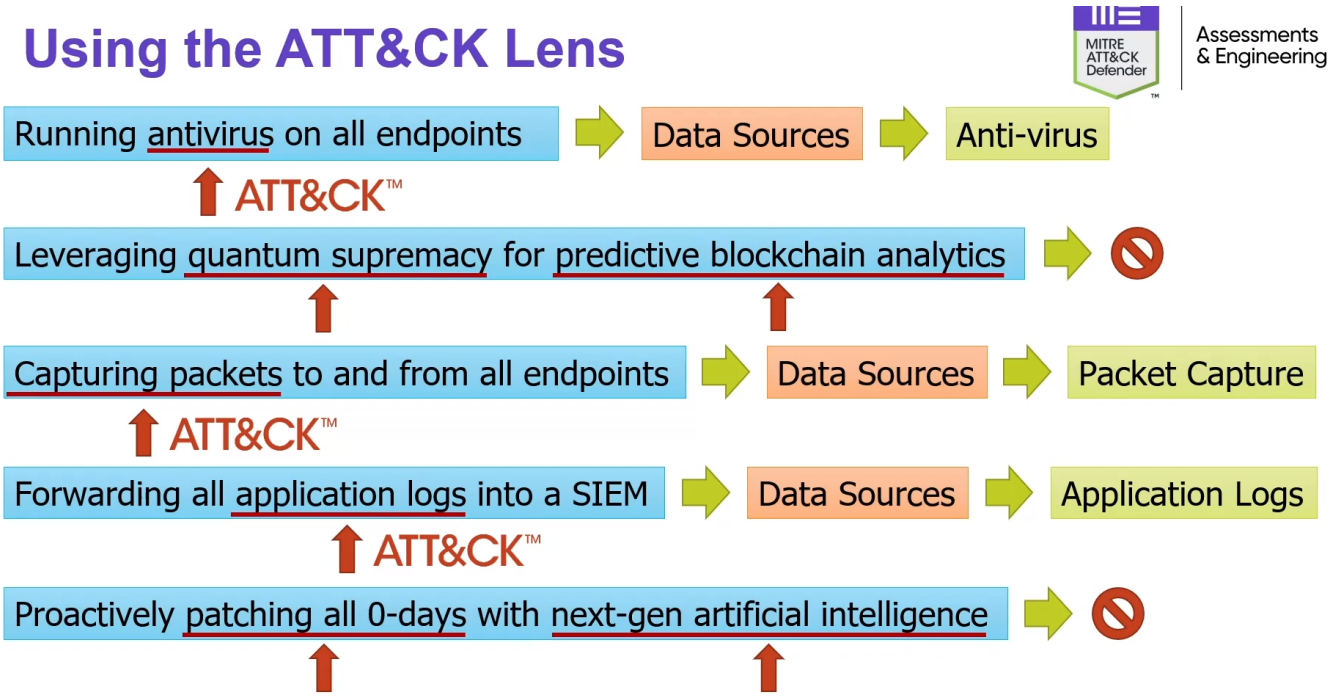
Domain	ID	Name	Detects
Enterprise	T1586	Compromise Accounts	Consider monitoring social media activity related to your organization. Suspicious activity may include personas claiming to work for your organization or recently modified accounts making numerous connection requests to accounts affiliated with your organization.Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access (ex: Phishing).
	.001	Social Media Accounts	Consider monitoring social media activity related to your organization. Suspicious activity may include personas claiming to work for your organization or recently modified accounts making numerous connection requests to accounts affiliated with your organization.Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access (ex: Spearphishing via Service).
Enterprise	T1585	Establish Accounts	Consider monitoring social media activity related to your organization. Suspicious activity may include personas

Most usefull and common are **Process Monitoring**, **Process command line parameter** and **File monitoring**. But why are usefull?

1. Every **SOC tap into data sources** in some way (logging, IDS, firewall, ecc...)
2. Understand what SOC does can infer in some kind of coverage

> Remember, **deploying =/= collecting =/= using** this is a difference that the assessment team should clearly understand in every context to a better compilation of the heatmap. This because coverage depends on how data sources are used

This is an example on how **translate natural language** interview/documentation **in Data Sources**



Than you compile separate heatmaps for each Data Source

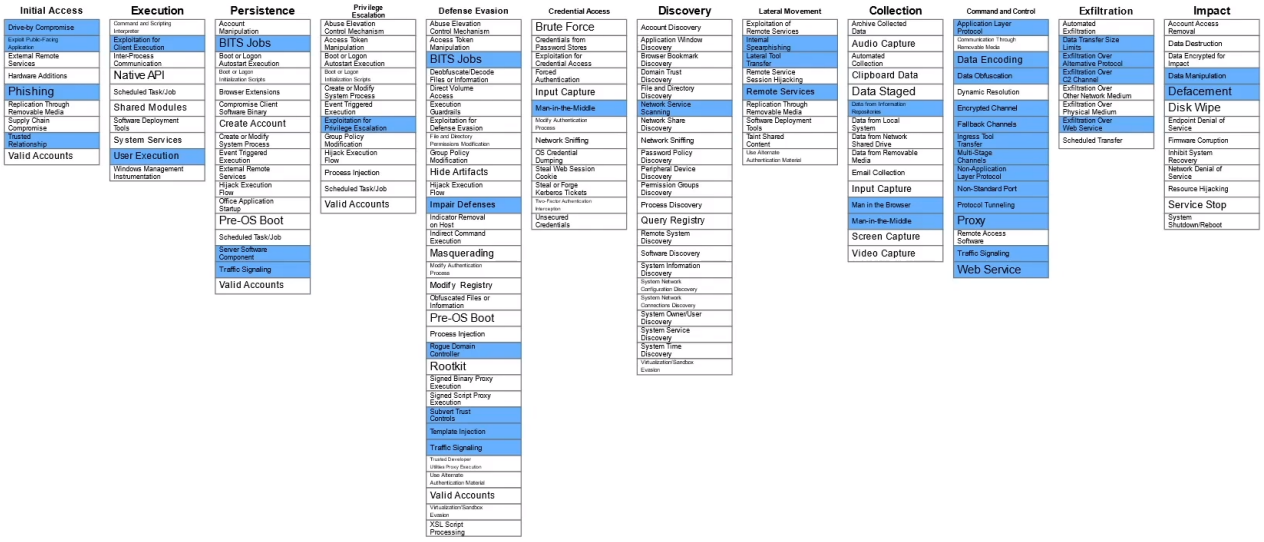
Anti-virus

Packet Capture

Application Logs

And you end to aggregating the different heatmaps to a unique one

Anti-virus + Packet Capture + Application Logs



You can also evaluate the datasources separated one-by-one (you need to decide the criteria)

DataSource	Event	Completeness	Timeliness	Availability	Score
Web application firewall logs	F5 logs	0	0	0	0.0
Web logs	Nginx logs	0	2	2	1.2
Web proxy	BlueCoat trafficlog	3	2	0	1.6
Web proxy	Nginx logs	0	0	0	0.0
Windows Error Reporting	Windows:1000,1001	0	5	4	2.6
Windows event logs	Windows:4724, 4738,4728,4732	1	0	0	0.4
Windows event logs	Windows:1102	0	0	0	0.0
Windows Registry	Windows:4657	0	4	4	2.4
Windows Registry	Sysmon:12	5	5	2	3.8
Windows Registry	Sysmon:13	1	5	5	3.4
Windows Registry	Sysmon:14	2	5	5	3.8
Windows Registry	Windows:4656	0	0	1	0.4
Windows Registry	Windows:4663	5	0	1	2.4
Windows Registry	Windows:4670	0	2	0	0.4
Windows Registry	Windows:4660	0	0	0	0.0
WMI Objects	Windows WMI:5857,5860,5861	4	4	1	2.8
WMI Objects	Sysmon:19	3	1	5	3.4

Source: ATTACKdatamap by Olaf Hartong

(3.2) ANALYZING ANALYTICS

ANALYTICS = Detection rules designed to detect specific behavior, in other words **how data sources are used**

```
Analytics -> Techniques -> Coverage Map
```

How can we make the upper equation?

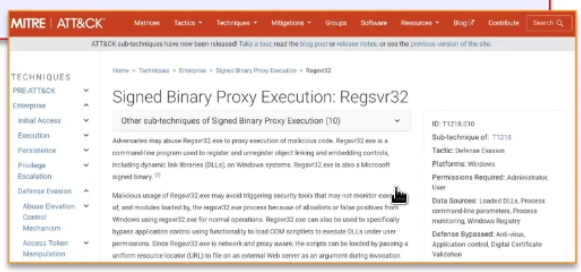
1. Finds the **Data Sources correlated with the analytics**
2. Determine what each "filter" is doing
3. **Map identifiers** in the filter **to ATT&CK techniques** (ID can be string/number in ATT&CK, metadata give clues and not all analytics are easy to map)
4. **For each retrieved technique give a coverage**

Here a quick example

```
processes = search Process:Create 1
regsvr_processes = filter processes where (
  parent_image_path == "*regsvr32.exe" and image_path != "*regsvr32.exe*"
 )                                    2
output regsvr_processes  4
```

https://car.mitre.org/analytics/CAR-2019-04-002/

1. This analytic looks at process monitoring
2. It's returning processes spawned by regsvr32.exe (but not itself)
3. "regsvr32.exe" maps to the technique Regsvr32 (ID: T1218.010)
4. It provides good coverage of it



3

(3.3) ANALYZE TOOLS

Tools are primary sources of detection (passively detection, active threat hunts and logging) knwoing how to coverage tool is essential but hard too

- Hard to understand/evaluate core functionality of every tool
- Often, market material is not the description on how is deployed
- Usually you need to treat tools as black-box giving margin error

Asking the SOC how they use the tool and look at analytics is complementary with this operation

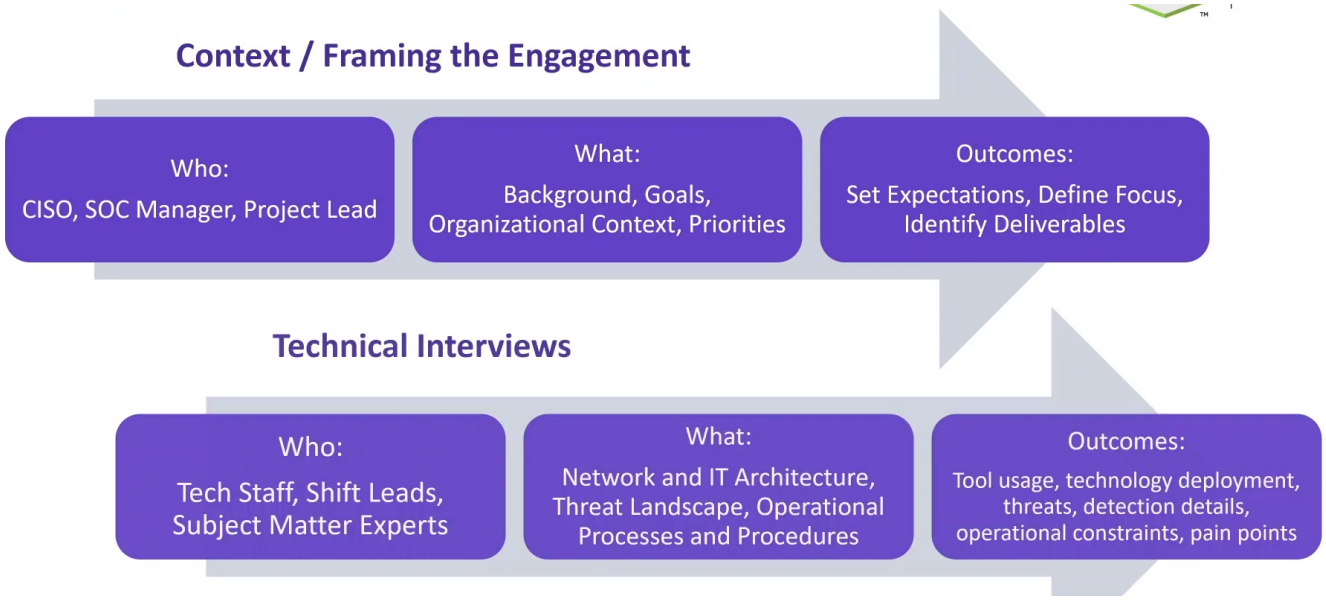
You can analyze tool with 3 on-point question

1. Where does the tool run? (endpoints, network appliance, email gateway)
2. How does the tool detect? (static indicator, dynamic or adversary artifacts based)
3. What data sources?

(4) STAFF INTERVIEW

This is a focal step, **not everything is stored within documentation, manuals or dump configurations** in addition after all interviews you can **understand SOC enviroment** (organization, business model, ecc...) and you would have a big picture

1. **Identify** the type of interview -> contextual or technical?



2. **Prepare** the interview
   You should have (at least) 1 leader + 1 notekeeper (avoid "gang-up"), duration is important and 45/90 minutes per team session is good. Can be usefull to **ask for a preliminary data request** usefull to construct pre-built questions (avoid favored question or one that suggest the solution).

   Also decide if interview 1 or more member (pros and cons for each choice) and remember that you objective here is to extract **Organizational Attributes** and **Technology**.

   Stay neutral, avoid bias and understand different perspective
3. **Conduct** the interview
   Identify the gaps and the strenght and drill down deeper topics, different team need different qustion perspective. Capture jargon and terminology used by the SOC
4. Process the finding
   Compare notes with you collagues and cleaned as soon as they are clear on your head, capture conflicting reports/statement on different problem/member. Identify ATT&CK topics

(5) COMMUNICATE WITH ATT&CK

In this phase we start planning and compile the **heatmap**

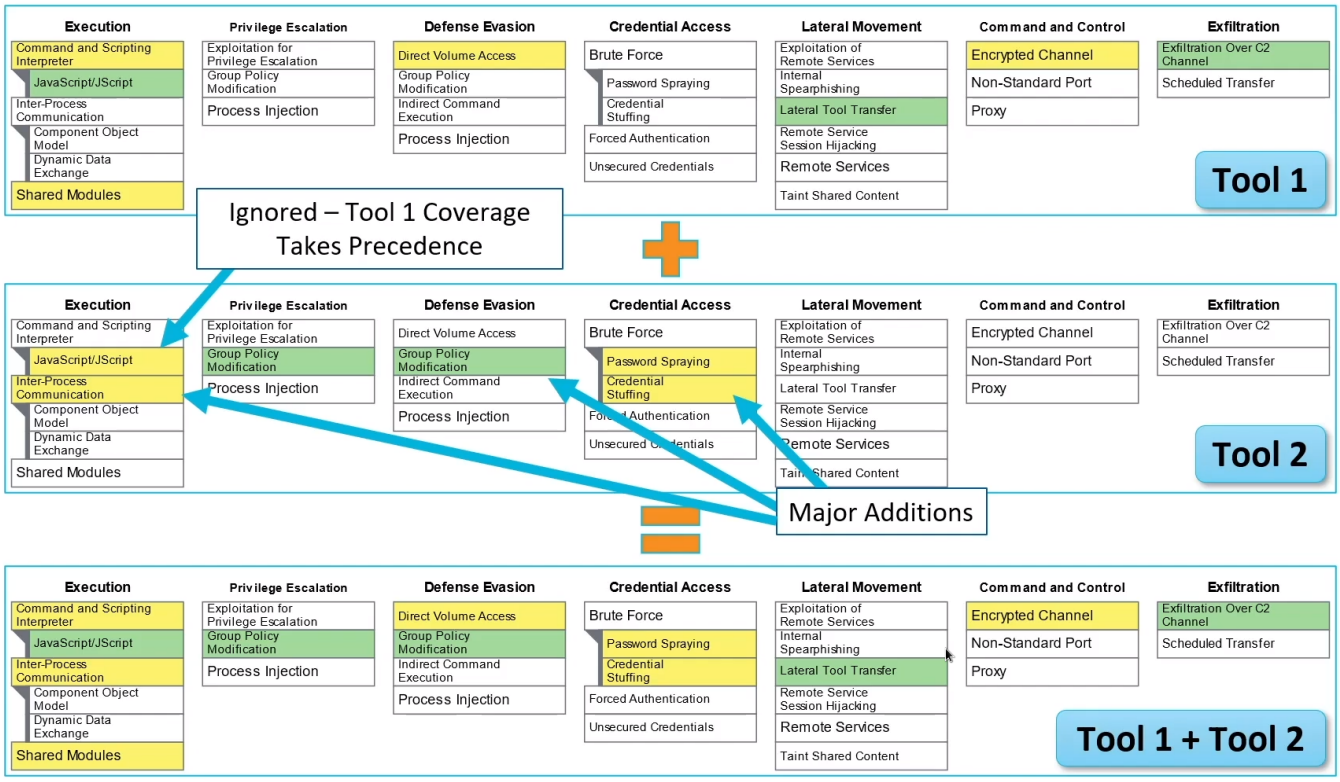
```
HeatMaps = Scope + Measurement + Color Scheme
```

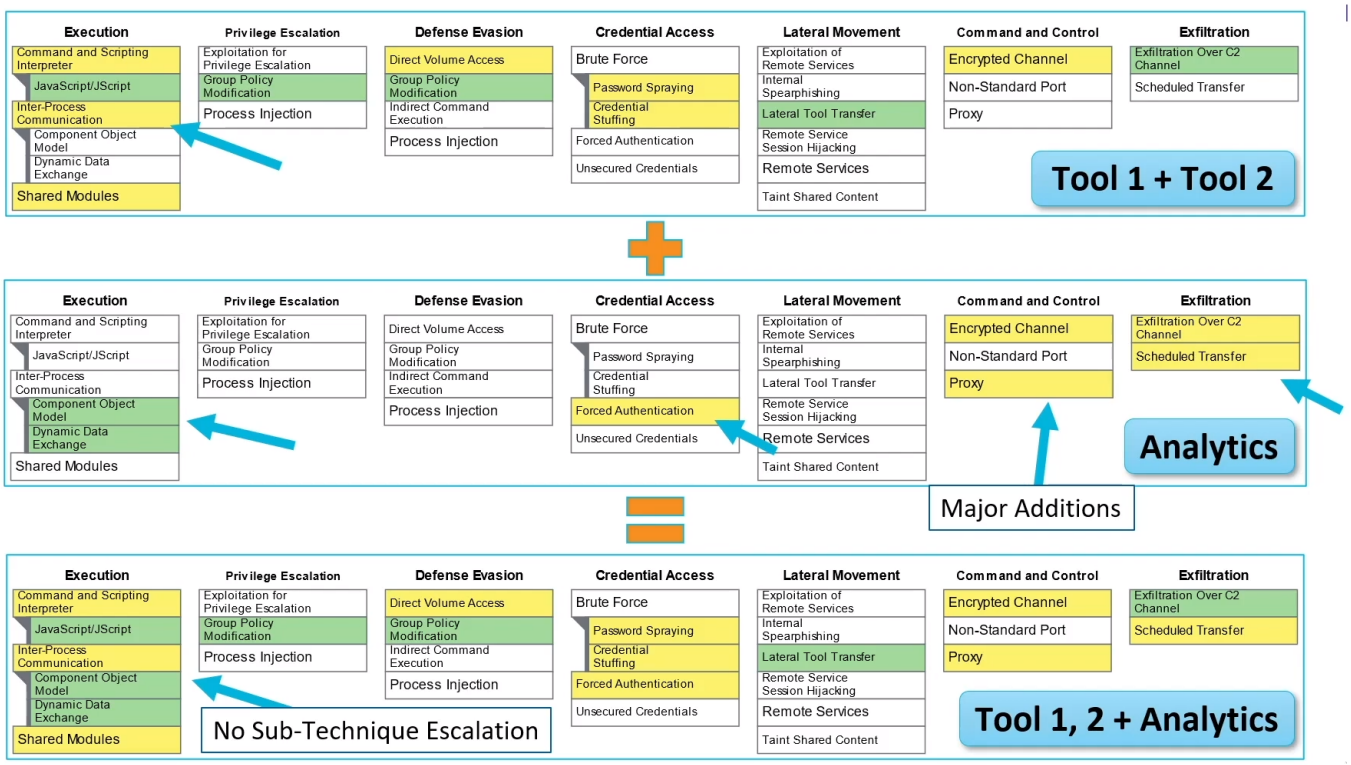
The heatmaps are really usefull because they communicate in a quick and clear way the results of the assessments.

- **Don't use too many categories**, you need to paint broad strokes
- Put just the **right info on the right layer**
- **Different heatmap for different team members** (leadership want big picture, staff need details)
- Add and explain **justification for every metrics**

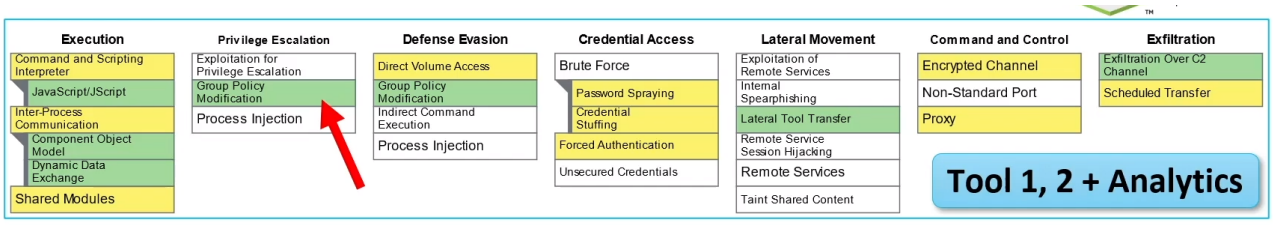
Heatmaps have their cons, that you need to make clear to your clients : 1) Coverage doesn't always allign with real attack execution 2) Coverage are not static (attacker and defnder rotate) 3) They are approximate

Start from single heatmap for tool and analytics and use aggregation to build the final scheme

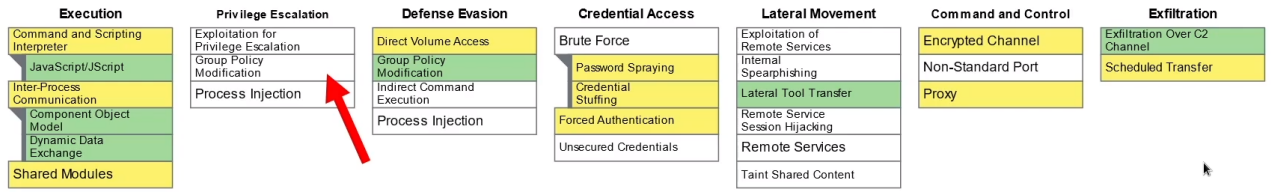




Last but not least, remind to aggregate results from interview and documentations



- **Via red team: "The SOC *never* detects when we escalate privileges"**



We can simplify this procedure with an equations (remember that every context need some changes at your procedure)

```
Tool Coverage + Analytic Coverage + Interview Positives - Interview Negatives
```

Avoid red color (look antagonistic), decide how many categories include and the type of coverage (usually detection is fine but can change based on what the clients require)

(6) PROPOSING RECOMMENDATIONS

You will NEVER compile and deliver the heatmap without recommendations on how to improve that heatmap :

- Provide small sets where SOC need to focus
- Starting spot
- **Technique Prioritization**/Roadmap (short-term wins, technique with low coverage/ relevant on the immediate)
- Provide at the SOC your methodology so they can try to figure out by themselves

Process Refinement -> What they could cover tomorrow (communication, documentation)

- Add Analytics = + coverage
- Add new tools = free/commercial, focus on tool types, coverage-budget, look previous analysis
- Ingesting Data Sources = easy to ingest, usefull coverage, roll-out strategies, tooling+analytics data sources recommendations
- Implementing Mitigations = Hard to verify and keep up-to-date

Always propose a follow-up, usually this is the cycle to improve based on ATT&CK