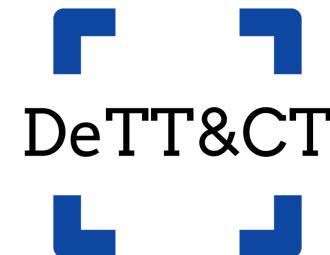


AUTOMATING ATT&CK COVERAGE WITH DETT&CT



22 NOVEMBER 2022



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
 - Dettectorator
- Contributor to open-source projects



@rubinatorz

AGENDA

MAPPING YOUR BLUE TEAM

- Short introduction to ATT&CK
- ATT&CK in practice using DeTT&CT
- Automation with Dettectorator
- Ask questions!



“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.)

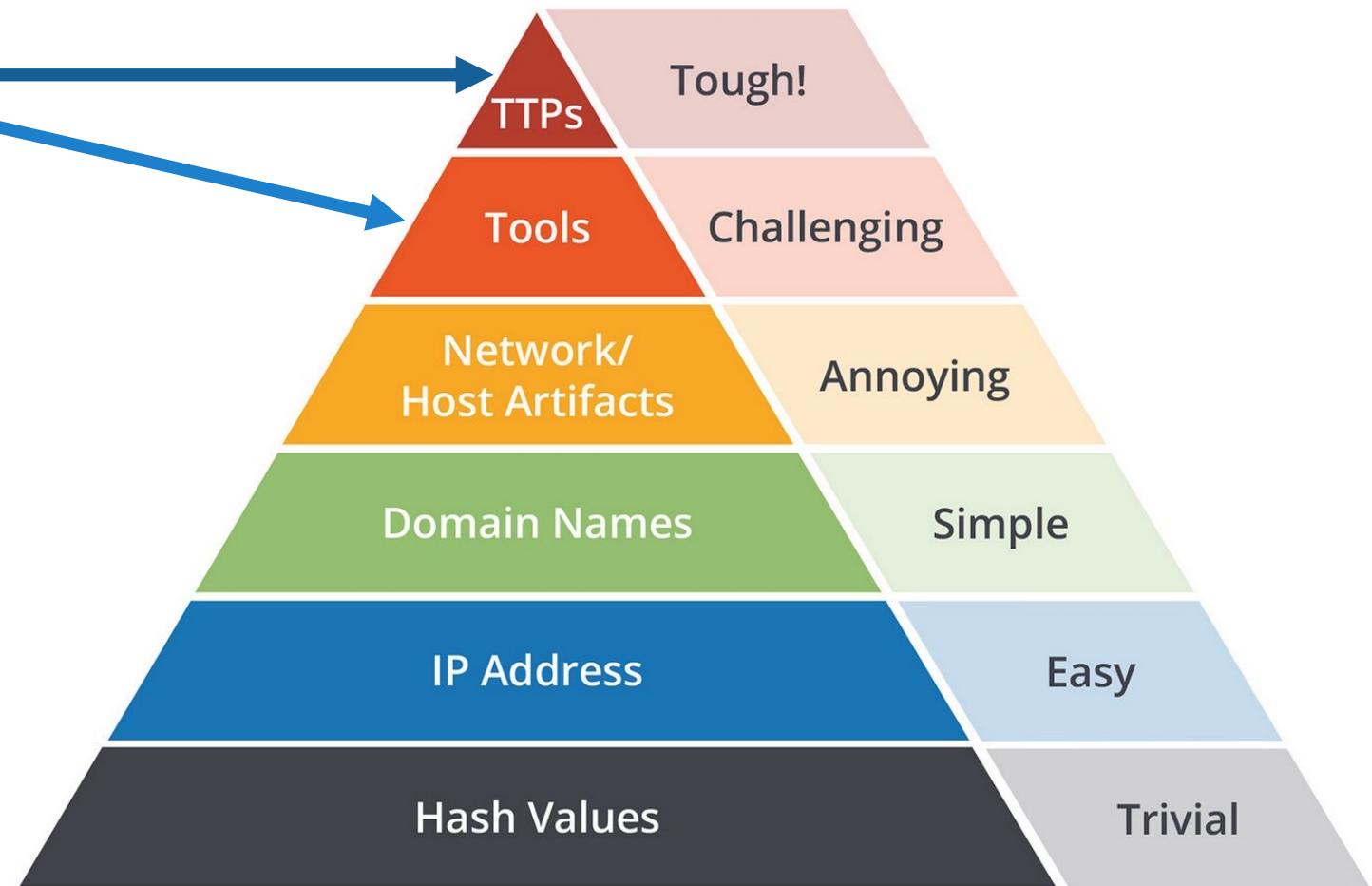


[1] <https://posts.specterops.io/whats-in-a-name-ttps-in-info-sec-14f24480ddcc>

ATT&CK AND THE PYRAMID OF PAIN



"Wikipedia on cyber attacks"



ATT&CK MATRIX

Cyber Kill Chain



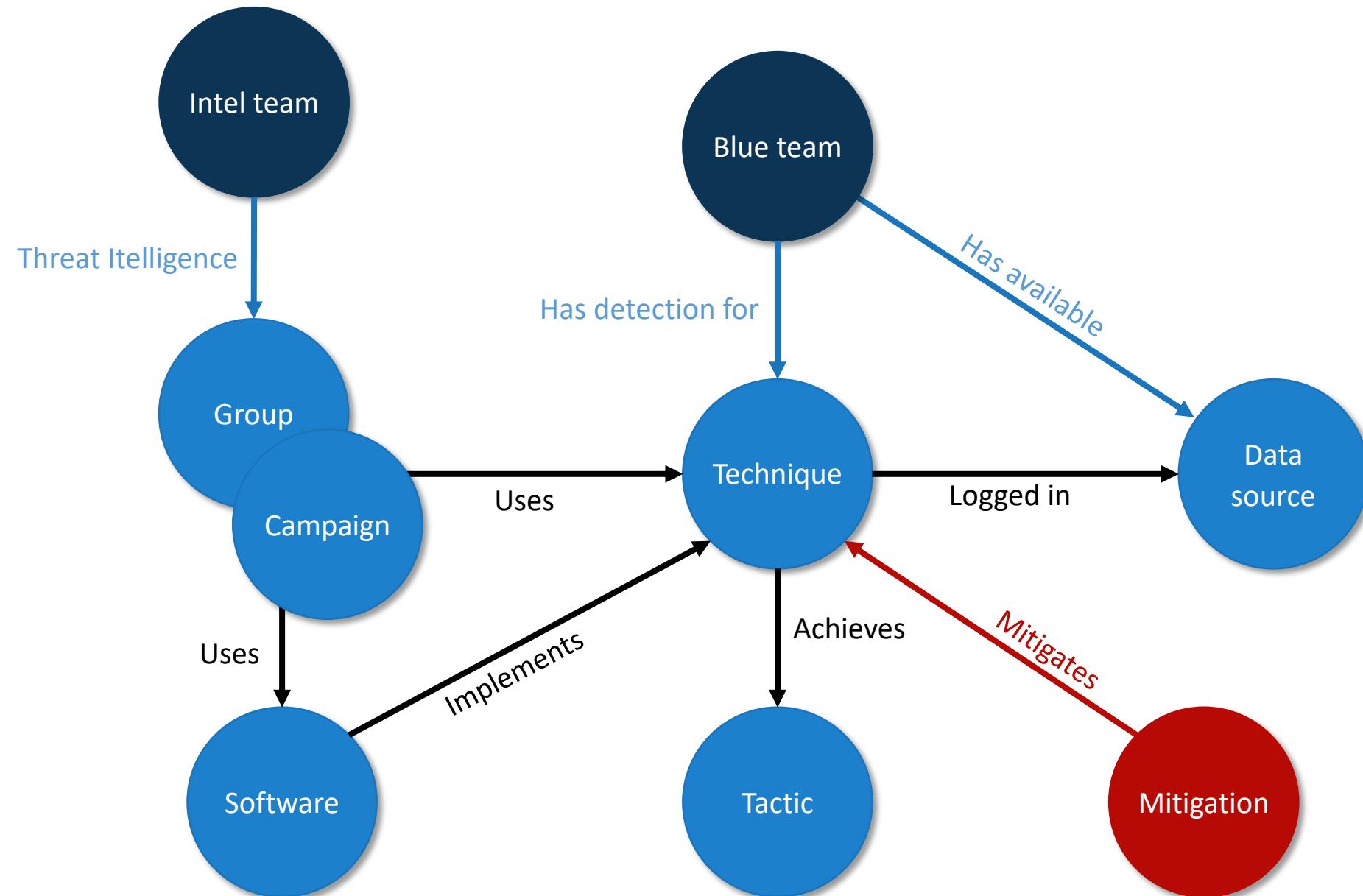
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	39 techniques	15 techniques	27 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Scanning IP Blocks	Domains	Exploit Public-Facing Application	PowerShell	Additional Cloud Credentials	Setuid and Setgid	Setuid and Setgid	Password Guessing	Local Account	Internal Spearphishing	Archive via Utility	Web Protocols	Traffic Duplication	Data Destruction
Vulnerability Scanning	DNS Server	External Remote Services	AppleScript	Exchange Email Delegate Permissions	Bypass User Account Control	Bypass User Account Control	Password Cracking	Domain Account	Archive via Library	File Transfer Protocols	Mail Protocols	Data Transfer Size Limits	Data Encrypted for Impact
Gather Victim Host Information (4)	Virtual Private Server	Hardware Additions	Windows Command Shell	Sudo and Sudo Caching	Sudo and Sudo Caching	Elevated Execution with Prompt	Password Spraying	Email Account	Lateral Tool Transfer	DNS	Exfiltration Over Alternative Protocol (3)	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Data Manipulation (3)
Hardware	Server	Phishing (3)	Unix Shell	Add Office 365 Global Administrator Role	Access Token Manipulation (5)	Access Token Manipulation (5)	Credential Stuffing	Cloud Account	Remote Service Session Hijacking (2)	Audio Capture	Communication Through Removable Media	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Stored Data Manipulation
Software	Botnet	Spearphishing Attachment	Visual Basic	SSH Authorized Keys	Token Impersonation/Theft	Token Impersonation/Theft	Credentials from Password Stores (5)	Application Window Discovery	SSH Hijacking	Automated Collection	Data Encoding (2)	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	Transmitted Data Manipulation
Firmware	Web Services	Spearphishing Link	Python	JavaScript	Create Process with Token	Create Process with Token	Keychain	Browser Bookmark Discovery	RDP Hijacking	Clipboard Data	Standard Encoding	Exfiltration Over C2 Channel	Runtime Data Manipulation
Client Configurations	Compromise Accounts (2)	Spearphishing via Service	Network Device CLI	BITS Jobs	Make and Impersonate Token	Make and Impersonate Token	Securityd Memory	Cloud Infrastructure Discovery	Remote Services (6)	Data from Cloud Storage Object	Non-Standard Encoding	Defacement (2)	Defacement (2)
Gather Victim Identity Information (3)	Social Media Accounts	Replication Through Removable Media	Container Administration Command	Boot or Logon Autostart Execution (14)	Parent PID Spoofing	Credentials from Web Browsers	Cloud Service Dashboard	Cloud Service Discovery	Remote Desktop Protocol	SMB/Windows Admin Shares	SNMP (MIB Dump)	Exfiltration Over Other Network Medium (1)	Internal Defacement
Credentials	Email Accounts	Compromise Infrastructure (6)	Supply Chain Compromise (3)	Deploy Container	Parent PID Spoofing	Windows Credential Manager	Container and Resource Discovery	Domain Trust Discovery	Distributed Component Object Model	Junk Data	Protocol Impersonation	Exfiltration Over Bluetooth	External Defacement
Email Addresses	Compromise Infrastructure (6)	Domains	Compromise Software Dependencies and Development Tools	Exploitation for Client Execution	SID-History Injection	SID-History Injection	Cloud Service Discovery	File and Directory Discovery	SSH	Network Device Configuration Dump	Dynamic Resolution (3)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Employee Names	Replication Through Removable Media	Inter-Process Communication (2)	Component Object Model	Authentication Package	BITS Jobs	BITS Jobs	Cloud Service Discovery	Network Service Scanning	VNC	Windows Remote Management	Confluence	Exfiltration over USB	Disk Content Wipe
Gather Victim Network Information (6)	Supply Chain Compromise (3)	Compromise Software Dependencies and Development Tools	Dynamic Data Exchange	Winlogon Helper DLL	Build Image on Host	Build Image on Host	Network Share Discovery	Network Sniffing	Windows Remote Management	Sharepoint	Domain Generation Algorithms	Exfiltration Over Web Service (2)	Disk Structure Wipe
Domain Properties	Domains	Exploitation for Client Execution	Native API	Registry Run Keys / Startup Folder	Deobfuscate/Decode Files or Information	Exploitation for Credential Access	Network Share Discovery	Network Sniffing	Dynamic Resolution (3)	Replication Through Removable Media	Fast Flux DNS	Exfiltration to Code Repository	Endpoint Denial of Service (4)
DNS	Inter-Process Communication (2)	Authentication Package	Kernel Modules and Extensions	Authenticaton Package	Deploy Container	Forced Authentication	Network Sniffing	Network Sniffing	Dynamic Resolution (3)	Sharepoint	DNS Calculation	Exfiltration to Cloud Storage	OS Exhaustion Flood
Network Trust Dependencies	Component Object Model	Dynamic Data Exchange	Time Providers	Direct Volume Access	Forge Web Credentials (2)	Forge Web Credentials (2)	Network Share Discovery	Network Share Discovery	Dynamic Resolution (3)	Domain Generation Algorithms	Encrypted Channel (2)	Scheduled Transfer	Service Exhaustion Flood
Network Topology	Dynamic Data Exchange	Native API	Re-opened Applications	Time Providers	Domain Policy Modification (2)	Web Cookies	Peripheral Device Discovery	Peripheral Device Discovery	Dynamic Resolution (3)	Fast Flux DNS	Symmetric Cryptography	Transfer Data to Cloud Account	Application Exhaustion Flood
IP Addresses	Native API	Kernel Modules and Extensions	Winlogon Helper DLL	Winlogon Helper DLL	Group Policy Modification	SAML Tokens	Sharepoint	Sharepoint	Dynamic Resolution (3)	DNS Calculation	Asymmetric Cryptography	Exfiltration to Cloud Storage	Application or System Exploitation
Network Security Appliances	Develop Capabilities (4)	Re-opened Applications	Security Support Provider	Security Support Provider	Domain Trust Modification	Input Capture (4)	Replication Through Removable Media	Replication Through Removable Media	Dynamic Resolution (3)	Encrypted Channel (2)	Encrypted Channel (2)	Scheduled Transfer	Firmware Corruption
Gather Victim Org Information (4)	Trusted Relationship	At (Windows)	Kernel Modules and Extensions	Kernel Modules and Extensions	Domain Trust Modification	Keylogging	Permission Groups Discovery (3)	Permission Groups Discovery (3)	Dynamic Resolution (3)	Fast Flux DNS	Symmetric Cryptography	Transfer Data to Cloud Account	Inhibit System Recovery
Business Relationships	Code Signing Certificates	At (Windows)	Shortcuts Modification	Shortcuts Modification	Domain Trust Modification	GUI Input Capture	Domain Groups	Domain Groups	Dynamic Resolution (3)	DNS Calculation	Asymmetric Cryptography	Exfiltration to Cloud Storage	Network Denial of Service
Determine Physical Locations	Valid Accounts (4)	Scheduled Task	Kernel Modules and Extensions	Kernel Modules and Extensions	Domain Trust Modification	Input Capture (4)	Cloud Groups	Cloud Groups	Dynamic Resolution (3)	Encrypted Channel (2)	Encrypted Channel (2)	Scheduled Transfer	Service Exhaustion Flood
Identify Business Tempo	Digital Certificates	Default Accounts	Re-opened Applications	Re-opened Applications	Execution Guardrails (1)	Keylogging	Local Groups	Local Groups	Dynamic Resolution (3)	Fast Flux DNS	Symmetric Cryptography	Transfer Data to Cloud Account	Application Exhaustion Flood
Identify Roles	Exploits	Domain Accounts	At (Linux)	At (Linux)	Environmental Keying	GUI Input Capture	Process Discovery	Process Discovery	Dynamic Resolution (3)	DNS Calculation	Asymmetric Cryptography	Exfiltration to Cloud Storage	Application or System Exploitation
Phishing for Information (3)	Establish Accounts (2)	Local Accounts	Launchd	Launchd	Execution Guardrails (1)	Web Portal Capture	Query Registry	Query Registry	Dynamic Resolution (3)	Encrypted Channel (2)	Encrypted Channel (2)	Scheduled Transfer	Firmware Corruption
	Social Media Accounts	Cloud Accounts	Port Monitors	Port Monitors	Environmental Keying	Web Portal Capture	Remote System Discovery	Remote System Discovery	Dynamic Resolution (3)	Fast Flux DNS	Fast Flux DNS	Transfer Data to Cloud Account	Inhibit System Recovery
			Cron	Cron	Exploitation for Defense Evasion	Web Portal Capture	Credential API Hooking	Credential API Hooking	Dynamic Resolution (3)	DNS Calculation	DNS Calculation	Exfiltration to Cloud Storage	Network Denial of Service
			Print Processors	Print Processors	File and Directory Permissions Modification (2)	Web Portal Capture	Software Discovery (1)	Software Discovery (1)	Dynamic Resolution (3)	Encrypted Channel (2)	Encrypted Channel (2)	Scheduled Transfer	Service Exhaustion Flood
			XDG Autostart Entries	XDG Autostart Entries	Port Monitors	Web Portal Capture	Pass the Hash	Pass the Hash	Dynamic Resolution (3)	Fast Flux DNS	Fast Flux DNS	Transfer Data to Cloud Account	Application Exhaustion Flood
			Container Orchestration Job	Container Orchestration Job	Active Setup	Web Portal Capture	Pass the Ticket	Pass the Ticket	Dynamic Resolution (3)	DNS Calculation	DNS Calculation	Exfiltration to Cloud Storage	Application or System Exploitation
						Web Portal Capture	Remote Data Staging	Remote Data Staging	Dynamic Resolution (3)	Encrypted Channel (2)	Encrypted Channel (2)	Scheduled Transfer	Firmware Corruption
						Remote Data Staging	Local Data Staging	Local Data Staging	Dynamic Resolution (3)	Fast Flux DNS	Fast Flux DNS	Transfer Data to Cloud Account	Inhibit System Recovery
						Local Data Staging	Remote Data Staging	Remote Data Staging	Dynamic Resolution (3)	DNS Calculation	DNS Calculation	Exfiltration to Cloud Storage	Network Denial of Service
						Remote Data Staging	Application Access Token	Application Access Token	Dynamic Resolution (3)	Encrypted Channel (2)	Encrypted Channel (2)	Scheduled Transfer	Service Exhaustion Flood
						Application Access Token	Email	Email	Dynamic Resolution (3)	Fast Flux DNS	Fast Flux DNS	Transfer Data to Cloud Account	Application or System Exploitation

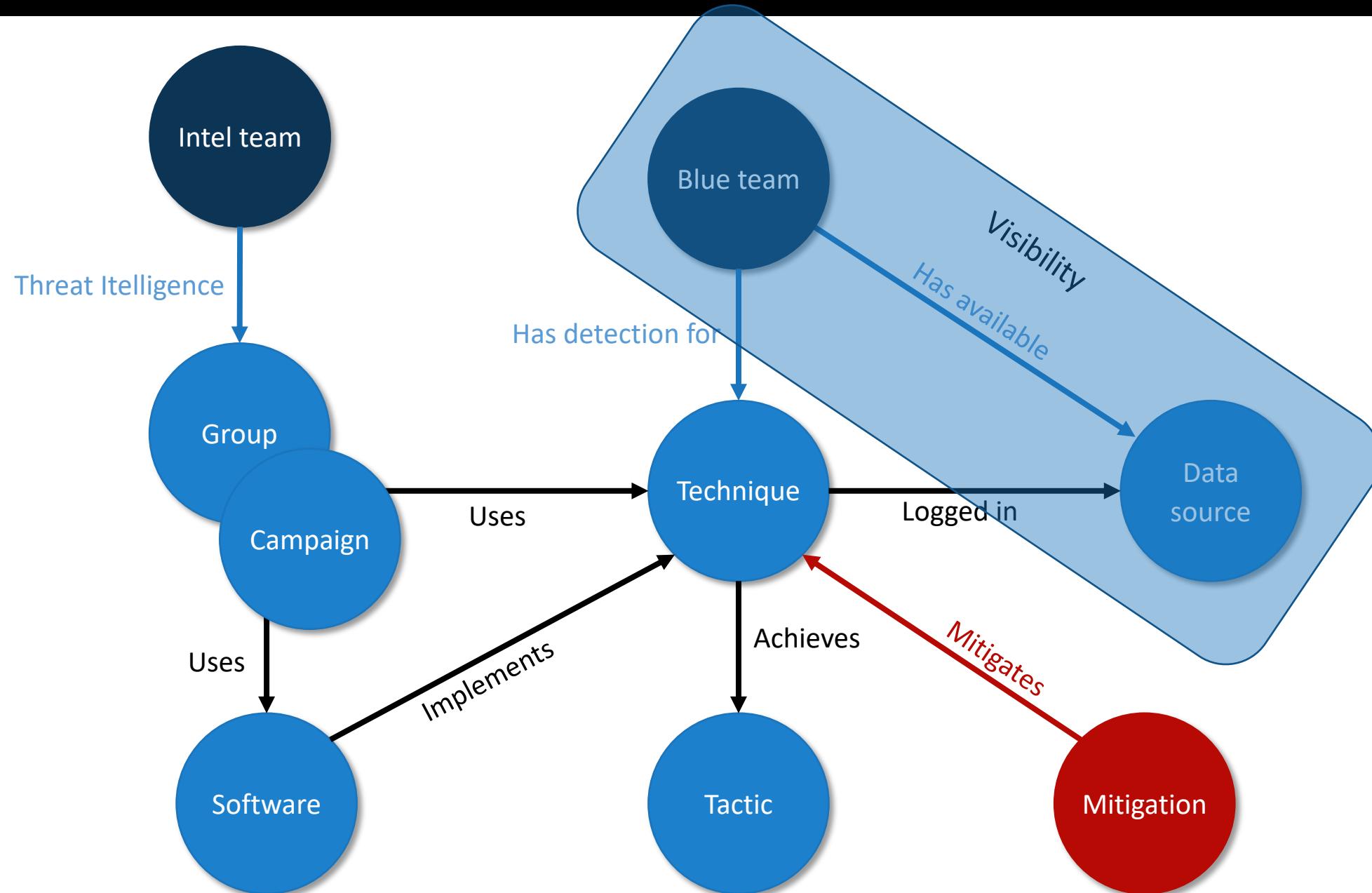
TACTICS, TECHNIQUES, AND PROCEDURES (TTP)

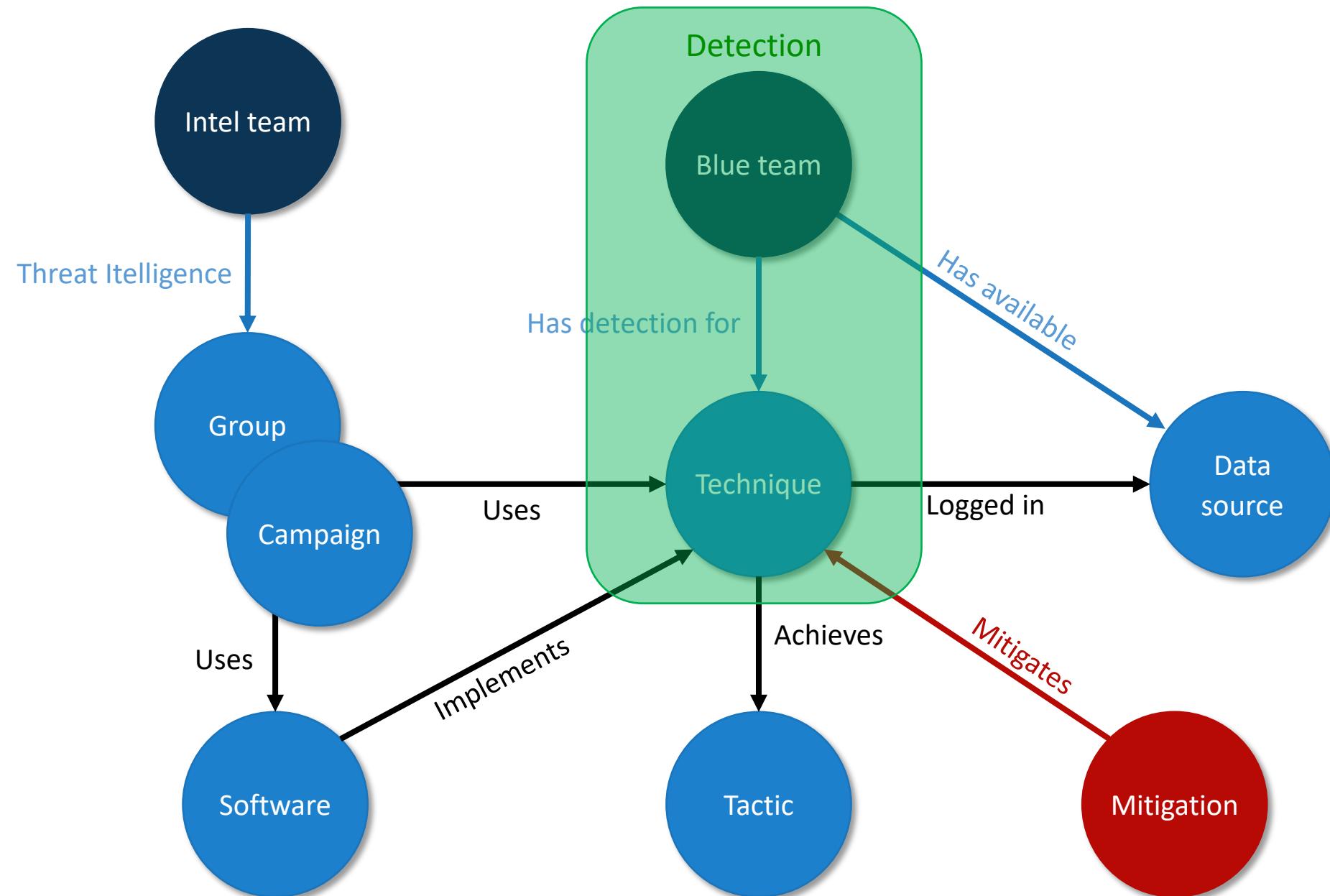
Tactics: the adversary's technical goals

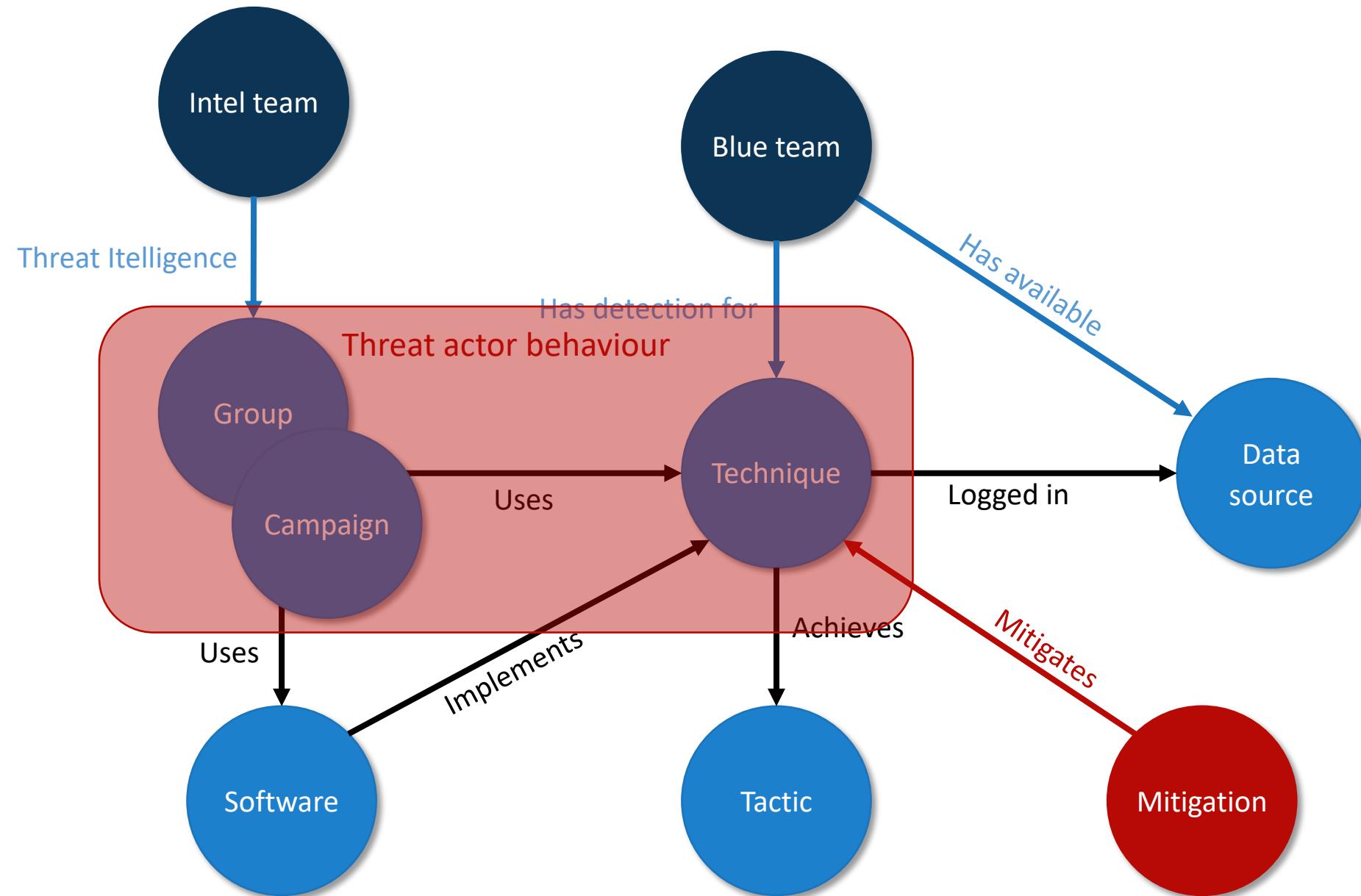
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	39 techniques	15 techniques	27 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (2) Scanning IP Blocks Vulnerability Scanning Gather Victim Host Information (4) Hardware Software Firmware Client Configurations Gather Victim Identity Information (3) Credentials Email Addresses Employee Names Gather Victim Network Information (6) Domain Properties DNS Network Trust Dependencies Network Topology IP Addresses Network Security Appliances Gather Victim Org Information (4) Business Relationships Determine Physical Locations Identify Business Tempo Identify Roles Phishing for Information (3) Spearphishing Service Spearphishing Attachment Spearphishing Link Search Closed	Acquire Infrastructure (6) Domains DNS Server Virtual Private Server Server Botnet Web Services Compromise Accounts (2) Social Media Accounts Email Accounts Replication Through Removable Media Compromise Infrastructure (6) Domains DNS Server Virtual Private Server Server Botnet Web Services Develop Capabilities (4) Malware Code Signing Certificates Digital Certificates Exploits Establish Accounts (2) Social Media Accounts Email Accounts Obtain Capabilities (6) Malware Tool	Drive-by Compromise Exploit Public-Facing Application External Remote Services Hardware Additions Phishing (3) Spearphishing Attachment Spearphishing Link Spearphishing via Service Supply Chain Compromise (3) Compromise Software Dependencies and Development Tools Compromise Software Supply Chain Compromise Hardware Supply Chain Trusted Relationship Valid Accounts (4) Default Accounts Domain Accounts Local Accounts Cloud Accounts Shared Modules Software Deployment Tools System Services (2)	Command and Scripting Interpreter (8) PowerShell AppleScript Windows Command Shell Unix Shell Visual Basic Python JavaScript Network Device CLI Container Administration Command Deploy Container Exploitation for Client Execution Inter-Process Communication (2) Component Object Model Dynamic Data Exchange Native API Scheduled Task/Job (7)	Account Manipulation (4) Additional Cloud Credentials Exchange Email Delegate Permissions Add Office 365 Global Administrator Role SSH Authorized Keys BITS Jobs Container Administration Command Deploy Container Exploitation for Client Execution Inter-Process Communication (2) Component Object Model Dynamic Data Exchange Native API Scheduled Task/Job (7)	Abuse Elevation Control Mechanism (4) Bypass Control Sudo and Cache Elevate with Process Access Manipulation Token Impersonation Create Token Make a Impersonation Parent SID-History Boot or Logon Autostart Execution (14) Registry Run Keys / Startup Folder Authentication Package Time Providers Winlogon Helper DLL Security Support Provider Kernel Modules and Extensions Re-opened Applications Winlogon Helper DLL LSASS Driver Shortcut Modification Port Monitors Plist Modification Print Processors XDG Autostart Entries Active Setup Boot or Logon Initialization Scripts (5) Software Deployment Tools XDG Autostart Entries Logon Script (Windows) Active Setup	Brute Force (4) Account Discovery (4) Exploitation of Remote Services Archive Collected Application Layer Protocol (4) Automated Exfiltration (1) Account Access Removal Data Destruction Data Encrypted for Exfiltration Data Manipulation (3) Stored Data Manipulation Transmitted Data Manipulation Runtime Data Manipulation Defacement (2) Internal Defacement External Defacement Disk Wipe (2) Disk Content Wipe Disk Structure Wipe Endpoint Denial of Service (4) OS Exhaustion Flood Service Exhaustion Flood Application Exhaustion Flood Application or System Exploitation Firmware Corruption Inhibit System Recovery Network Denial of Service (2) Direct Network Flood Reflection Amplification	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]											

Techniques:
how the
goals are
achieved

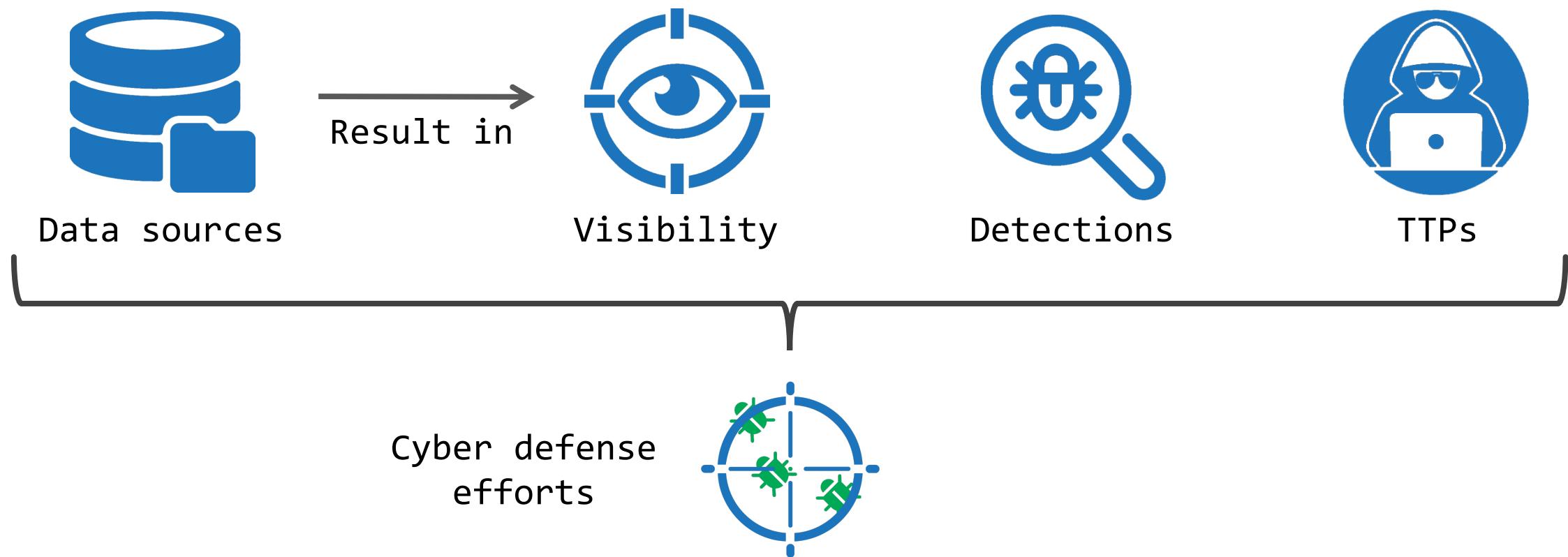






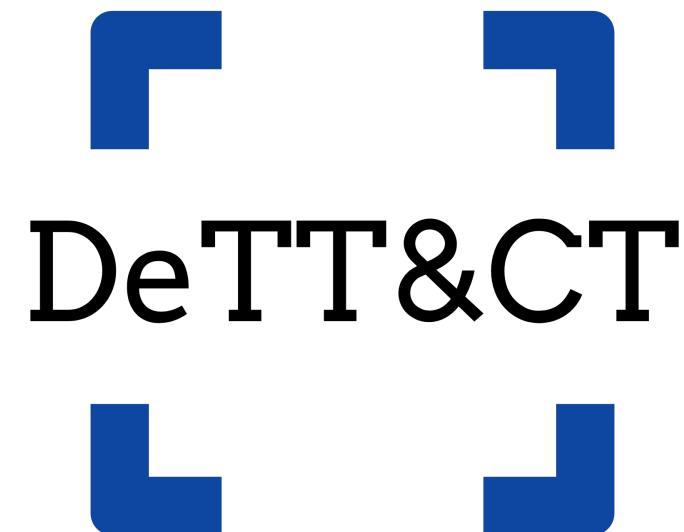


CHALLENGE: WHERE DO WE START OUR CYBER DEFENSE EFFORTS



DETECT TTCOMBAT T

- 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



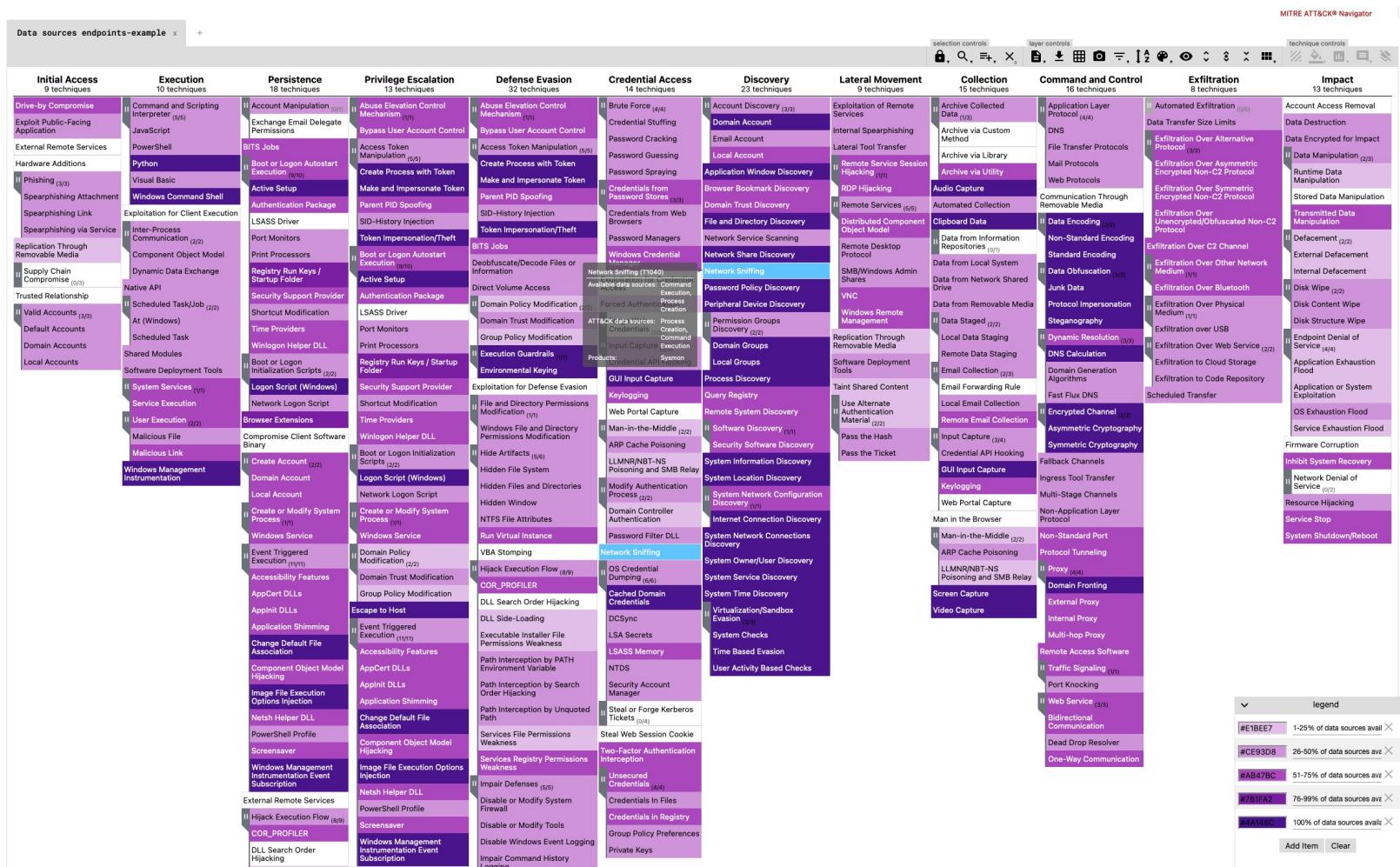
github.com/rabobank-cdc/DeTTECT



DATA SOURCES: WHAT DO WE LOG

- Identify data sources

ID	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 qua

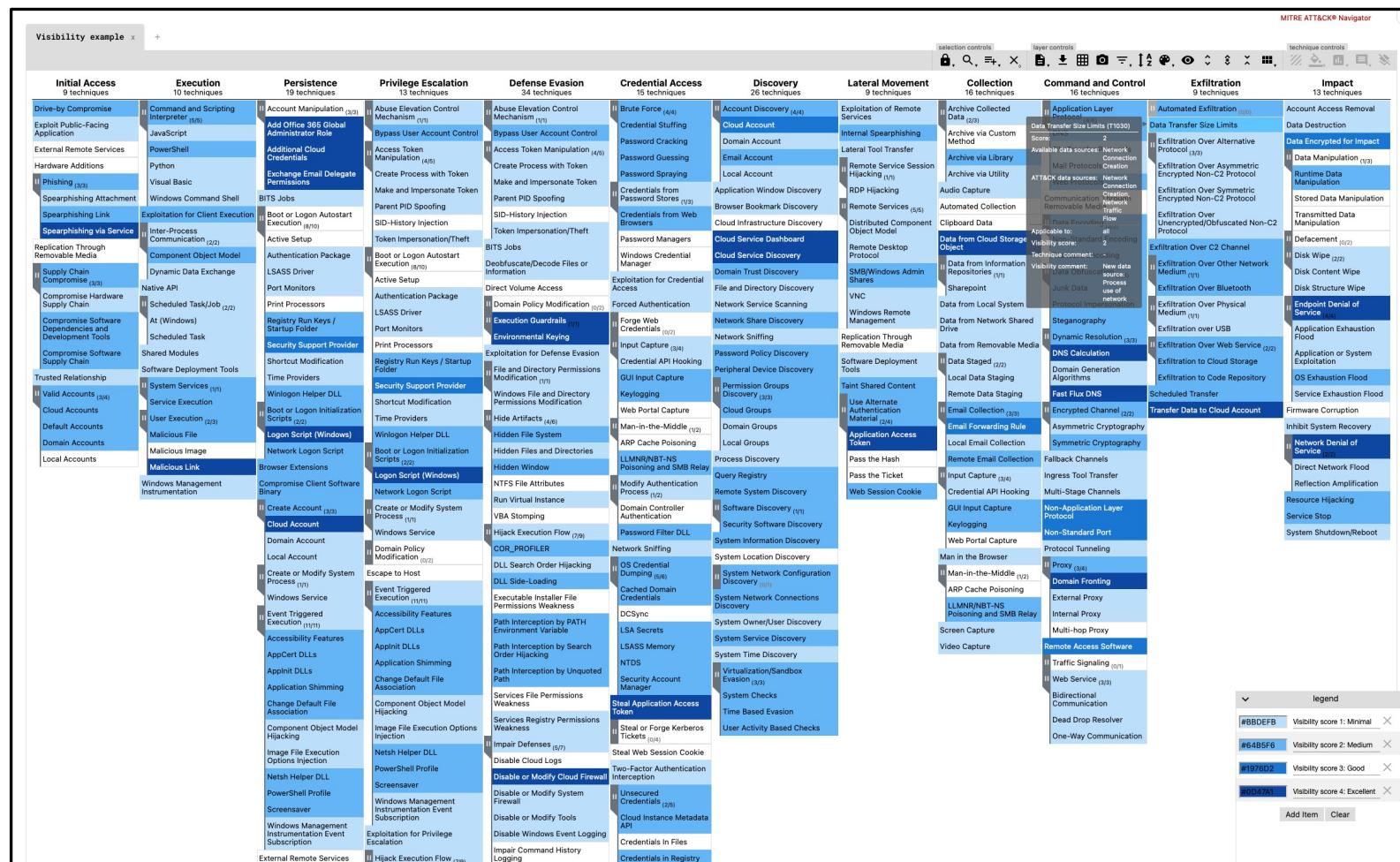
- device completeness
 - field completeness
 - timeliness
 - consistency and retention

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.



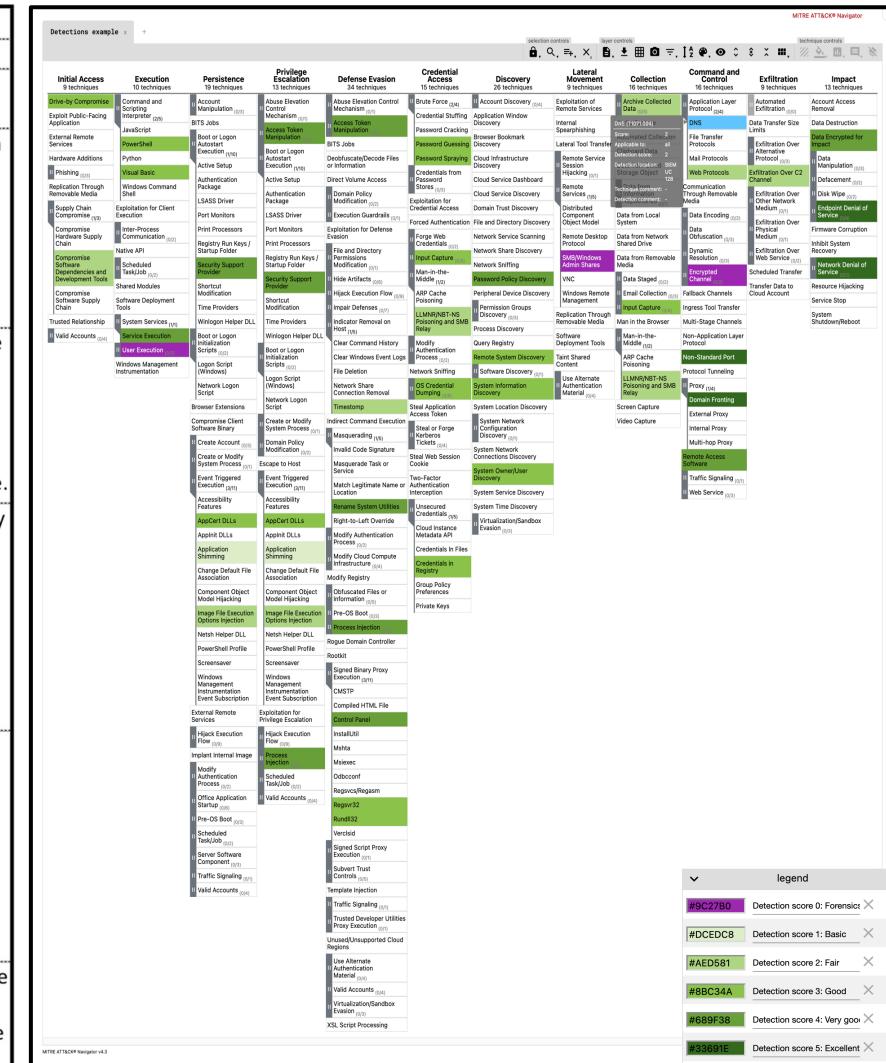


DETECTION: WHAT IS OUR DETECTION COVERAGE?

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

Detection scores

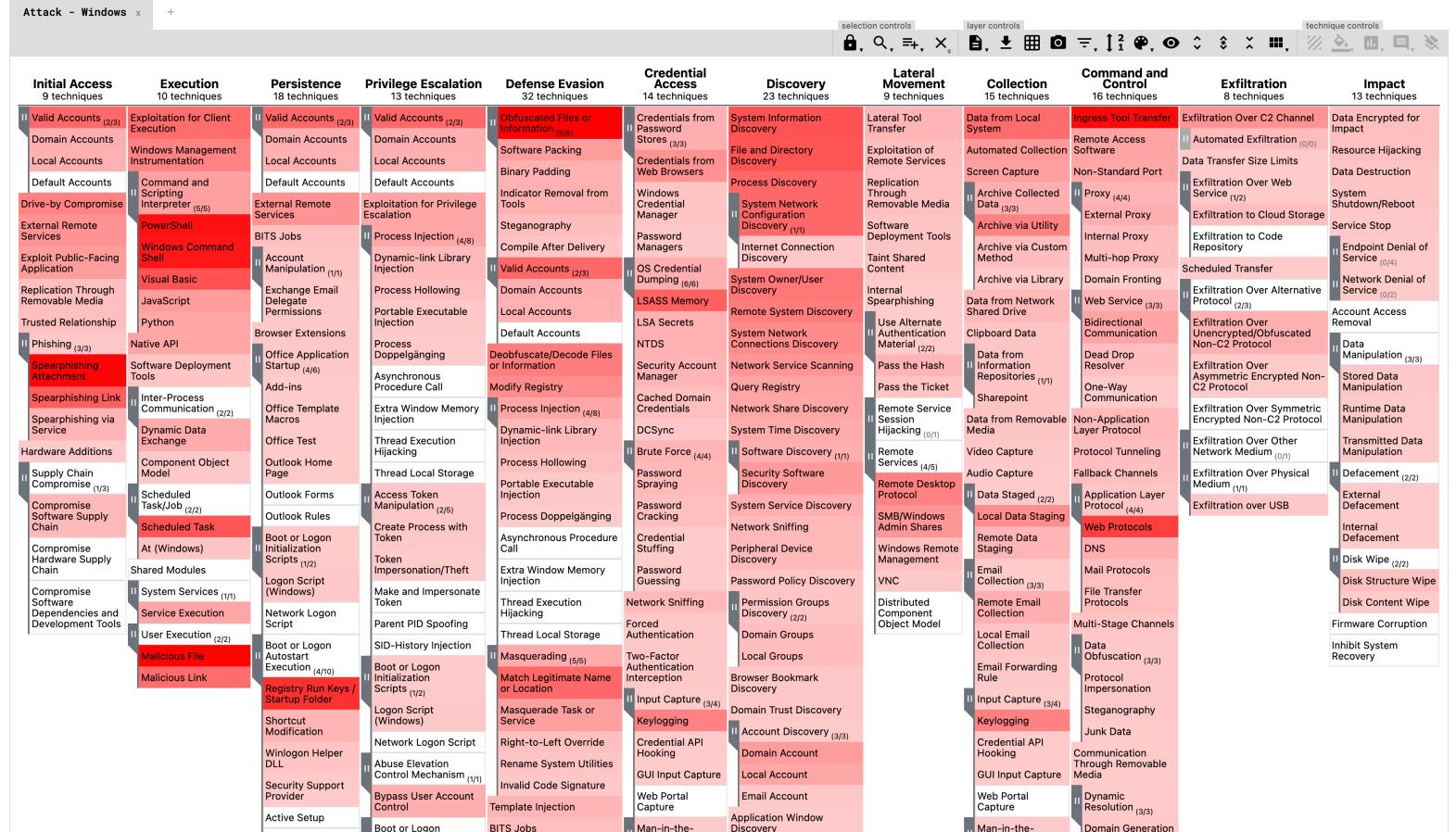
Score	Score name	Description
-1	None	No detection.
0	Forensics / context	No detection, but the technique is being logged for forensic purposes and can be used to provide context.
1	Basic	<p>Detection is in place using a basic signature to detect a specific part(s) of the technique's procedures.</p> <p>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.</p>
2	Fair	<p>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.</p>
3	Good	<p>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.</p> <p>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.</p> <p>Detection is real time.</p>
4	Very good	<p>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.</p> <p>False positives may still be present but are easy to recognize and can possibly be filtered out.</p>
5	Excellent	<p>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".</p>





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/DeTECT/tree/master/threat-actor-data>

DETT&CT EDITOR

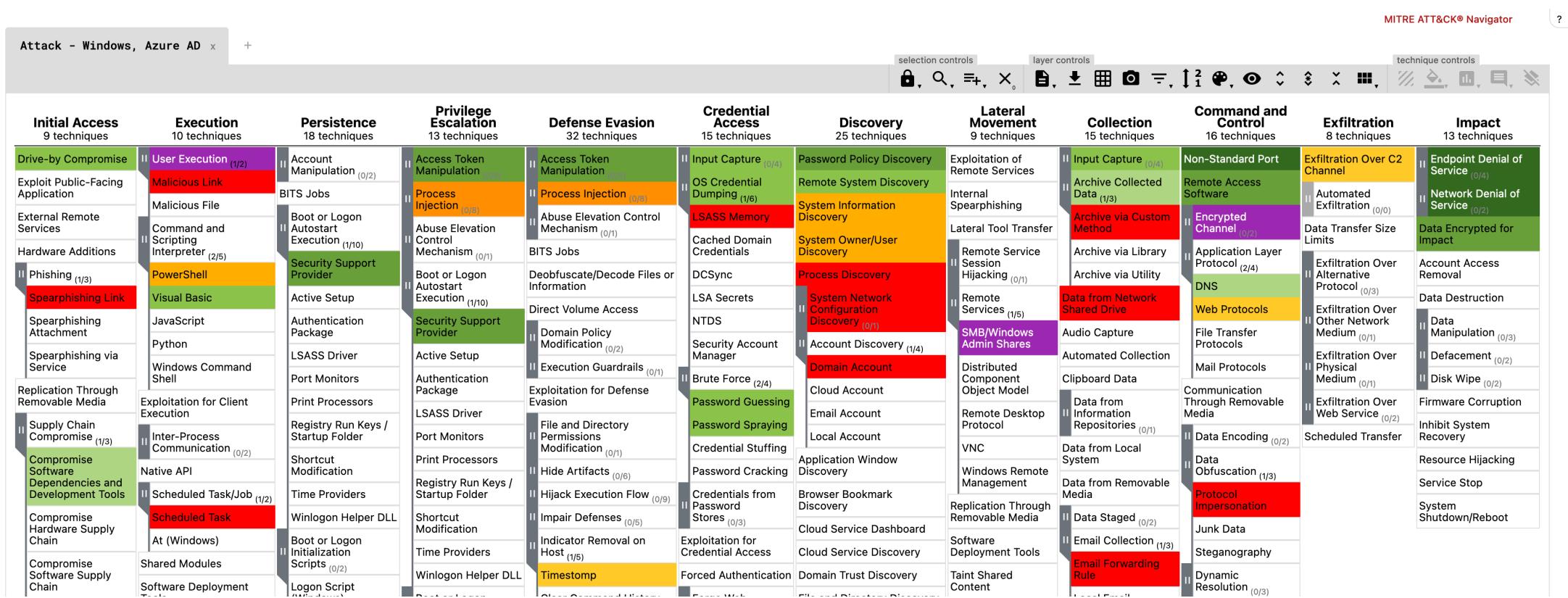
- Workbench for use case analysts and management
- Can be used to create or edit all types of DeTT&CT files and overviews
- Completely browser based, nothing is stored on the server

The screenshot displays the DeTT&CT Editor application interface. On the left, a sidebar menu includes HOME, DATA SOURCES (selected), TECHNIQUES, and GROUPS. The main area shows a "Data Sources" section with a file named "data-sources-endpoints.yaml". The "File details" pane shows the filename, type, version, name, notes, and platform support (all, PRE, Windows, macOS, Linux, Office 365, Azure AD, Google Workspace, SaaS, IaaS, Network, Containers). A "Save YAML file" button is present. Below this is a table titled "Add data source" with columns for Name, Date registered, and Products. The table lists various system events: Command Execution, Network Connection Creation, Network Traffic Content, OS API Execution, Process Creation, User Account Authentication, Windows Registry Key Creation, Windows Registry Key Deletion, Windows Registry Key Modification, and WMI Creation, all registered on 2021-05-05 by Sysmon. To the right, a "Command Execution" panel shows key-value pairs (Data source registered: 2021-05-05, Date connected: 2020-03-10), data source enable status (Yes), availability for analytics (Yes), products (Sysmon), and a comment field. At the bottom, there are sections for "Data quality" (Device completeness, Timeliness, Consistency, Retention) and "Custom key-value pairs" with a "key" input, "value" input, and an "Add" button.



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									
ID	Description	Technique		Applicable to	Date	Score	Location	Detection	
		Tactic	Technique					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		
T1071.004	DNS	Command-and-control		all	2021-10-06	4	Splunk use case X3		
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!

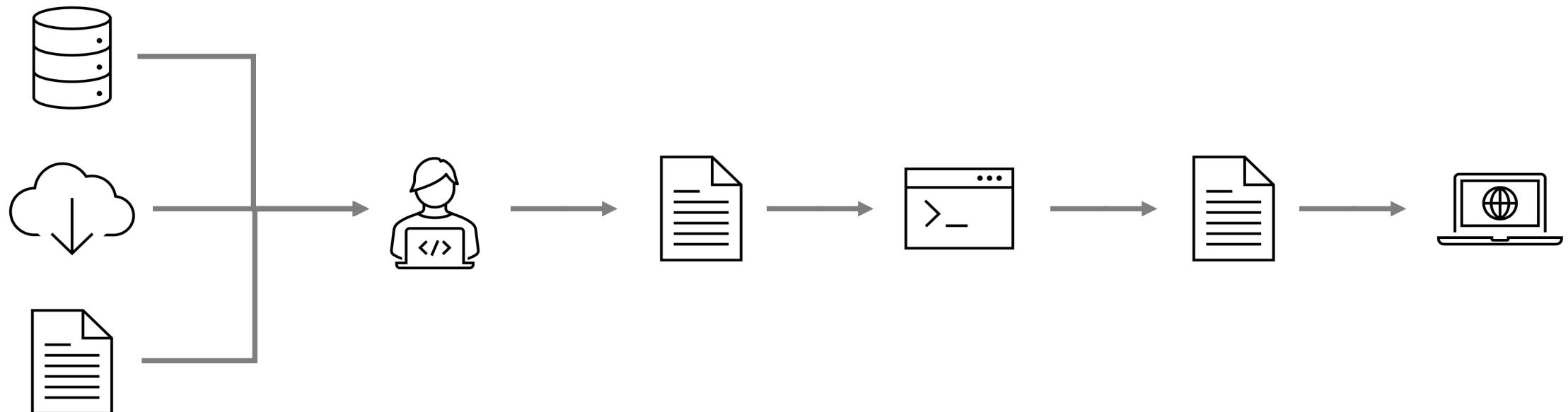
DEMO TIME

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

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

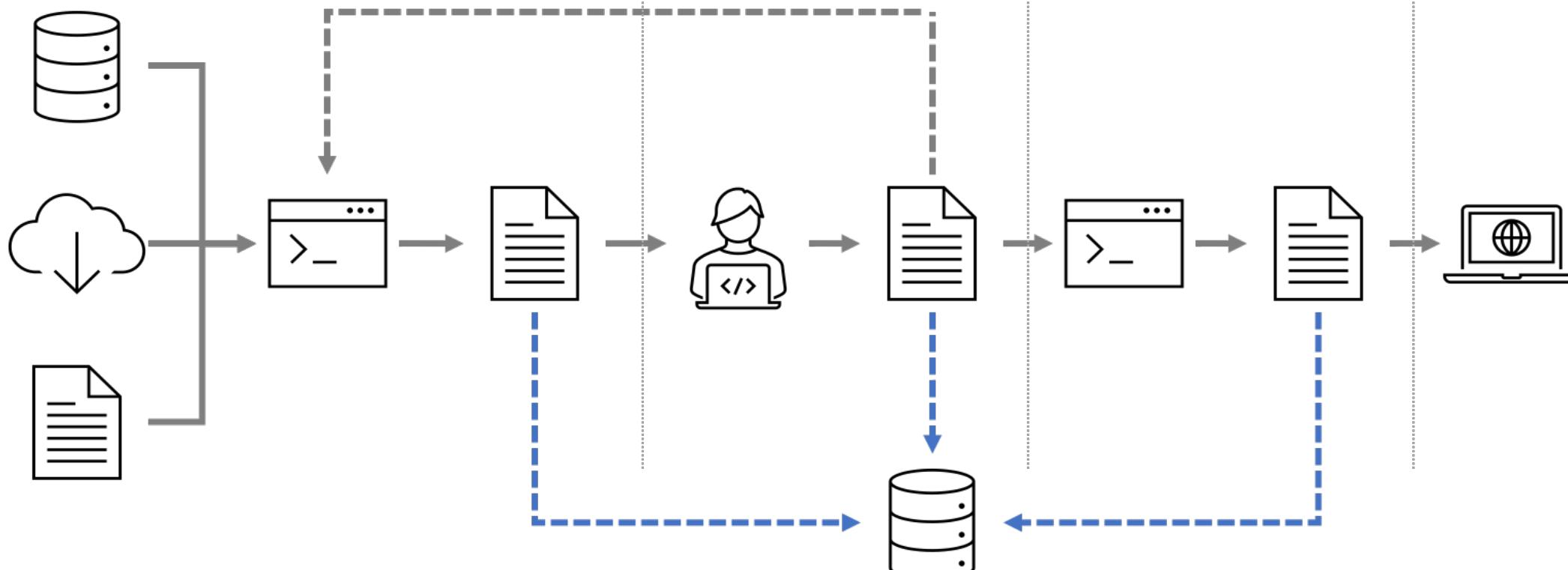
The analyst uses the DeTT&CT editor to adjust scoring of the techniques based on the new information.

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!

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/DeTECT
- github.com/siriussecurity/detectinator

