AUTOMATING ATT&CK COVERAGE WITH DETT&CT

22 NOVEMBER 2022

Sirius Security

#DEFINE ME

RUBEN BOUMAN

- Freelance Cyber Defense Expert
- Co-owner Sirius Security
- Roots in development
  - Love Python
- 11 years of experience in Info Security
- Co-developer of open-source projects:
  - DeTT&CT framework
  - Dettectinator
- Contributor to open-source projects

@rubinatorz

AGENDA

- Short introduction to ATT&CK
- ATT&CK in practice using DeTT&CT
- Automation with Dettectinator

- Ask questions!

ATT&CK: WIKIPEDIA

“Wikipedia on cyber attacks”

Example

Phishing

Sub-techniques (3)

ID	Name
T1566.001	Spearphishing Attachment
T1566.002	Spearphishing Link
T1566.003	Spearphishing via Service

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns.

Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source.

TACTICS, TECHNIQUES, AND PROCEDURES (TTP)

- Origin: US Department of Defense
- Terminology has been adopted within cyber security

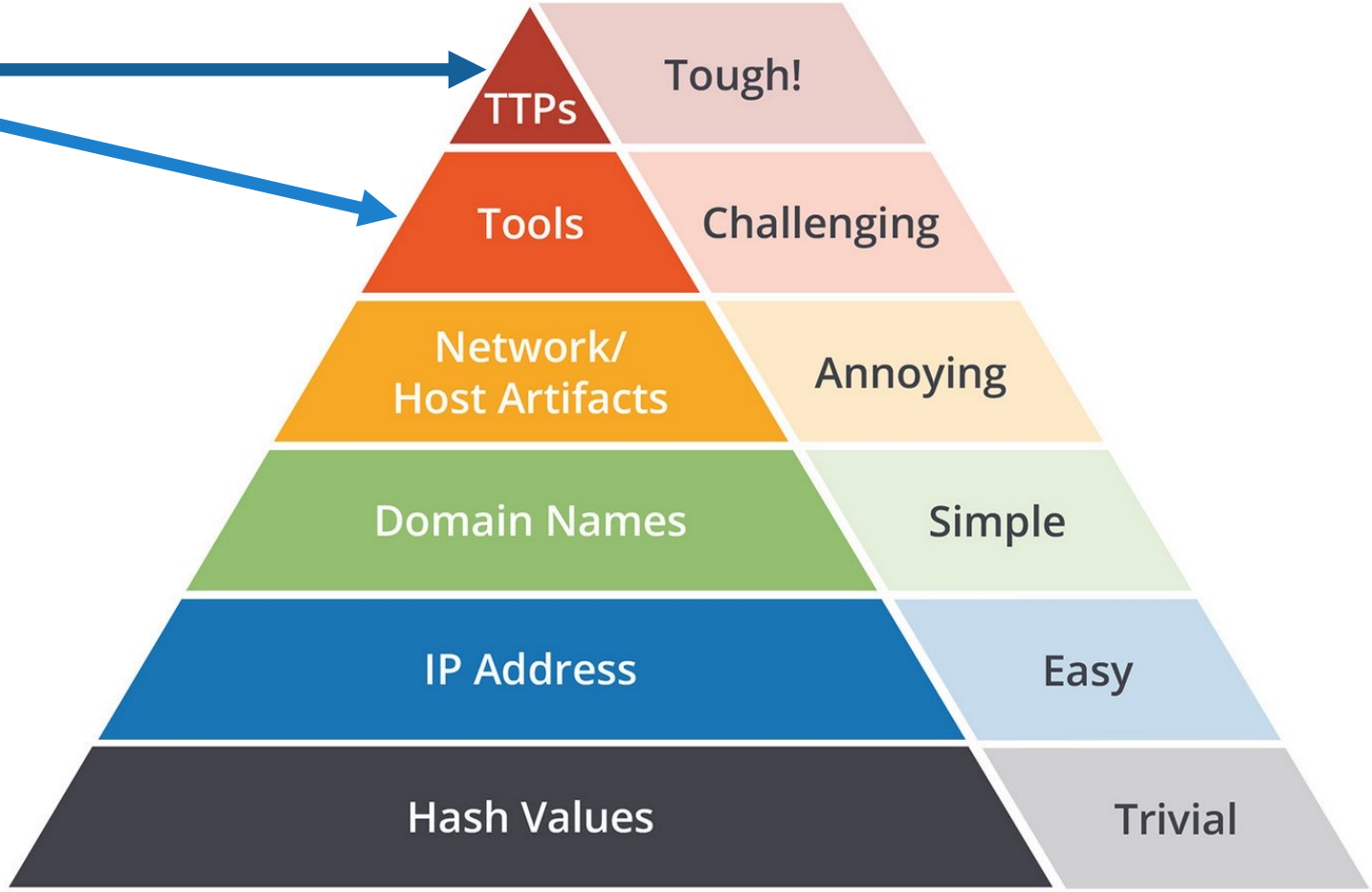
- Analogy of car ownership[1]
  - Tactics (goals)
    - Providing fuel
    - Cleaning
    - **Preventive maintenance**
  - Techniques (how goals are achieved)
    - **Changing the oil**
    - Rotating tires
    - Replacing breaks
  - Procedures (specific technique implementation)
    - **VW Golf 7** (specific to the car: type of oil, type of filter, location of the drain plug, tools required, etc.)

[1] https://posts.specterops.io/whats-in-a-name-ttps-in-info-sec-14f24480ddcc

ATT&CK AND THE PYRAMID OF PAIN

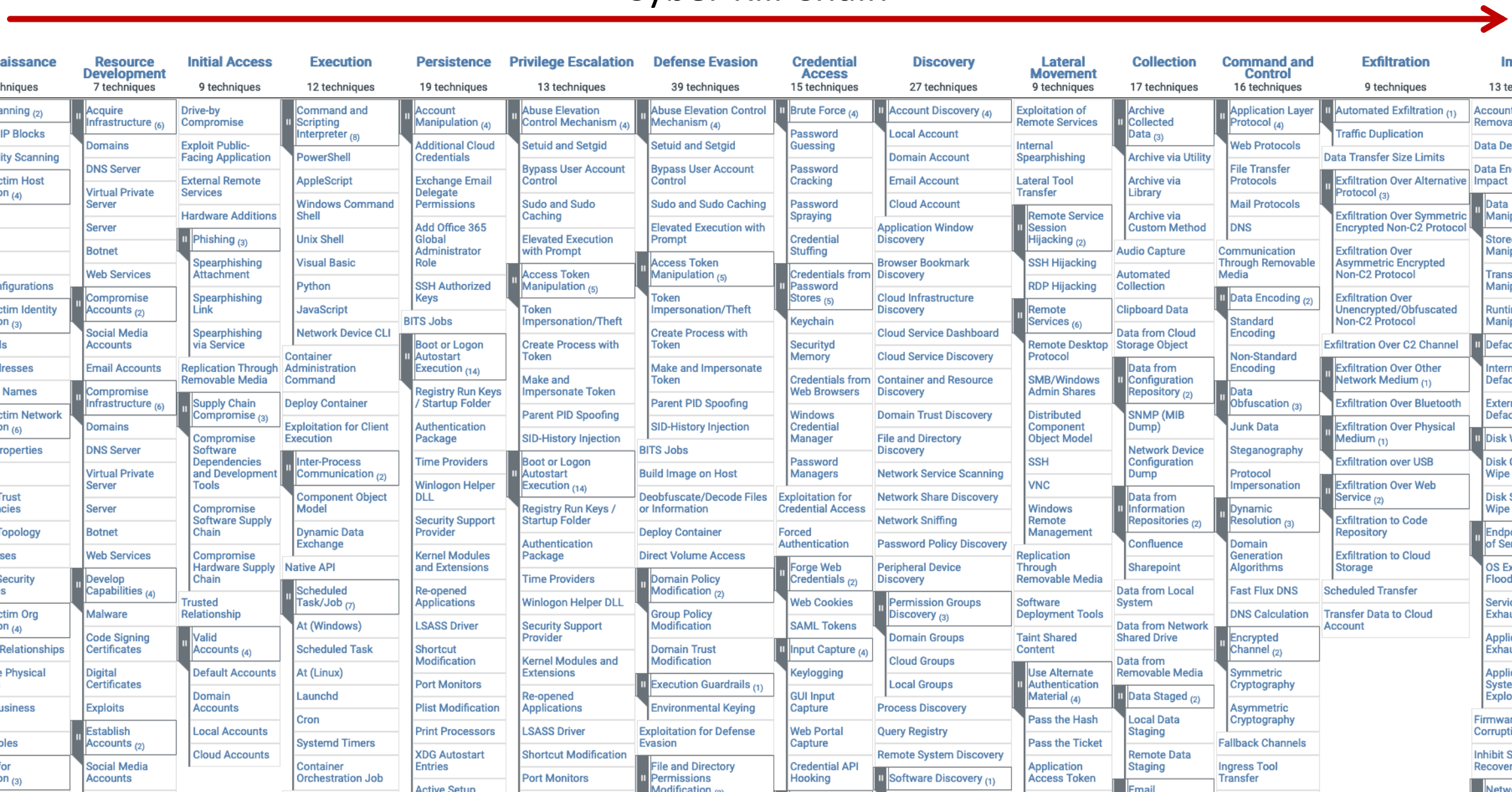
ATT&CK®

"Wikipedia on cyber attacks"



ATT&CK MATRIX

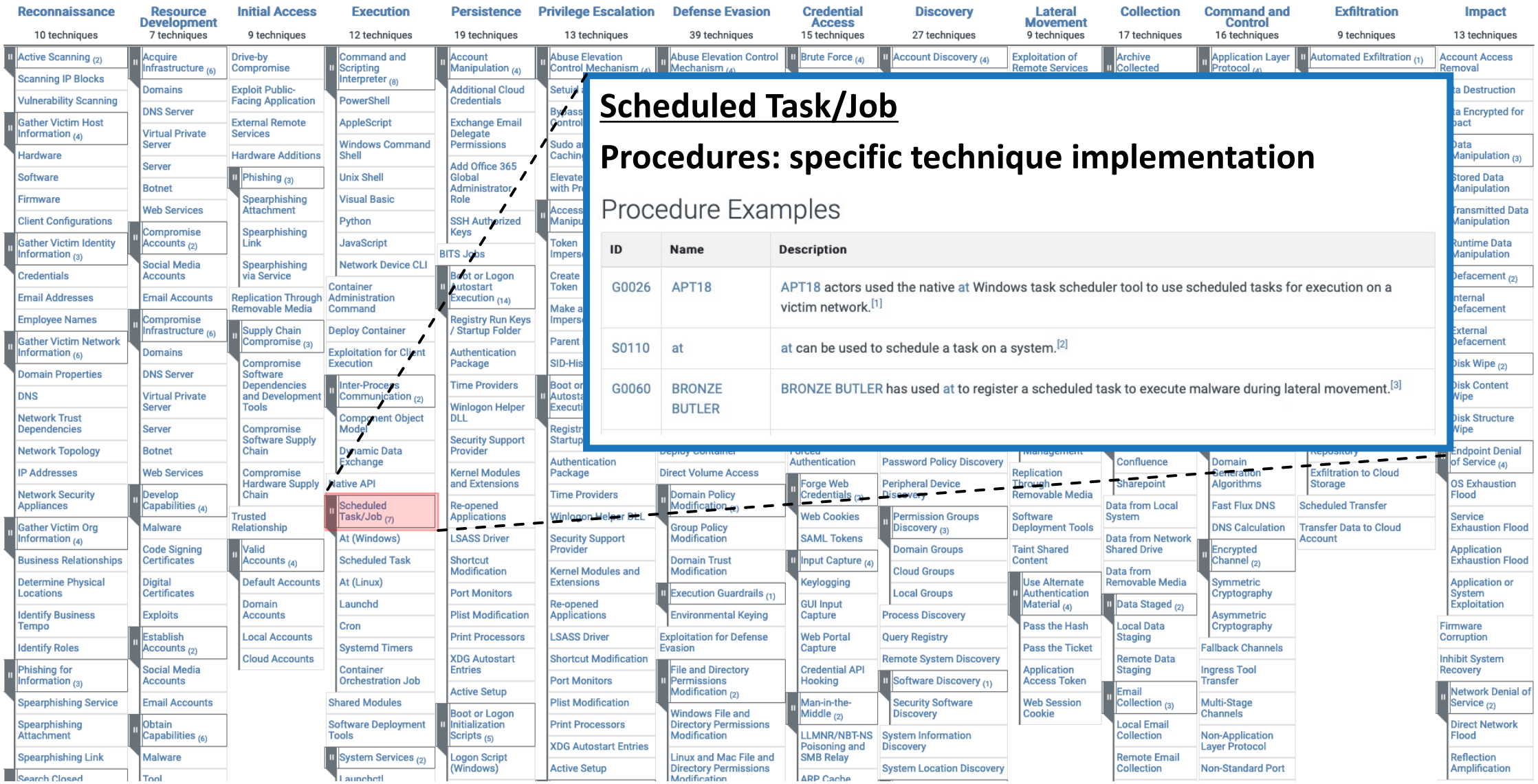
Cyber Kill Chain



TACTICS, TECHNIQUES, AND PROCEDURES (TTP)

Tactics: the adversary's technical goals

Techniques: how the goals are achieved



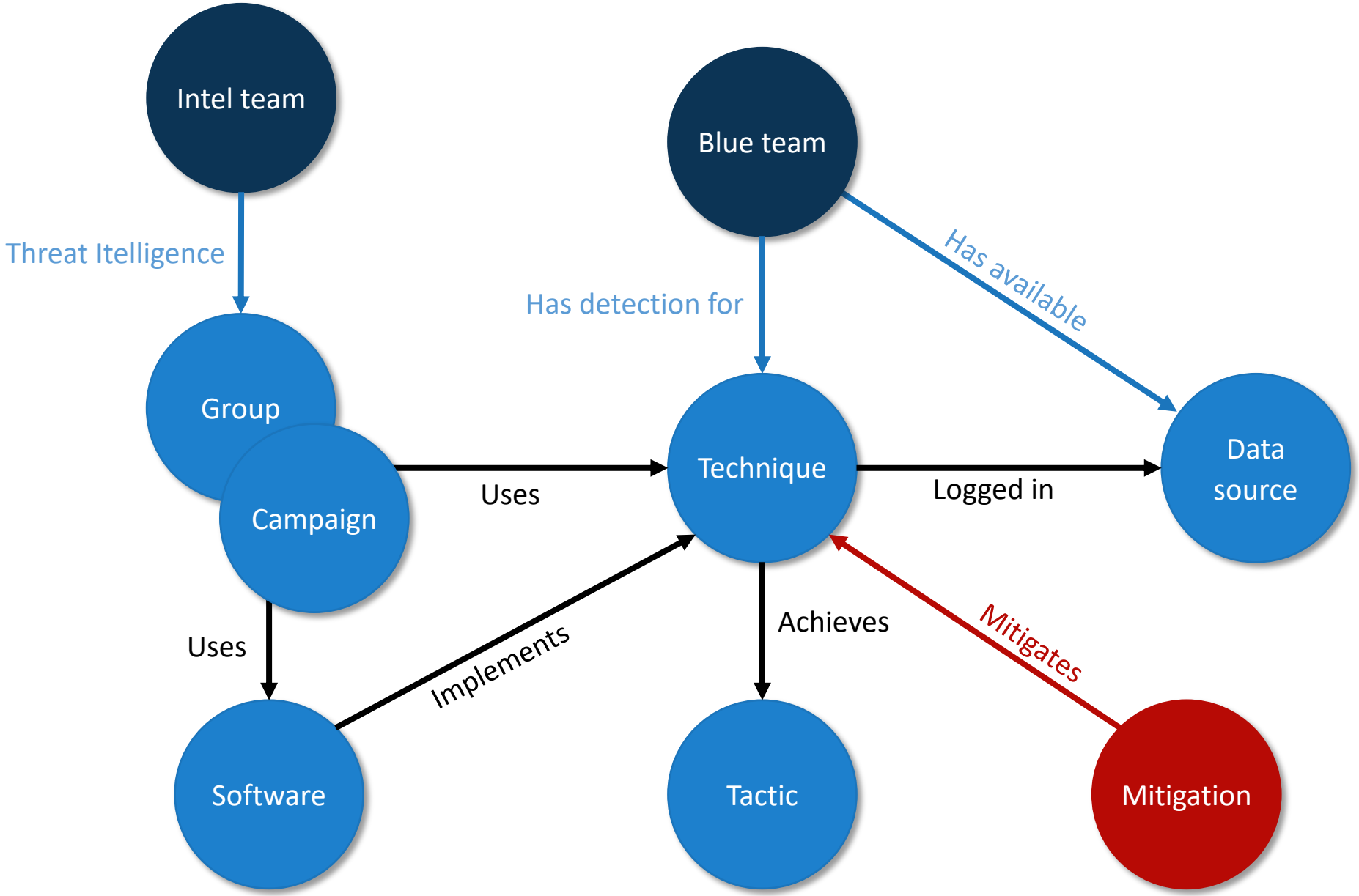
Scheduled Task/Job

Procedures: specific technique implementation

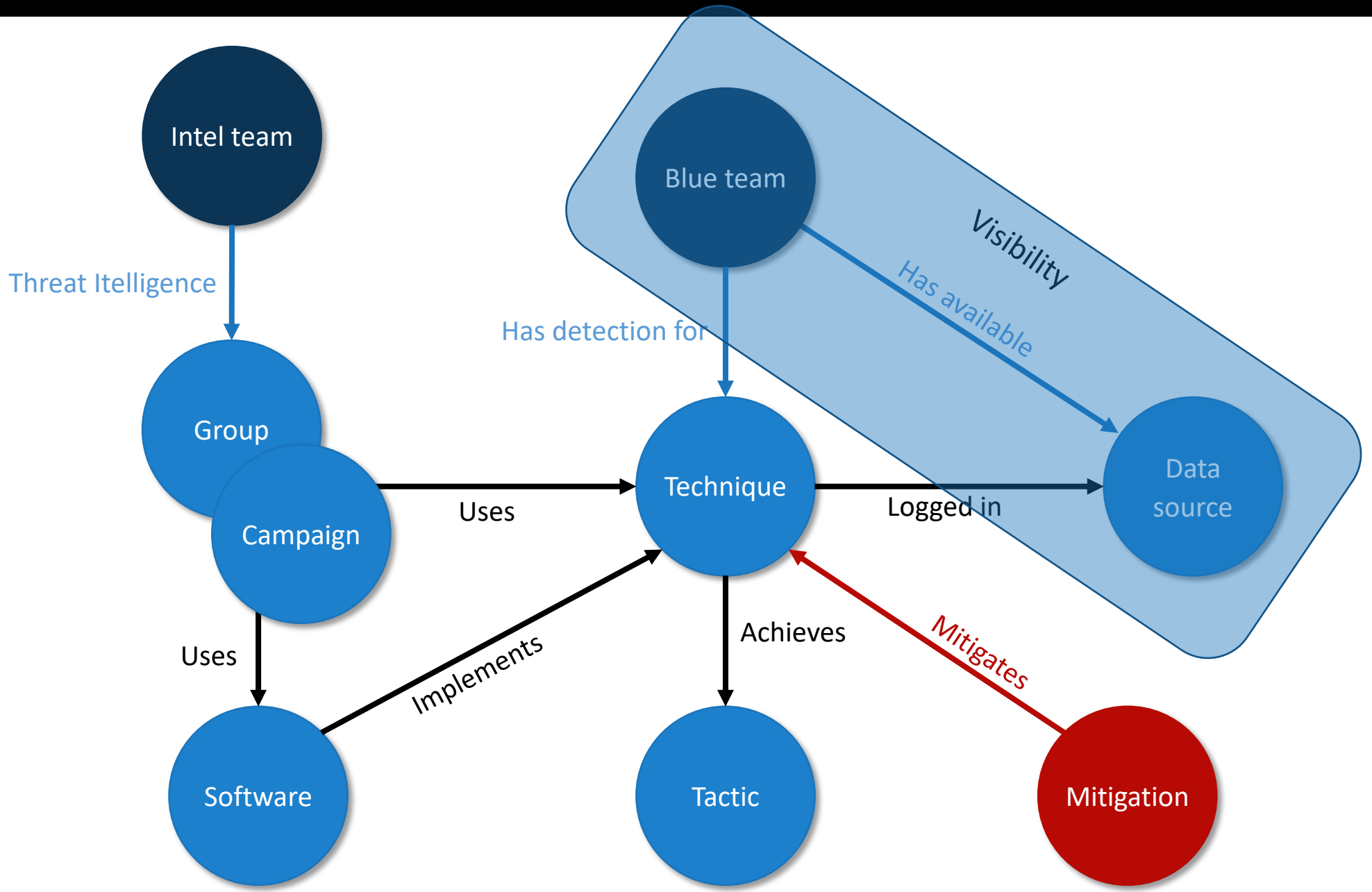
Procedure Examples

ID	Name	Description
G0026	APT18	APT18 actors used the native at Windows task scheduler tool to use scheduled tasks for execution on a victim network.[1]
S0110	at	at can be used to schedule a task on a system.[2]
G0060	BRONZE BUTLER	BRONZE BUTLER has used at to register a scheduled task to execute malware during lateral movement.[3]

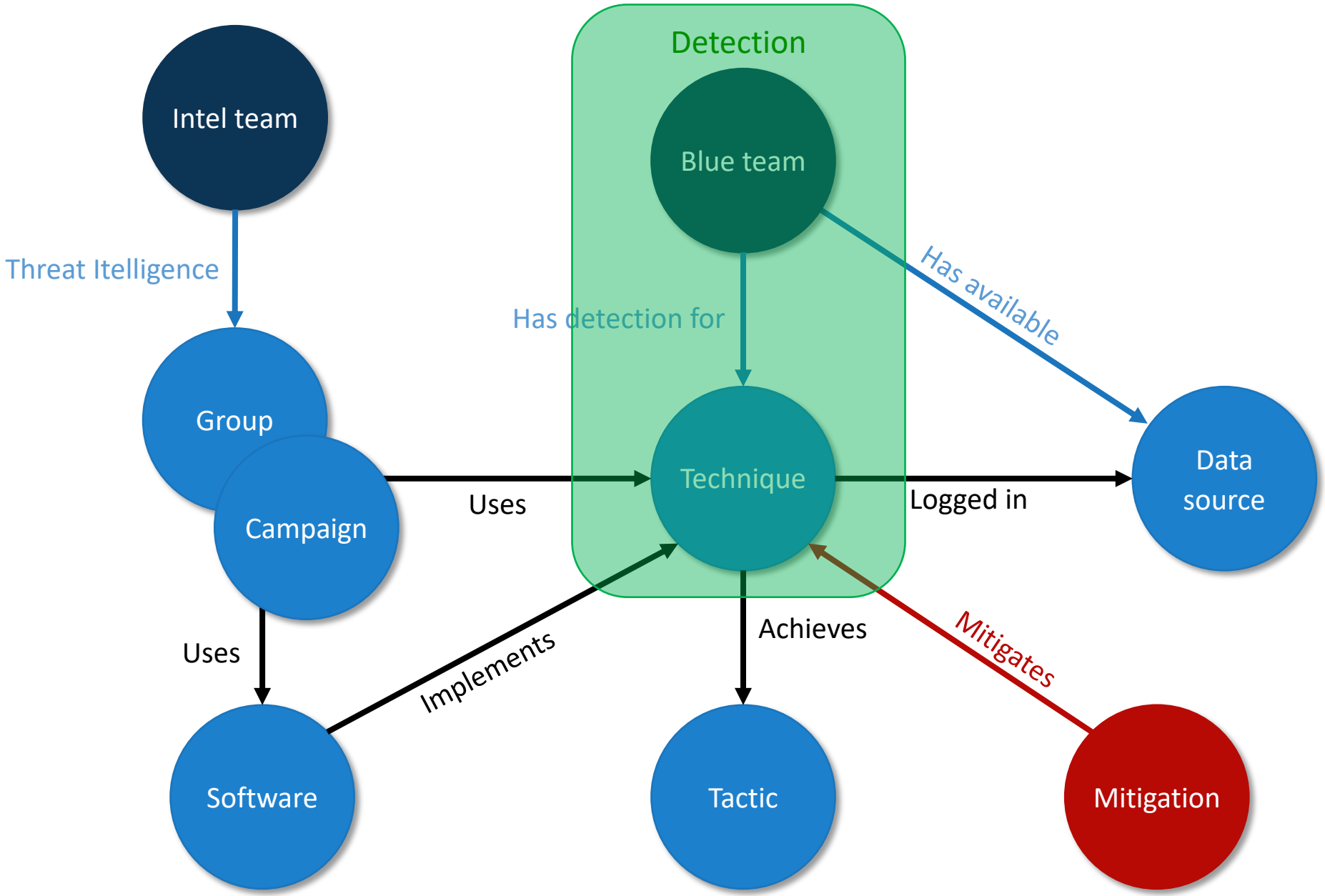
ATT&XONOMY


Intel team
Blue team
Threat Itelligence
Has detection for
Has available
Group
Campaign
Technique
Data source
Uses
Logged in
Uses
Implements
Achieves
Mitigates
Software
Tactic
Mitigation

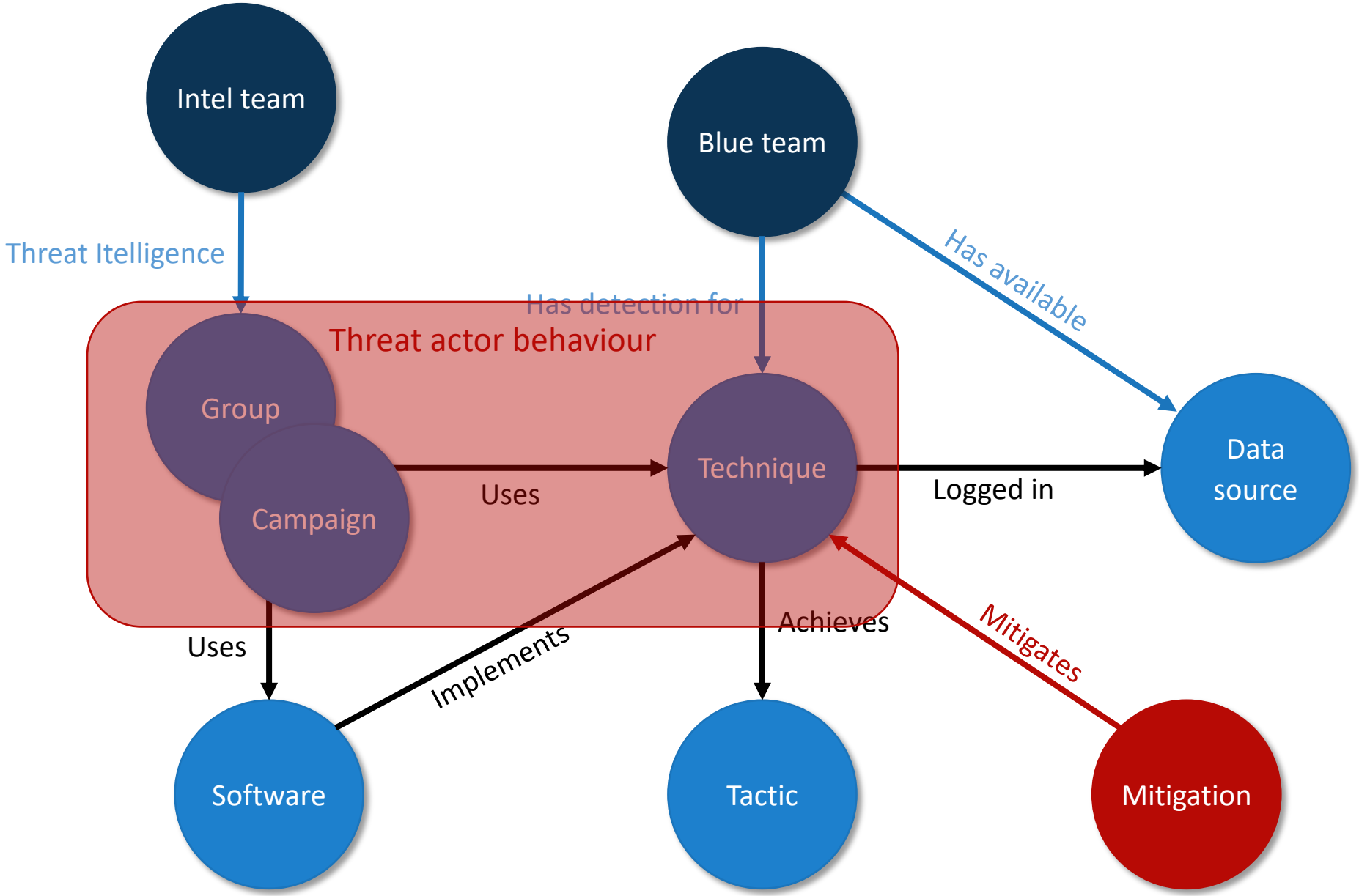
ATT&XONOMY


Intel team
Threat Itelligence
Group
Campaign
Uses
Uses
Software
Implements
Blue team
Has detection for
Technique
Visibility
Has available
Data source
Logged in
Achieves
Tactic
Mitigates
Mitigation

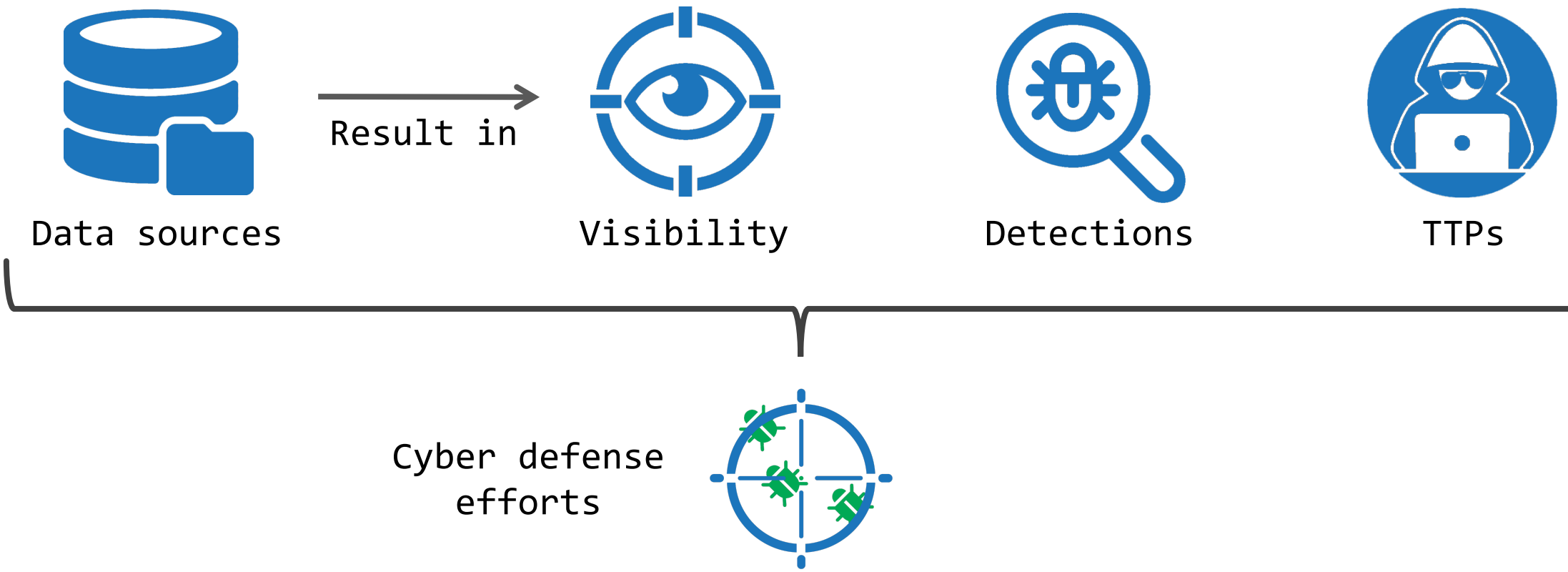
ATT&XONOMY


Detection
Intel team
Blue team
Threat Itelligence
Has detection for
Has available
Group
Campaign
Technique
Data source
Uses
Logged in
Uses
Implements
Achieves
Mitigates
Software
Tactic
Mitigation

ATT&XONOMY

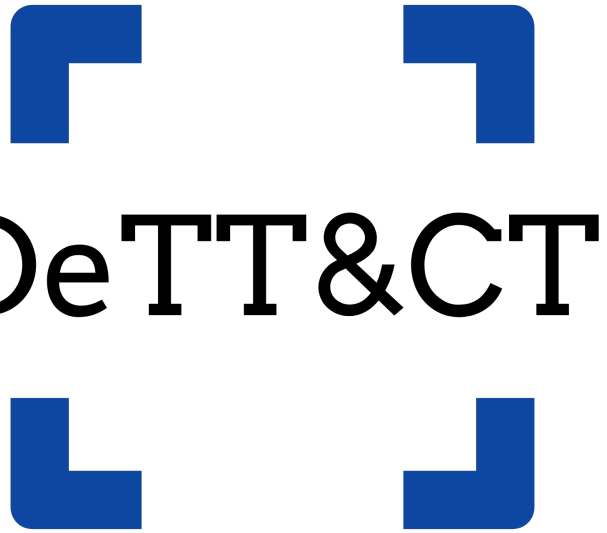

Intel team
Blue team
Threat Itelligence
Has available
Has detection for
Threat actor behaviour
Group
Campaign
Technique
Uses
Logged in
Data source
Uses
Implements
Achieves
Mitigates
Software
Tactic
Mitigation

CHALLENGE: WHERE DO WE START OUR CYBER DEFENSE EFFORTS



DETECT TACTICS, TECHNIQUES & COMBAT THREATS

- Solution to administrate, score and compare:
  - Data source quality
  - Visibility
  - Detections
  - Threat actor behaviours
- Based on MITRE ATT&CK
  - Creates overviews to load into ATT&CK Navigator
  - Supports ATT&CK Enterprise, Mobile and ICS
- The main goal of DeTT&CT:
  - Identify gaps in detection and visibility
  - Integrate threat intelligence to prioritise work
- Consists of:
  - Framework
  - Editor
  - Methodology including scoring tables



`github.com/rabobank-cdc/DeTTECT`

DATA SOURCES: WHAT DO WE LOG

- Identify data sources

ID: T1055

Sub-techniques: T1055.001, T1055.002, T1055.003, T1055.004, T1055.005, T1055.008, T1055.009, T1055.011, T1055.012, T1055.013, T1055.014

Tactics: Defense Evasion, Privilege Escalation

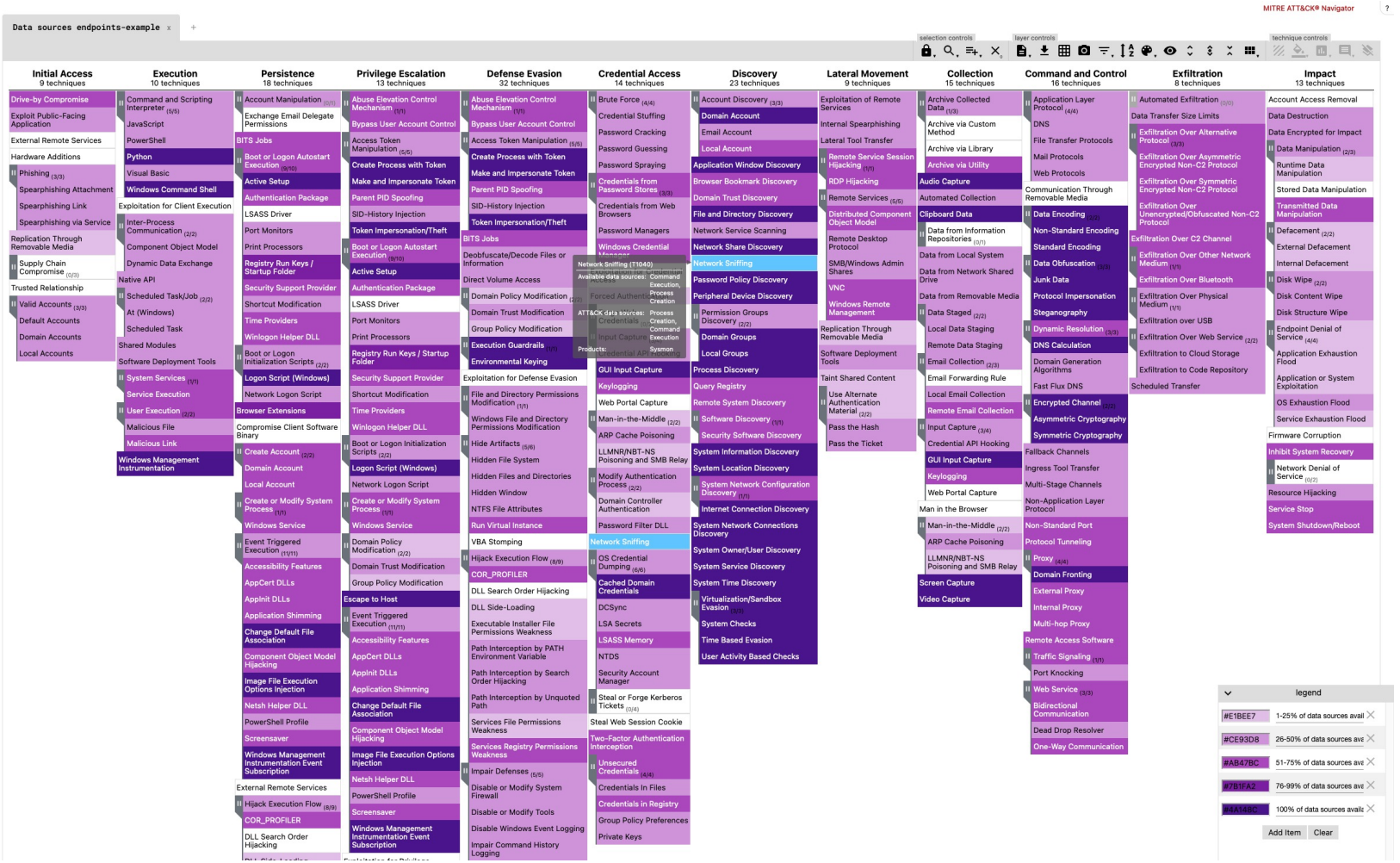
Platforms: Linux, Windows, macOS

Defense Bypassed: Anti-virus, Application control

CAPEC ID: CAPEC-640

Detection

ID	Data Source	Data Component
DS0022	File	File Metadata
		File Modification
DS0011	Module	Module Load
DS0009	Process	OS API Execution
		Process Access
		Process Modification



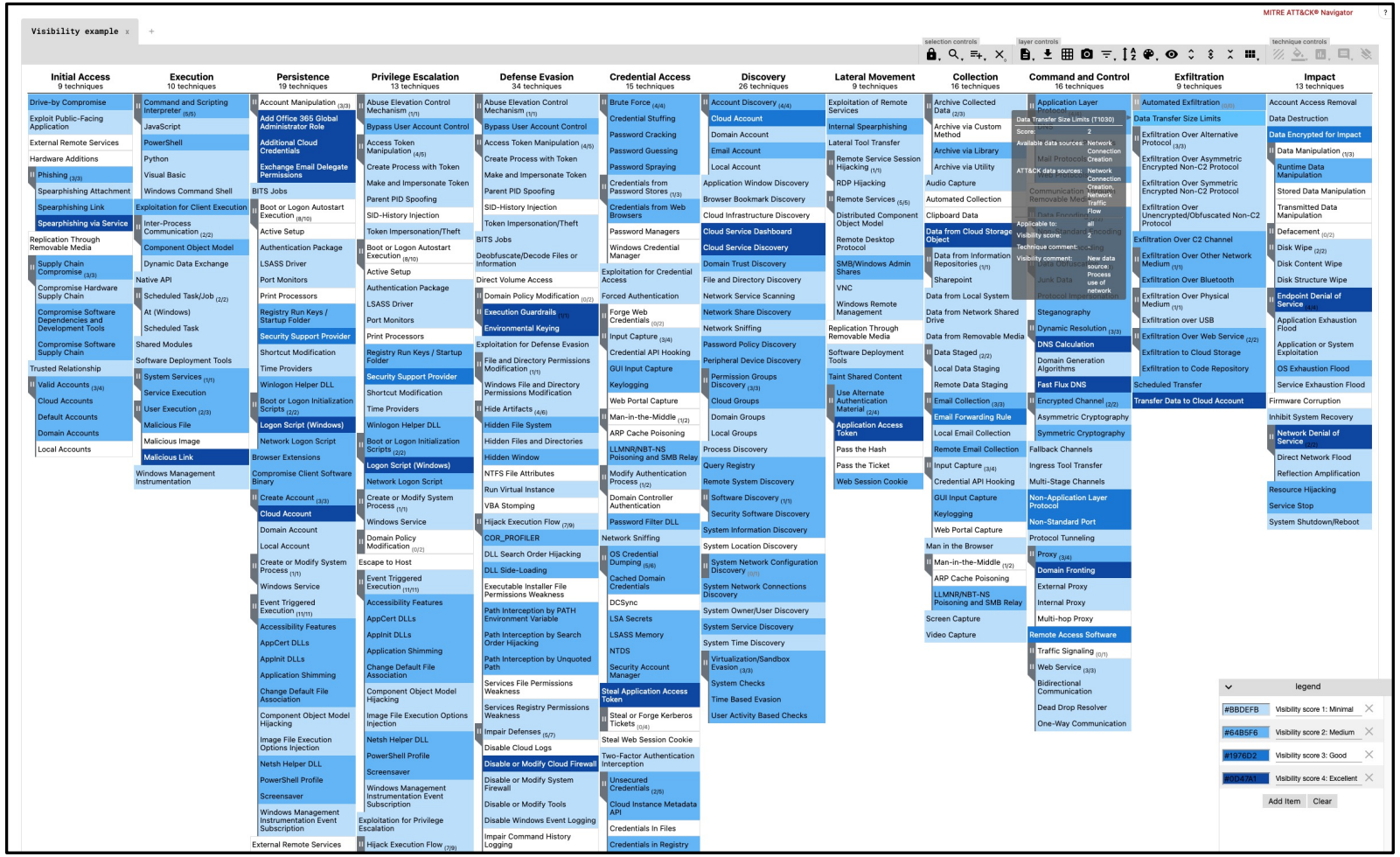
- Score data quality
  - device completeness
  - field completeness
  - timeliness
  - consistency and retention

VISIBILITY: WHAT CAN WE SEE?

- More detailed look at data sources
- Score visibility using scoring table

Visibility scores

Score	Score name	Description
0	None	No visibility at all.
1	Minimal	Sufficient data sources with sufficient quality available to be able to see one aspect of the technique's procedures.
2	Medium	Sufficient data sources with sufficient quality available to be able to see more aspects of the technique's procedures compared to "1/Minimal".
3	Good	Sufficient data sources with sufficient quality available to be able to see almost all known aspects of the technique's procedures.
4	Excellent	All data sources and required data quality necessary to be able to see all known aspects of the technique's procedures are available.

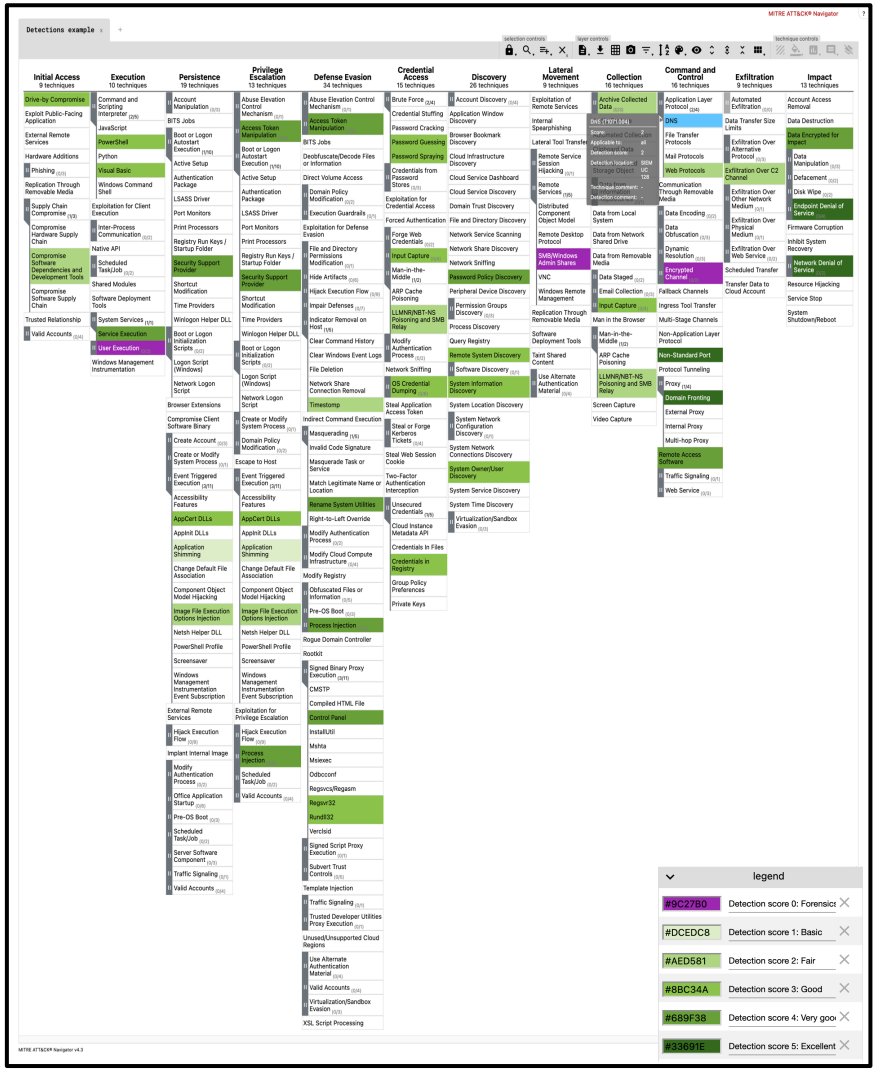


DETECTION: WHAT IS OUR DETECTION COVERAGE?

- Map all detections to their appropriate techniques
- Score detection using scoring table

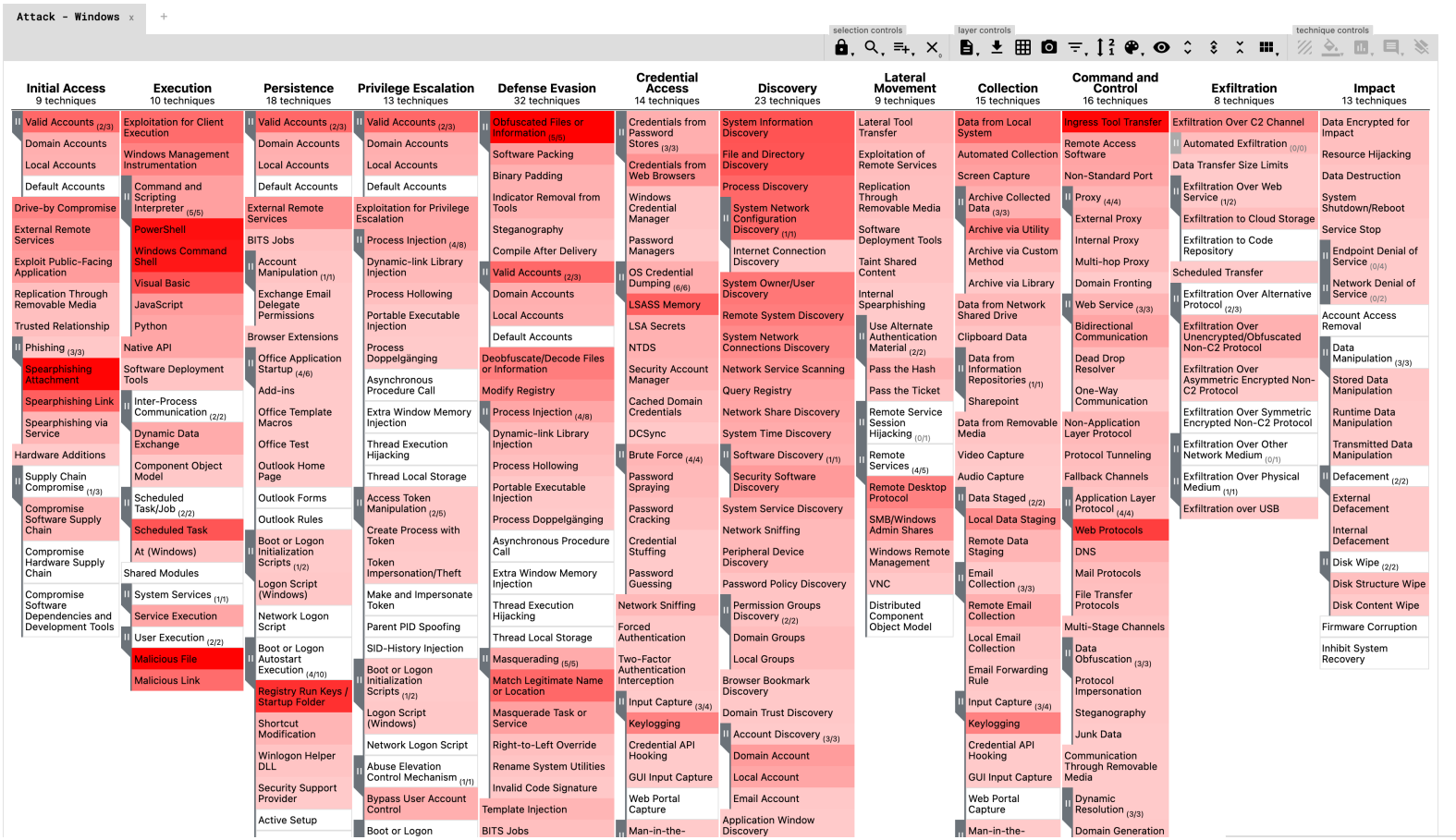
Detection scores

Score	Score name	Description
-1	None	No detection.
0	Forensics / context	No detection, but the technique is being logged for forensic purposes and can be used to provide context.
1	Basic	Detection is in place using a basic signature to detect a specific part(s) of the technique's procedures. Therefore, only a very small number of aspects of the technique are covered. Hence number of false negatives is high and possible (but not necessarily) a high false positive rate. Detection is possibly not real time.
2	Fair	The detection no longer only relies on a basic signature but makes use of a (correlation) rule to cover more aspects of the technique's procedures. Therefore, the number of false negatives is lower compared to "1/Poor" but may still be significant. False positives may still be present. Detection is possibly not real time.
3	Good	Effective in detecting malicious use of the technique by making use of more complex analytics. Many known aspects of the technique's procedures are covered. Bypassing detection by means of evasion and obfuscation could be possible. False negatives are present. False positives may still be present but are easy to recognize and can possibly be filtered out. Detection is real time.
4	Very good	Very effective in detecting malicious use of the technique in real time by covering almost all known aspects of the technique's procedures. Bypassing detection by means of evasion and obfuscation methods is harder compared to level "3/good". The number of false negatives is low but could be present. False positives may still be present but are easy to recognize and can possibly be filtered out.
5	Excellent	Same level of detection as level "4/very good" with one exception: all known aspects of the technique's procedures are covered. Therefore, the number of false negatives is lower compared to level "4/very good".



GROUPS: WHAT ARE ATTACKERS DOING?

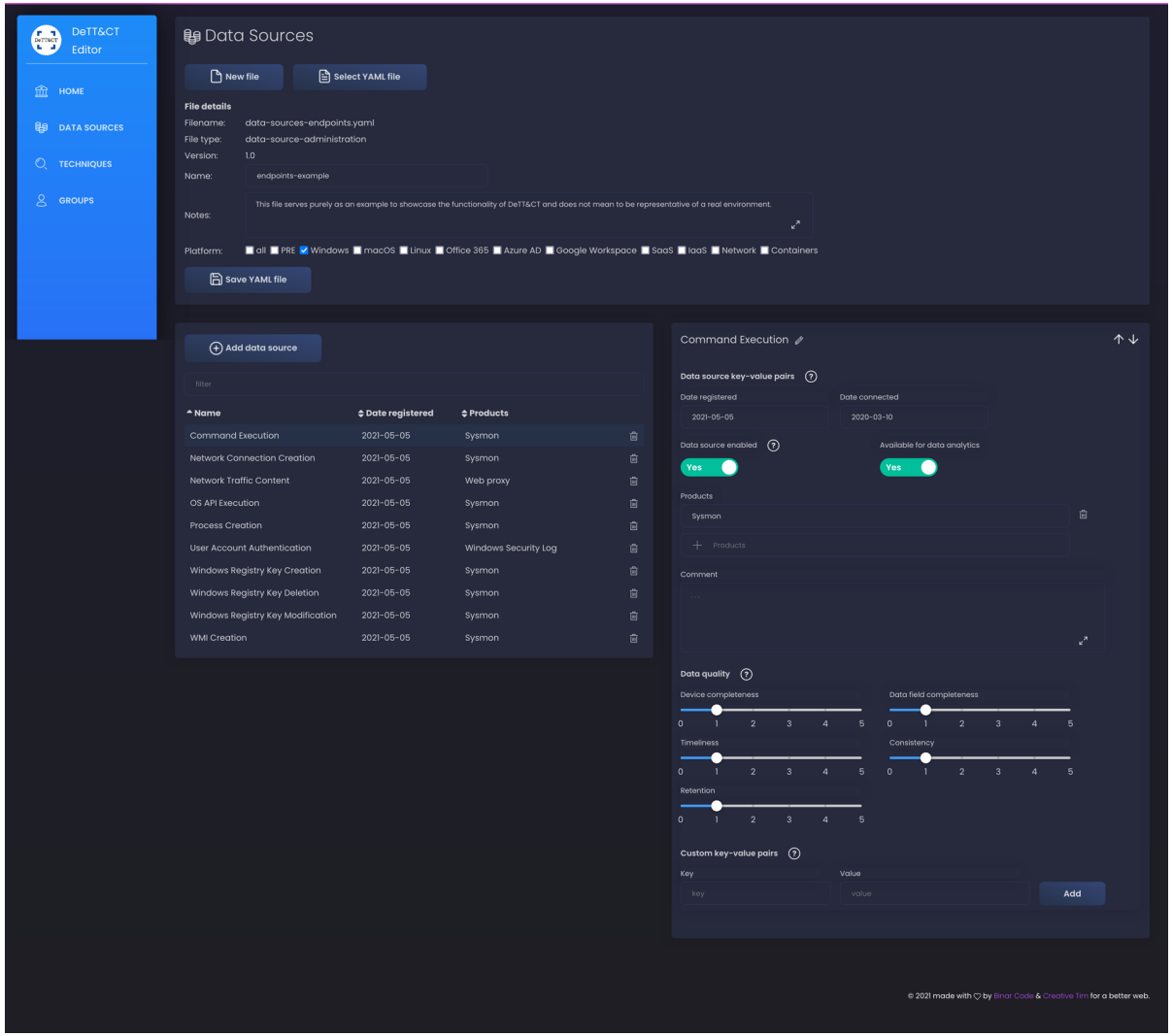
- Generate heat maps
  - Threat actor group data from ATT&CK
  - Own intel stored in a group YAML file
  - Threat actor data from third parties *1
- Compare threat actors



*1 https://github.com/rabobank-cdc/DeTTECT/tree/master/threat-actor-data

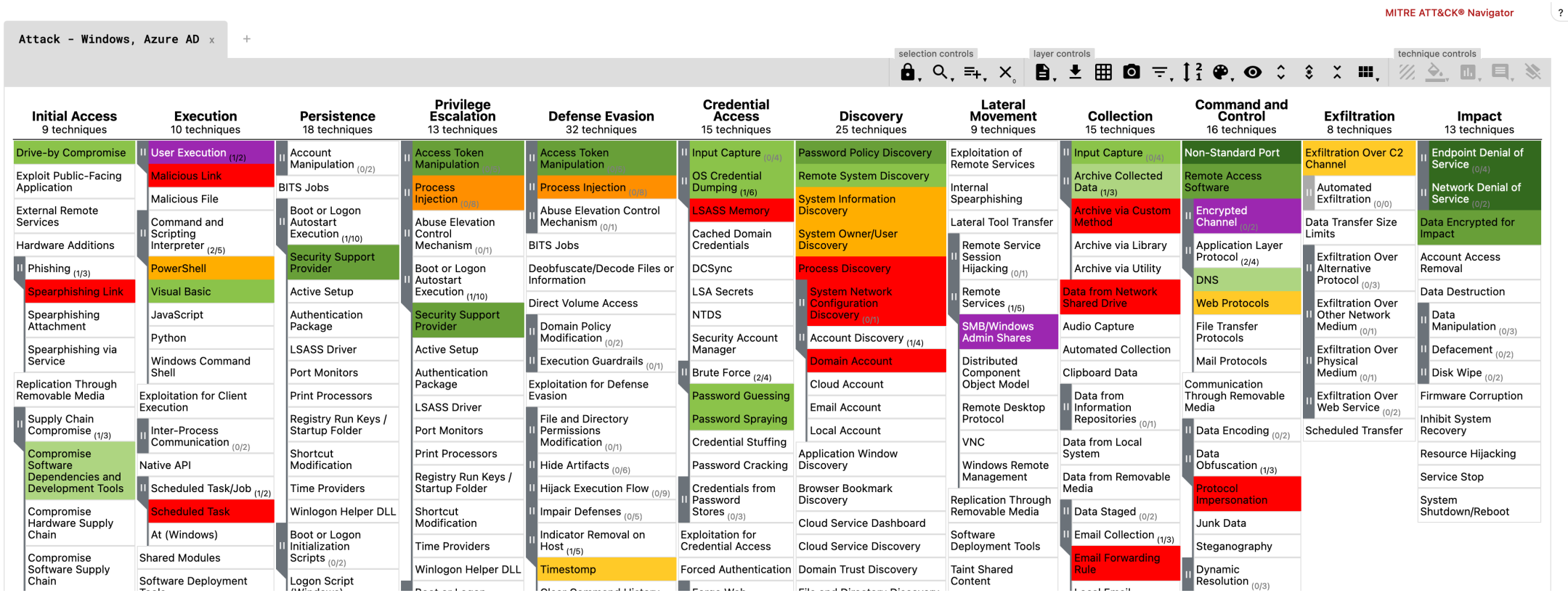
DETT&CT EDITOR

- Workbench for use case analysts and management
- Can be used to create or edit all types of DeTT&CT files and overviews
- Completely browser based, nothing is stored on the server



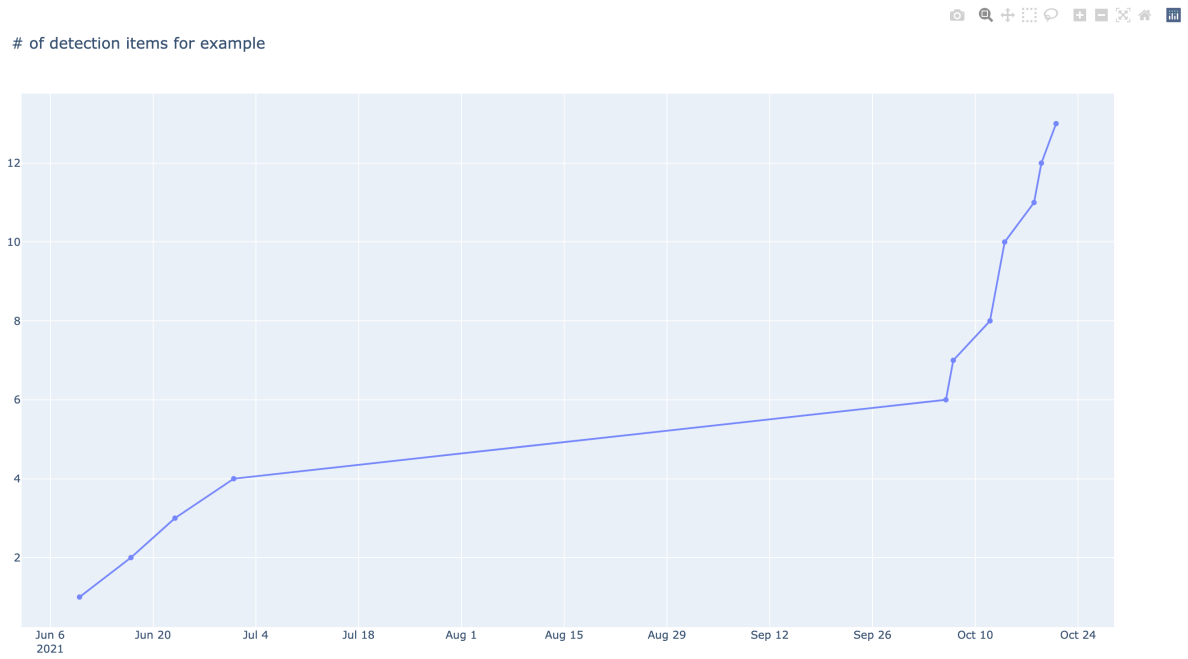
COMPARE DIFFERENT TYPES OF VIEWS

- What techniques do we detect compared to what is possible?
- Do we detect all the techniques that threat actor X uses?
- What techniques did the Red Team use and what did we detect?
- Etc.



DETT&CT: GRAPHS AND EXCEL EXPORTS

- Create timelines to visualize progress of data sources and detections over time
- Create Excel exports for reporting and life cycle management

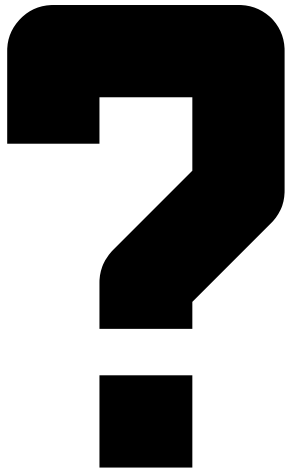


Overview of detections for example

Technique			Detection					
ID	Description	Tactic	Applicable to	Date	Score	Location	Technique comment	Detection comment
T1003.001	LSASS Memory	Credential-access	Windows workstations	2021-10-14	3	EDR		
T1021.006	Windows Remote Management	Lateral-movement	Windows workstations	2021-06-23	3	Splunk use case X6		
T1033	System Owner/User Discovery	Discovery	all	2021-06-10	2	Splunk use case X4	This technique is also often called "user hunting" by red teams.	
T1053.001	At (Linux)	Execution, Persistence, Privilege-escalation	Linux servers	2021-10-18	2	Splunk use case X8		
T1053.003	Cron	Execution, Persistence, Privilege-escalation	Linux servers	2021-10-14	3	EDR		
T1053.005	Scheduled Task	Execution, Persistence, Privilege-escalation	Windows workstations	2021-10-19	2	Splunk use case X7		
T1055	Process Injection	Defense-evasion, Privilege-escalation	Windows workstations	2021-10-06	3	EDR		
T1055	Process Injection	Defense-evasion, Privilege-escalation	Linux servers	2021-10-07	1	EDR		
T1056.001	Keylogging	Collection, Credential-access	Windows workstations	2021-10-12	3	EDR		It was tested during a purple team exercise—room for improvement.
T1071.004	DNS	Command-and-control	all	2021-10-06	4	Splunk use case X3		Could be implemented thanks to the DNS data source now being present in Splunk
T1110.003	Password Spraying	Credential-access	all	2021-07-01	3	Splunk use case X1		
T1197	BITS Jobs	Defense-evasion, Persistence	Windows workstations	2021-06-17	4	Splunk use case X5		
T1204	User Execution	Execution	all	2021-06-02	0	Splunk		
T1569.002	Service Execution	Execution	Windows workstations	2021-10-21	4	Splunk use case X2		Improved the detection after the results and lessons learned from a purple teaming exercise.

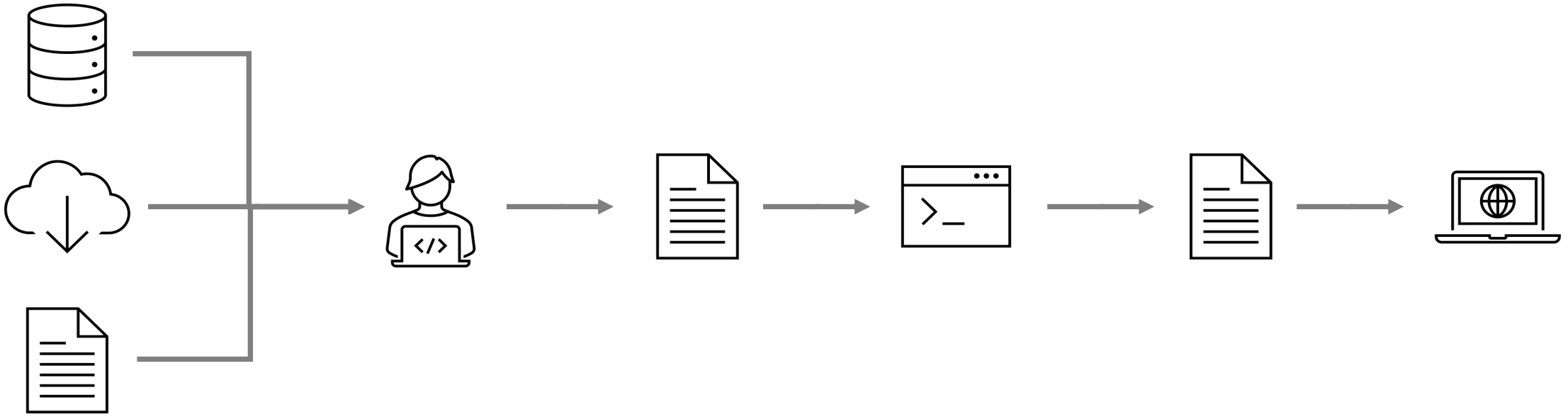
DEMO TIME

QUESTIONS



NEXT LEVEL

- Need for automation
  - Quite some manual work
  - Error prone
  - ATT&CK mapping is administrated in source tool (EDR, SIEM, …)
  - Time
- Integrate different types of products
- Current process:



DETTECTINATOR

- Tool to automatically import data source and detection data from source systems
  - Creates and updates DeTT&CT YAML files
- Reduces both the workload and registration errors
- The analyst can focus on quality and scoring
- Can be integrated in repository pipelines or scheduling
  - Command Line Interface
  - Python library

- Use cases:
  - Use it for an initial assessment of a new tool / solution
  - Integrate it in your detection engineering workflow to automate ATT&CK mappings with DeTT&CT

`github.com/siriussecurity/dettectinator`

DETTECTINATOR

- Currently supports:
  - Microsoft Sentinel: Analytics Rules (API)
  - Microsoft Defender: Alerts (API)
  - Microsoft Defender for Identity: Detection Rules (loaded from Github)
  - Tanium: Signals (API)
  - Elastic Security: Rules (API)
  - CSV, Excel (file)
  - Suricata rules (file)
  - Sigma rules (files)
  - Splunk config (file) (dev branch)
  - Microsoft Defender: Custom Detection Rules (under construction b/c private preview MS)
- Easily extensible to support other platforms or solutions
- Currently working on data source plugins: Sysmon, MDE, Windows Security Events
  - Based on OSSEM
  - Will be part of next release

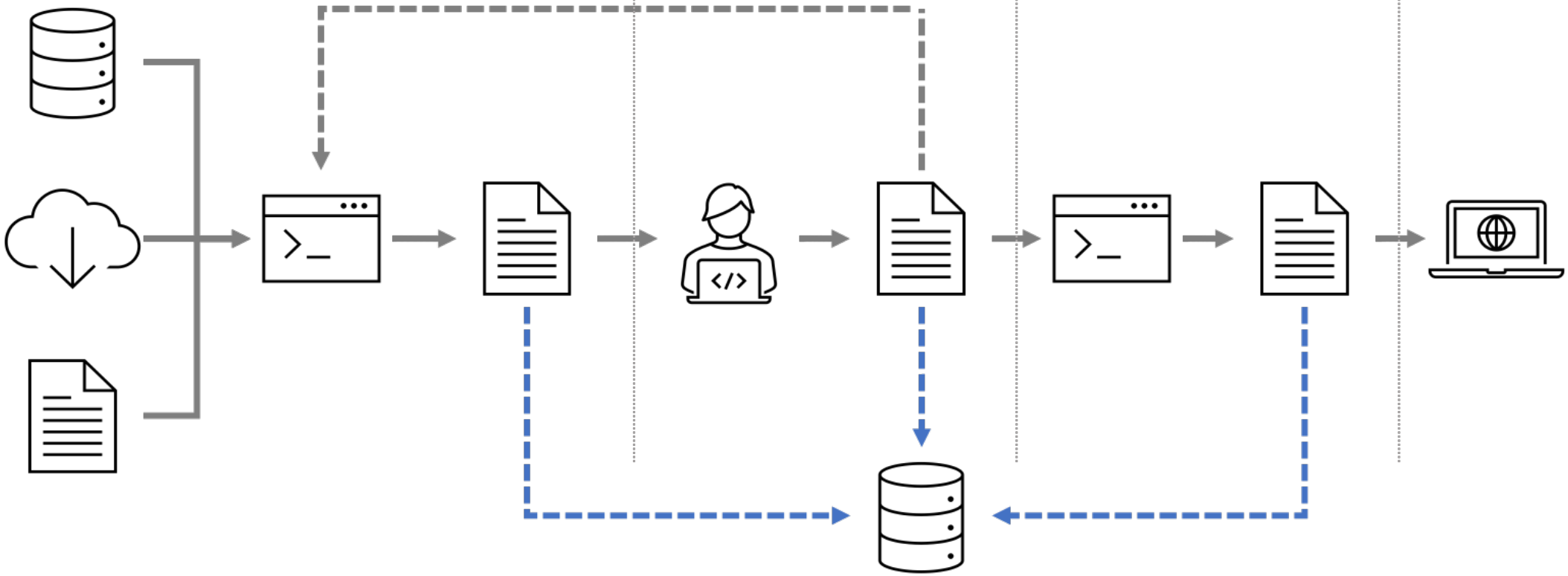
AUTOMATED DETT&CT WORKFLOW

1. Create DeTT&CT YAML file from source system
Detectinator connects to an API, database or file and retrieves technique and detection information. This information is either appended to an existing DeTT&CT YAML file or a new one is created.

2. Enrich the DeTT&CT YAML
The analyst uses the DeTT&CT editor to adjust scoring of the techniques based on the new information.

3. Create MITRE ATT&CK layer
The YAML file is converted into a MITRE ATT&CK layer using the DeTT&CT application.

4. View results in ATT&CK navigator
The created layer file can be viewed in the MITRE ATT&CK navigator.



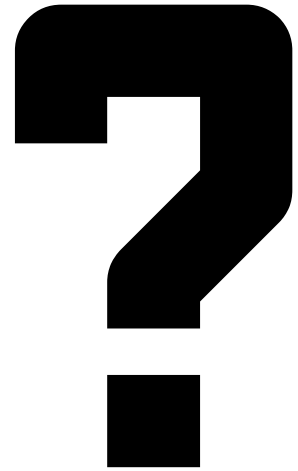
Store files in version control system
YAML en layer files can be stored under version control. Pipelines can be used to trigger steps in the process.

DEMO TIME

THE END. QUESTIONS?

- Sirius Security provides training on this topic:
  - Next Level Cyber Defense with MITRE ATT&CK
  - siriussecurity.nl/training

- Resources:
  - attack.mitre.org
  - github.com/rabobank-cdc/DeTTECT
  - github.com/siriussecurity/dettectinator



@rubinatorz