

**MB SECURE**

Sirius  Security

**DETT&CT: MAPPING YOUR BLUE TEAM TO ATT&CK®**



## RUBEN BOUMAN

- Freelance Cyber Defense Expert
- Co-owner Sirius Security
- Roots in development
- Nine years of experience in Info Security
- Co-developer of the DeTT&CT framework

 @RubenB\_2



## MARCUS BAKKER

- Freelance Cyber Defense Expert
- Nine years of experience in Info Security
- Co-developer of the DeTT&CT framework
- Co-author of the TaHiTI Threat Hunting Methodology

 @Bakk3rM



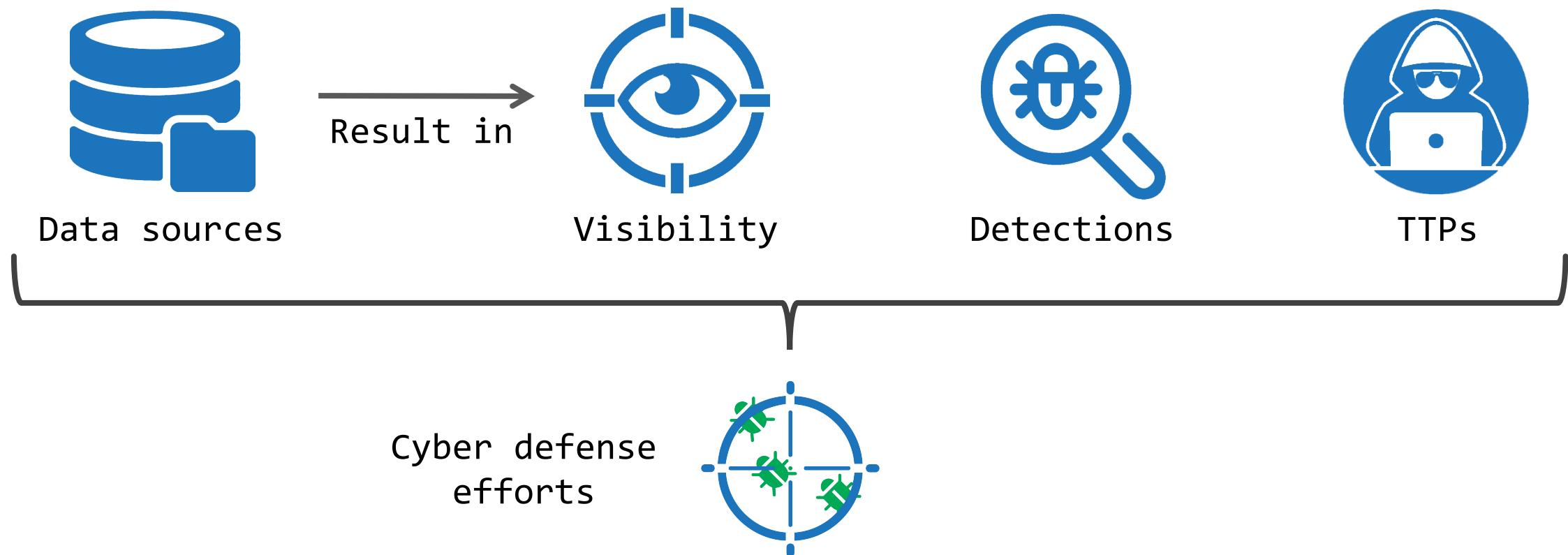
# AGENDA

MAPPING YOUR BLUE TEAM

- Introduction on DeTT&CT
- New features
- Roadmap

# CHALLENGE: WHERE DO WE START OUR CYBER DEFENSE EFFORTS

- Intelligence-driven approach with a focus on TTPs



# DETECT TTCOMBAT T

- Framework to administrate, score and compare:
  - Data source quality
  - Visibility
  - Detections
  - Threat actor behaviours
- Result: where do you focus on
  - Which techniques?
  - Where to improve visibility?
- Scoring tables to guide you
- Administration = YAML files

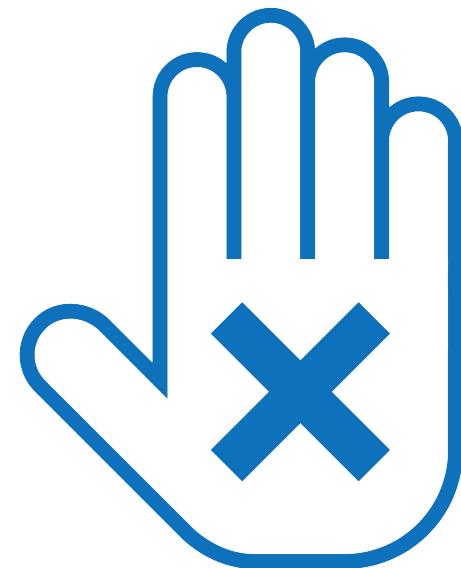


DeTT&CT



[github.com/rabobank-cdc/DeTTECT](https://github.com/rabobank-cdc/DeTTECT)

All shown data and visualisation regarding  
data quality, visibility, detection and  
threat actor groups are based on sample data.



# DATA SOURCES: WHAT DO WE LOG

- Identify data sources

## Process injection

ID: T1055

Tactic: Defense Evasion, Privilege Escalation

Platform: Linux, macOS, Windows

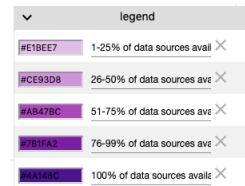
Permissions Required: User, Administrator, SYSTEM, root

Effective Permissions: User, Administrator, SYSTEM, root

Data Sources: API monitoring, Windows Registry, File monitoring, DLL monitoring, Process monitoring, Named Pipes

- Score data quality (DQ)
- Visualise in the ATT&CK Navigator
- Export to Excel

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	27 items	42 items	21 items	57 items	16 items	22 items	15 items	13 items	21 items	9 items	14 items
<a href="#">Drive-by Compromise</a>	<a href="#">CMSTP</a>	<a href="#">Accessibility Features</a>	<a href="#">Access Token Manipulation</a>	<a href="#">Account Manipulation</a>	<a href="#">Account Discovery</a>	<a href="#">Application Deployment Software</a>	<a href="#">Audio Capture</a>	<a href="#">Commonly Used Port</a>	<a href="#">Automated Exfiltration</a>	<a href="#">Data Destruction</a>	
<a href="#">Exploit Public-Facing Application</a>	<a href="#">Command-Line Interface</a>	<a href="#">Account Manipulation</a>	<a href="#">Access Token Manipulation</a>	<a href="#">Binary Padding</a>	<a href="#">Brute Force</a>	<a href="#">Application Window Discovery</a>	<a href="#">Clipboard Data</a>	<a href="#">Communication Through Removable Media</a>	<a href="#">Data Compressed</a>	<a href="#">Data Encrypted for Impact</a>	
<a href="#">External Remote Services</a>	<a href="#">Compiled HTML File</a>	<a href="#">AppCert DLLs</a>	<a href="#">Accessibility Features</a>	<a href="#">BITS Jobs</a>	<a href="#">Credential Dumping</a>	<a href="#">Browser Bookmark Discovery</a>	<a href="#">Custom Command and Control Protocol</a>	<a href="#">Data from Information Repositories</a>	<a href="#">Data Transfer Size Limits</a>	<a href="#">Defacement</a>	
<a href="#">Hardware Additions</a>	<a href="#">Control Panel Items</a>	<a href="#">AppInit DLLs</a>	<a href="#">Bypass User Account Control</a>	<a href="#">Credentials In Model</a>	<a href="#">T1003 - Malware: Domain Trust Discovery</a>	<a href="#">Custom Cryptographic Protocol</a>	<a href="#">Data from Local System</a>	<a href="#">Data from Network Shared Drive</a>	<a href="#">Disk Structure Wipe</a>	<a href="#">Disk Content Wipe</a>	
<a href="#">Replication Through Removable Media</a>	<a href="#">Dynamic Data Exchange</a>	<a href="#">Application Shimming</a>	<a href="#">CMSTP</a>	<a href="#">Credentials In Application Shimming</a>	<a href="#">Available data sources: Process monitoring, PowerShell logs, Service Scanning</a>	<a href="#">Exploitation of Remote Services</a>	<a href="#">Data from Removable Media</a>	<a href="#">Data Obfuscation</a>	<a href="#">Endpoint Denial of Service</a>	<a href="#">Firmware Corruption</a>	
<a href="#">Spearphishing Attachment</a>	<a href="#">Execution through API Load</a>	<a href="#">Bootkit</a>	<a href="#">Code Signing</a>	<a href="#">Exploitation for Client Execution</a>	<a href="#">Exploitation for C2X API Monitoring</a>	<a href="#">Logon Scripts</a>	<a href="#">Data from Network Shared Drive</a>	<a href="#">Data Staged</a>	<a href="#">Exfiltration Over Alternative Protocol Channel</a>	<a href="#">Inhibit System Recovery</a>	
<a href="#">Spearphishing Link</a>	<a href="#">Execution through Module</a>	<a href="#">BITS Jobs</a>	<a href="#">Compile After Delivery</a>	<a href="#">Forced Authentication</a>	<a href="#">PowerShell logs, Service Scanning</a>	<a href="#">Logon Scripts</a>	<a href="#">Data from Network Shared Drive</a>	<a href="#">Domain Fronting</a>	<a href="#">Exfiltration Over Other Network Medium</a>	<a href="#">Network Denial of Service</a>	
<a href="#">Spearphishing via Service</a>	<a href="#">Graphical User Interface</a>	<a href="#">Bypass User Account Control</a>	<a href="#">Credential Dumping</a>	<a href="#">Forced Authentication</a>	<a href="#">PowerShell logs, Service Scanning</a>	<a href="#">Logon Scripts</a>	<a href="#">Data from Network Shared Drive</a>	<a href="#">Email Collection</a>	<a href="#">Exfiltration Over Physical Medium</a>	<a href="#">Resource Hijacking</a>	
<a href="#">Supply Chain Compromise</a>	<a href="#">InstallUtil</a>	<a href="#">Component Firmware</a>	<a href="#">Component Object Model</a>	<a href="#">Hijacking</a>	<a href="#">PowerShell logs, Service Scanning</a>	<a href="#">Logon Scripts</a>	<a href="#">Data from Network Shared Drive</a>	<a href="#">Fallback Channels</a>	<a href="#">Scheduled Transfer</a>	<a href="#">Runtime Data Manipulation</a>	
<a href="#">Trusted Relationship</a>	<a href="#">LSASS Driver</a>	<a href="#">Extra Window Memory Injection</a>	<a href="#">Control Panel Items</a>	<a href="#">Kerberoasting</a>	<a href="#">Process Discovery</a>	<a href="#">Logon Scripts</a>	<a href="#">Data from Network Shared Drive</a>	<a href="#">Shared Webroot</a>	<a href="#">Screen Capture</a>	<a href="#">Service Stop</a>	
<a href="#">Valid Accounts</a>	<a href="#">Mshra</a>	<a href="#">File System Permissions</a>	<a href="#">DCShadow</a>	<a href="#">Poisoning and Relay</a>	<a href="#">Query Registry</a>	<a href="#">Replication Through Removable Media</a>	<a href="#">Data from Network Shared Drive</a>	<a href="#">Shared Content</a>	<a href="#">Video Capture</a>	<a href="#">Stored Data Manipulation</a>	
	<a href="#">PowerShell</a>	<a href="#">Create Account</a>	<a href="#">Deobfuscate/Decode Files or Information</a>	<a href="#">Network Sniffing</a>	<a href="#">Remote System Discovery</a>	<a href="#">Security Software Discovery</a>	<a href="#">Data from Network Shared Drive</a>	<a href="#">Taint Shared Content</a>	<a href="#">Third-party Software</a>	<a href="#">Transmitted Data Manipulation</a>	
	<a href="#">Regsvcs/Regasm</a>	<a href="#">DLL Search Order Hijacking</a>	<a href="#">Disabling Security Tools</a>	<a href="#">Password Filter DLL</a>	<a href="#">System Information Discovery</a>	<a href="#">System Network Configuration Discovery</a>	<a href="#">Data from Network Shared Drive</a>	<a href="#">Multiband Communication</a>	<a href="#">Multilayer Encryption</a>	<a href="#">Remote Access Tools</a>	
	<a href="#">Regsvr32</a>	<a href="#">External Remote Services</a>	<a href="#">Image File Execution Options Injection</a>	<a href="#">Private Keys</a>	<a href="#">Two-Factor Authentication Interception</a>	<a href="#">System Network Connections Discovery</a>	<a href="#">Data from Network Shared Drive</a>	<a href="#">Remote File Copy</a>	<a href="#">Standard Application Layer Protocol</a>	<a href="#">Standard Cryptographic Protocol</a>	
	<a href="#">Rundll32</a>	<a href="#">File System Permissions</a>	<a href="#">DLL Side-Loading</a>	<a href="#">System Owner/User Discovery</a>	<a href="#">Windows Admin Shares</a>	<a href="#">System Service Discovery</a>	<a href="#">Data from Network Shared Drive</a>	<a href="#">Standard Non-Application Layer Protocol</a>	<a href="#">Uncommonly Used Port</a>	<a href="#">Web Service</a>	
	<a href="#">Scheduled Task</a>	<a href="#">Weakness</a>	<a href="#">New Service</a>	<a href="#">Execution Guardrails</a>	<a href="#">Windows Remote Management</a>	<a href="#">System Time Discovery</a>	<a href="#">Data from Network Shared Drive</a>				
	<a href="#">Scripting</a>	<a href="#">Hidden Files and Directories</a>	<a href="#">Path Interception</a>	<a href="#">Exploitation for Defense Evasion</a>	<a href="#">Virtualization/Sandbox Evasion</a>						
	<a href="#">Service Execution</a>	<a href="#">Port Monitors</a>	<a href="#">Port Monitors</a>	<a href="#">Extra Window Memory Injection</a>							
	<a href="#">Signed Binary Proxy Execution</a>	<a href="#">Hypervisor</a>	<a href="#">Scheduled Task</a>	<a href="#">File Deletion</a>							
	<a href="#">Signed Script Proxy Execution</a>	<a href="#">Image File Execution Options Injection</a>	<a href="#">File Permissions Modification</a>	<a href="#">File System Logical Offsets</a>							
	<a href="#">Third-party Software</a>	<a href="#">Logon Scripts</a>	<a href="#">Service Registry Permissions Weakness</a>	<a href="#">Group Policy Modification</a>							
	<a href="#">Trusted Developer Utilities</a>	<a href="#">LSASS Driver</a>	<a href="#">SID-History Injection</a>	<a href="#">Hidden Files and Directories</a>							
	<a href="#">User Execution</a>	<a href="#">Valid Accounts</a>	<a href="#">Image File Execution Options Injection</a>	<a href="#">Image File Execution Options Injection</a>							
	<a href="#">Windows Management Instrumentation</a>	<a href="#">Web Shell</a>	<a href="#">Indicator Blocking</a>	<a href="#">Indicator Removal from Tools</a>							
	<a href="#">Windows Remote Management</a>	<a href="#">Netsh Helper DLL</a>	<a href="#">New Service</a>	<a href="#">Indicator Removal on Host</a>							
			<a href="#">Office Application Startup</a>	<a href="#">Indirect Command Execution</a>							
			<a href="#">Path Interception</a>	<a href="#">Install Root Certificate</a>							
			<a href="#">Port Monitors</a>	<a href="#">InstallUtil</a>							
			<a href="#">Redundant Access</a>	<a href="#">Masquerading</a>							
			<a href="#">Registry Run Keys / Startup Folder</a>	<a href="#">Modify Registry</a>							
			<a href="#">Scheduled Task</a>	<a href="#">Mshra</a>							
			<a href="#">Screensaver</a>	<a href="#">Network Share Connection Removal</a>							
			<a href="#">Security Support Provider</a>	<a href="#">NTFS File Attributes</a>							
			<a href="#">Service Registry Permissions Weakness</a>	<a href="#">Obfuscated Files or Information</a>							
			<a href="#">Shortcut Modification</a>	<a href="#">Process Doppelgänging</a>							
			<a href="#">SIP and Trust Provider Hijacking</a>	<a href="#">Process Hollowing</a>							
			<a href="#">System Firmware</a>	<a href="#">Process Injection</a>							
			<a href="#">Time Providers</a>	<a href="#">Redundant Access</a>							
			<a href="#">Valid Accounts</a>	<a href="#">Regsvcs/Regasm</a>							
			<a href="#">Web Shell</a>	<a href="#">Regsvr32</a>							
			<a href="#">Windows Management Instrumentation Event Subscription</a>	<a href="#">Rootkit</a>							
			<a href="#">Winlogon Helper DLL</a>	<a href="#">Rundll32</a>							
				<a href="#">Scripting</a>							
				<a href="#">Signed Binary Proxy Execution</a>							
				<a href="#">Signed Script Proxy Execution</a>							
				<a href="#">SIP and Trust Provider Hijacking</a>							
				<a href="#">Software Packing</a>							
				<a href="#">Template Injection</a>							



# VISIBILITY: WHAT CAN WE SEE?

- Manual score visibility
  - Allows you to be exact
  - One source is more important than the other
  - Minimal set of data sources to have useful visibility

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.

- Administristrate in YAML file
- Visualise in the ATT&CK Navigator
- Export to Excel

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	27 items	42 items	21 items	57 items	16 items	22 items	15 items	13 items	21 items	9 items	14 items
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Commonly Used Port	Automated Exfiltration	Compressed Data	Data Encrypted for Impact
Exploit Public-Facing Application	Command-Line Interface	Account Manipulation	Binary Padding	Brute Force	Application Window Discovery	Distributed Component Object Model	Clipboard Data	Communication Through Removable Media	Connection Proxy	Metadata:	T1043
External Remote Services	Compiled HTML File	Accessibility Features	BITS Jobs	Credential Dumping	Browser Bookmark Discovery	Custom Command and Control Protocol	Data from Information Repositories	Custom Command and Control Protocol	Custom Cryptographic Protocol	File and Registry Monitoring	Defacement
Hardware Additions	Control Panel Items	AppCert DLLs	AppCert DLLs	Credentials in File	Domain Trust Discovery	Exploitation of Remote Services	Data from Local System	Data from Network Shared Drive	Data Encoding	File Monitoring	Disk Content Wipe
Dynamic Data Exchange	Dynamic Shimming	Appmit DLLs	CMSTP	Credentials in Registry	File and Directory Discovery	Exploitation of Remote Services	Exploitation of Remote Services	Data from Removable Media	Data Obfuscation	File Transfer	Disk Structure Wipe
Replication Through Removable Media	Execution through API	Authentication Package	Application Shimming	Code Signing	Forced Authentication	Fileless Exploit	Fileless Exploit	Data Staged	Domain Fronting	Fileless Monitoring	Endpoint Denial of Service
Exploitation through Module Load	Execution through BITS Jobs	Bypass User Account Control	Bypass User Account Control	Forced Authentication	Fileless Exploit	Fileless Exploit	Fileless Exploit	Email Collection	Domain Fronting	Fileless Monitoring	Firmware Corruption
Spearphishing Attachment	Exploitation for Client Execution	Bootkit	DLL Search Order Hijacking	Forced Authentication	Fileless Exploit	Fileless Exploit	Fileless Exploit	Inhibit System Recovery	Domain Fronting	Fileless Monitoring	Inhibit System Recovery
Spearphishing Link	Exploitation for Client Execution	Browser Extensions	Forced Authentication	Fileless Exploit	Fileless Exploit	Fileless Exploit	Fileless Exploit	Domain Generation Algorithm	Domain Fronting	Fileless Monitoring	Network Denial of Service
Spearphishing via Service	Graphical User Interface	Change Default File Association	Fileless Exploit	Fileless Exploit	Fileless Exploit	Fileless Exploit	Fileless Exploit	Exfiltration Over Physical Medium	Domain Fronting	Fileless Monitoring	Resource Hijacking
Supply Chain Compromise	InstallUtil	Component Firmware	Extra Window Memory Injection	Fileless Exploit	Fileless Exploit	Fileless Exploit	Fileless Exploit	Exfiltration Over Physical Medium	Domain Fronting	Fileless Monitoring	Runtime Data Manipulation
Trusted Relationship	LSASS Driver	Component Object Model Hijacking	File System Permissions	Fileless Exploit	Fileless Exploit	Fileless Exploit	Fileless Exploit	Exfiltration Over Physical Medium	Domain Fronting	Fileless Monitoring	Service Stop
Valid Accounts	Mstfa	Create Account	Weakness	Fileless Exploit	Fileless Exploit	Fileless Exploit	Fileless Exploit	Exfiltration Over Physical Medium	Domain Fronting	Fileless Monitoring	Stored Data Manipulation
	PowerShell	Create Account	Weakness	Fileless Exploit	Fileless Exploit	Fileless Exploit	Fileless Exploit	Exfiltration Over Physical Medium	Domain Fronting	Fileless Monitoring	Transmitted Data Manipulation
	Resgvcs/Regasm	DLL Search Order Hijacking	Hijacking	Disabling Security Tools	Fileless Exploit	Fileless Exploit	Fileless Exploit	Exfiltration Over Physical Medium	Domain Fronting	Fileless Monitoring	
	Resgv32	External Remote Services	Image File Execution Options Injection	Fileless Exploit	Fileless Exploit	Fileless Exploit	Fileless Exploit	Exfiltration Over Physical Medium	Domain Fronting	Fileless Monitoring	
	Rundll32	File System Permissions	New Service	Fileless Exploit	Fileless Exploit	Fileless Exploit	Fileless Exploit	Exfiltration Over Physical Medium	Domain Fronting	Fileless Monitoring	
	Scheduled Task	Weakness	Execution Guardrails	Fileless Exploit	Fileless Exploit	Fileless Exploit	Fileless Exploit	Exfiltration Over Physical Medium	Domain Fronting	Fileless Monitoring	
	Scripting	Hidden Files and Directories	Path Interception	Fileless Exploit	Fileless Exploit	Fileless Exploit	Fileless Exploit	Exfiltration Over Physical Medium	Domain Fronting	Fileless Monitoring	
	Service Execution	Port Monitors	Port Monitors	Fileless Exploit	Fileless Exploit	Fileless Exploit	Fileless Exploit	Exfiltration Over Physical Medium	Domain Fronting	Fileless Monitoring	
	Signed Binary Proxy Execution	Process Injection	Process Injection	Fileless Exploit	Fileless Exploit	Fileless Exploit	Fileless Exploit	Exfiltration Over Physical Medium	Domain Fronting	Fileless Monitoring	
	Signed Script Proxy Execution	Hijacking	Hijacking	Fileless Exploit	Fileless Exploit	Fileless Exploit	Fileless Exploit	Exfiltration Over Physical Medium	Domain Fronting	Fileless Monitoring	
	Signed Script Proxy Execution	Hypervisor	Scheduled Task	Fileless Exploit	Fileless Exploit	Fileless Exploit	Fileless Exploit	Exfiltration Over Physical Medium	Domain Fronting	Fileless Monitoring	
	Third-party Software	Image File Execution Options Injection	Service Registry Permissions Weakness	Fileless Exploit	Fileless Exploit	Fileless Exploit	Fileless Exploit	Exfiltration Over Physical Medium	Domain Fronting	Fileless Monitoring	
	Trusted Developer Utilities	Logon Scripts	SID-History Injection	Fileless Exploit	Fileless Exploit	Fileless Exploit	Fileless Exploit	Exfiltration Over Physical Medium	Domain Fronting	Fileless Monitoring	
	User Execution	LSASS Driver	Valid Accounts	Fileless Exploit	Fileless Exploit	Fileless Exploit	Fileless Exploit	Exfiltration Over Physical Medium	Domain Fronting	Fileless Monitoring	
	Windows Management Instrumentation	Modify Existing Service	Web Shell	Fileless Exploit	Fileless Exploit	Fileless Exploit	Fileless Exploit	Exfiltration Over Physical Medium	Domain Fronting	Fileless Monitoring	
	New Service	Netsh Helper DLL	Indicator Blocking	Fileless Exploit	Fileless Exploit	Fileless Exploit	Fileless Exploit	Exfiltration Over Physical Medium	Domain Fronting	Fileless Monitoring	
	Windows Remote Management	Office Application Startup	Indicator Removal from Tools	Fileless Exploit	Fileless Exploit	Fileless Exploit	Fileless Exploit	Exfiltration Over Physical Medium	Domain Fronting	Fileless Monitoring	
	XSL Script Processing	Path Interception	Indirect Command Execution	Fileless Exploit	Fileless Exploit	Fileless Exploit	Fileless Exploit	Exfiltration Over Physical Medium	Domain Fronting	Fileless Monitoring	
		Port Monitors	Install Root Certificate	Fileless Exploit	Fileless Exploit	Fileless Exploit	Fileless Exploit	Exfiltration Over Physical Medium	Domain Fronting	Fileless Monitoring	
		Redundant Access	InstallUtil	Fileless Exploit	Fileless Exploit	Fileless Exploit	Fileless Exploit	Exfiltration Over Physical Medium	Domain Fronting	Fileless Monitoring	
		Registry Run Keys / Startup Folder	Masquerading	Fileless Exploit	Fileless Exploit	Fileless Exploit	Fileless Exploit	Exfiltration Over Physical Medium	Domain Fronting	Fileless Monitoring	
			Modify Registry	Fileless Exploit	Fileless Exploit	Fileless Exploit	Fileless Exploit	Exfiltration Over Physical Medium	Domain Fronting	Fileless Monitoring	



# DETECTION: WHAT IS OUR DETECTION COVERAGE?

- Manual score detection
- Administrated in the same YAML file as visibility
- Visualise in the ATT&CK Navigator
- Export to Excel

## 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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	27 items	42 items	21 items	57 items	16 items	22 items	15 items	13 items	21 items	9 items	14 items
Spearphishing Attachment	Scripting	Registry Run Keys / Startup Folder	Valid Accounts	Scripting	Credential Dumping	Process Discovery	Remote File Copy	Data from Local	Remote File Copy	Data Compressed	Disk Structure Wipe
Valid Accounts	User Execution	Scheduled Task	Obfuscated Files or Information	Input Capture	System Information Discovery	Remote Desktop Protocol	T1105 Score: 30	Staged Metadata	Standard Application Layer Protocol	Data Encrypted	Data Destruction
Spearphishing Link	PowerShell	Scheduled Task	Process Injection	Valid Accounts	Brute Force	System Network Configuration Discovery	Windows Admin Shares	-Groups: Threat Group-3390, APT13, Cobalt Strike, Evil, Magic Hound, FIN7, Lure, Elderwood, APT38, Gorgon Group, Lazarus Group, PLATINUM, Dragonfly 2.0, MuddyWater, APT18, Turla, FIN8, Rancor, APT37, OilRig, FIN10, BRONZE BUTLER, Patchwork, APT32, WIRTE, APT33, APT28, Menapias	Commonly Used Port	Exfiltration Over Command and Control Channel	Data Encrypted for Impact
Drive-by Compromise	Command-Line Interface	External Remote Services	New Service	File Deletion	Credentials in Files	File and Directory Discovery	Web Service	Standard Cryptographic Protocol	Connection Proxy	Automated Exfiltration	Resource Hijacking
External Remote Services	Scheduled Task	New Service	Masquerading	Network Sniffing	System Owner/User Discovery	Remote System Discovery	Pass the Hash	Pass the Ticket	Data Transfer Size Limits	Uncommonly Used Port	Runtime Data Manipulation
Exploit Public-Facing Application	Exploitation for Client Execution	Web Shell	Deobfuscate/Decode Files or Information	Forced Authentication	Account Manipulation	Account Discovery	Exploitation of Remote Services	Exploitability	Data Encoding	Exfiltration Over Alternative Protocol	Disk Content Wipe
Replication Through Removable Media	Windows Management Instrumentation	Shortcut Modification	Software Packing	Credentials in Registry	System Network Connections Discovery	Network Service Scanning	Logon Scripts	Custom Command and Control Protocol	Network Medium	Service Stop	Transmitted Data Manipulation
Spearphishing via Service	Dynamic Data Exchange	Redundant Access	Privilege Escalation	Web Service	Hooking	Security Software Discovery	Replication Through Removable Media Repositories	Removable Media	Custom Cryptographic Protocol	Inhibit System Recovery	Network Denial of Service
Rundll32	Rundll32	Accessibility Features	Accessibility Features	Code Signing	Input Prompt	Query Registry	Application Deployment Software	Video Capture	Clipboard Data	Defacement	Endpoint Denial of Service
Trusted Relationship	Regsvr32	Create Account	Access Token Manipulation	Modify Registry	Exploitation for Credential Access	Permission Groups Discovery	Audio Capture	Custom Non-Application Layer Protocol	Man in the Browser	Data Obfuscation	Firmware Corruption
Supply Chain Compromise	Service Execution	Hidden Files and Directories	DLL Search Order Hijacking	Process Injection	Kerberoasting	System Service Discovery	Distributed Component Object Model	Taint Shared Content	Shared Webroot	Fallback Channels	Inhibit System Recovery
Compiled HTML File	Compiled HTML File	Service Execution	Bypass User Account Control	LLMNR/NBT-NS Poisoning and Relay	Private Keys	Network Share Discovery	Peripheral Device Discovery	Third-party Software	Multi-hop Proxy	Multi-Stage Channels	Network Denial of Service
Hardware Additions	Compiled HTML File	Account Manipulation	AppCert DLLs	DLL Side-Loading	Two-Factor Authentication Interception	System Time Discovery	Network Sniffing	Windows Remote Management	Communication Through Removable Media	Domain Fronting	Domain Generation Algorithms
Execution through API	Execution through API	Modify Existing Service	Application Shimming	Indicator Removal from Tools	Redundant Access	Virtualization/Sandbox Evasion	Application Window Discovery	Shared Webroot	Multi-band Communication	Multi-layer Encryption	Multilayer Encryption
Mshta	Windows Management Instrumentation Event Subscription	Hooking	DLL Side-Loading	Rundll32	Binary Padding	Browser Bookmark Discovery	Domain Trust Discovery				
Signed Binary Proxy Execution	CMSTP	BITS Jobs	Image File Execution Options Injection	Indicator Removal on Host	Indicator Removal on Host						
Graphical User Interface	Bootkit	Port Monitors	Port Monitors	Indicator Removal on Host	Two-Factor Authentication Interception						
Signed Script Proxy Execution	DLL Search Order Hijacking	Appinit DLLs	Appinit DLLs	Indicator Removal on Host	Redundant Access						
Third-party Software	Logon Scripts	Extra Window Memory Injection	Extra Window Memory Injection	Indicator Removal on Host	Binary Padding						
Windows Remote Management	Office Application Startup	File System Permissions Weakness	File System Permissions Weakness	Indicator Removal on Host	Indicator Removal on Host						
XSL Script Processing	Winlogon Helper DLL	Weakness	Weakness	Template Injection	Template Injection						
Control Panel Items	AppCert DLLs	Path Interception	Path Interception	Timestamp	Timestamp						
Execution through Module Load	Application Shimming	Service Registry Permissions Weakness	Service Registry Permissions Weakness	Access Token Manipulation	Access Token Manipulation						
InstallUtil	Browser Extensions	Weakness	Weakness	MSHTA	MSHTA						
LSASS Driver	Component Firmware	Weakness	Weakness	Process Hollowing	Process Hollowing						
Regsvcs/Regasm	Component Object Model Hijacking	Weakness	Weakness	Signed Binary Proxy Execution	Signed Binary Proxy Execution						
Trusted Developer Utilities	Hooking	Weakness	Weakness	BITS Jobs	BITS Jobs						
	Image File Execution Options Injection	Weakness	Weakness	CMSTP	CMSTP						
	Port Monitors	Weakness	Weakness	DLL Search Order Hijacking	DLL Search Order Hijacking						
	Appinit DLLs	Weakness	Weakness	Execution Guardrails	Execution Guardrails						
	Authentication Package	Weakness	Weakness	Rootkit	Rootkit						
	Change Default File Association	Weakness	Weakness	Virtualization/Sandbox Evasion	Virtualization/Sandbox Evasion						
	File System Permissions Weakness	Weakness	Weakness	Compile After Delivery	Compile After Delivery						
	Hypervisor	Weakness	Weakness	Component Firmware	Component Firmware						
	LSASS Driver	Weakness	Weakness	Component Object Model Hijacking	Component Object Model Hijacking						
				Exploitation for Defense Evasion	Exploitation for Defense Evasion						
				File Permissions Modification	File Permissions Modification						

\*1 <https://github.com/rabobank-cdc/DeTECT/tree/master/threat-actor-data>



# 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

```
%YAML 1.2
---
version: 1.0
file_type: group-administration
groups:
  - group_name: Red team
    campaign: Scenario 1
    technique_id: [T1086, T1053, T1193, T1204, T1003, T1055, T1027, T1085, T1099, T1082, T1016, T1033, T1087, T1075, T1057, T1039, T1041, T1071, T1043, T1001, T1114, T1002]
    software_id: [S0002] # Mimikatz
    enabled: True
```



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	27 items	42 items	21 items	57 items	16 items	22 items	15 items	13 items	21 items	9 items	14 items
Spearphishing Attachment	PowerShell	Scheduled Task	Process Injection	Obfuscated Files or Information	Credential Dumping	Account Discovery	Pass the Hash	Data from Network Shared Drive	Commonly Used Port	Data Compressed	Data Destruction
Rundll32	Accessibility Features	Scheduled Task	Process Injection	T1027 Score: 1 Metadata: -Groups: Red team	Brute Force	Process Discovery	System Information Discovery	Application Deployment Software	Email Collection	Standard Application Layer Protocol	Data Obfuscation
Drive-by Compromise	User Execution	Account Manipulation	Access Token Manipulation	Rundll32	Timestamp	Credentials in Files	System Network Configuration Discovery	Distributed Component Object Model	Audio Capture	Exfiltration Over Command and Control Channel	Defacement
Exploit Public-Facing Application	CMSTP	AppCert DLLs	Accessibility Features	Binary Padding	System Owner/User Discovery	Exploitation of Remote Services	Automated Collection	Communication Through Removable Media	Clipboard Data	Automated Exfiltration	Disk Content Wipe
External Remote Services	Command-Line Interface	AppInit DLLs	AppCert DLLs	BITS Jobs	Application Window Discovery	Logon Scripts	Data from Information Repositories	Connection Proxy	Data from Local System	Data Encrypted	Disk Structure Wipe
Hardware Additions	Compiled HTML File	Application Shimming	AppInit DLLs	Exploitation for Credential Access	Browser Bookmark Discovery	Pass the Ticket	Custom Command and Control Protocol	Custom Cryptographic	Custom	Data Transfer Size Limits	Endpoint Denial of Service
Replication Through Removable Media	Dynamic Data Exchange	BITS Jobs	Application Shimming Package	Bypass User Account Control	Domain Trust Discovery	Remote Desktop Protocol	Exfiltration Over Alternative	Custom	Custom	Firmware Corruption	
		Bootkit	Bypass User Account	CMSTP	Forced Authentication						
		Execution through	Code Signing								

\*1 <https://github.com/rabobank-cdc/DeTECT/tree/master/threat-actor-data>



# 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

```
groups:
  - group_name: Red team
    campaign: Scenario 1
    technique_id: [T1086, T1053, T1193, T1204, T1003, T1055, T1027, T1085, T1099, T1082, T1016, T1033, T1087, T1075, T1057, T1039, T1041, T1071, T1043, T1001, T1114, T1002]
    software_id: [S0002]
    enabled: True

  - group_name: APT3 (MITRE ATT&CK evaluation)
    campaign: First Scenario
    technique_id: [T1204, T1064, T1085, T1060, T1043, T1071, T1132, T1016, T1059, T1033, T1057, T1106, T1007, T1082, T1069, T1087, T1012, T1088, T1134, T1055, T1018, T1049, T1003, T1026, T1076, T1136, T1061, T1105, T1053, T1083, T1056, T1010, T1113, T1039, T1041, T1078]
    software_id: [S0154]
    enabled: True
```



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	27 items	42 items	21 items	57 items	16 items	22 items	15 items	13 items	21 items	9 items	14 items
Spearphishing Attachment	Rundll32	Scheduled Task	Process Injection	Process Injection	Credential Dumping	Account Discovery	Pass the Hash	Data from Network Shared Drive	Commonly Used Port	Exfiltration Over Command and Control Channel	Data Destruction
Valid Accounts	Scheduled Task	Create Account	Scheduled Task	T1055 Score: 2 Metadata: Token-Groups: APT3 (MITRE ATT&CK evaluation), Red team	Input Capture	Process Discovery	Remote Desktop Protocol	Standard Application Layer Protocol	Command and Control Protocol	Data Encrypted for Impact	
Drive-by Compromise	User Execution	Registry Run Keys / Startup Folder	Access Token Manipulation	Access Token Manipulation	Account Manipulation	System Information Discovery	Email Collection	Remote File Copy	Input Capture	Data Encoding	Defacement
Exploit Public-Facing Application	Command-Line Interface	Valid Accounts	Bypass User Account Control	Bypass User Account Control	Brute Force	System Network Configuration Discovery	System Owner/User Discovery	Application Deployment Software	Screen Capture	Data Obfuscation	Disk Content Wipe
External Remote Services	Execution through API	Accessibility Features	Obfuscated Files or Information	Obfuscated Files or Information	Credentials in Files	Application Window Discovery	Distributed Component Object Model	Multiband Communication	Data Compressed	Automated Exfiltration	Disk Structure Wipe
Hardware Additions	Graphical User Interface	Account Manipulation	Scripting	Scripting	Credentials in Registry	File and Directory Discovery	Automated Collection	Audio Capture	Data Encrypted	Data Transfer	Endpoint Denial of Service
Replication Through Removable Media	PowerShell	AppCert DLLs	Timestamp	Timestamp	Exploitation for Credential Access	Permission Groups Discovery	Clipboard Data Through	Communication Through	Remote File Copy	Remote Media	Firmware Corruption
Spearphishing Link	Scripting	AppInit DLLs	Valid Accounts	Valid Accounts	Binary Padding	File and Directory Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Removable Media	Inhibit System Recovery
Spearphishing via Service	CMSTP	Application Shimming	AppCert DLLs	AppInit DLLs	Forced Authentication	Query Registry	Custom Logon Scripts	Custom Command and Control Protocol	Custom Alternative Protocol	Exfiltration Over Other Network Medium	Network Denial of Service
Supply Chain Compromise	Compiled HTML File	Authentication Package	BITS Jobs	BITS Jobs	CMSTP	Remote System Discovery	Pass the Ticket	Data from Local System	Command and Control Protocol	Exfiltration Over Physical Medium	Resource Hijacking
	Control Panel Items	Application Shimming	DLL Search Order Hijacking	Code Signing	Hooking	System Network Connections Discovery	Remote Services	Data from Removable Media	Custom Cryptographic Protocol	Exfiltration Over Other Network Medium	Runtime Data Manipulation
	Dynamic Data Exchange	BITS Jobs	Compile After Delivery	Input Prompt	Kerberoasting	System Service Discovery	Replication Through Removable Media	Data Staged	Domain Fronting	Man in the Domain	
	Execution through Module Load	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Component Firmware	LLMNR/NBT-NS Poisoning and Relay	System Service Discovery				
	Exploitation for Client Execution	Browser Extensions	Change Default	Component Object	Extra Window						

\*1 <https://github.com/rabobank-cdc/DeTECT/tree/master/threat-actor-data>



# Prioritise Your Cyber Defense Efforts

- Intelligence-driven approach with a focus on TTPs

## Legend

The technique only present in the group

We have some level of detection

We have detection and used by the group

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	27 items	42 items	21 items	57 items	16 items	22 items	15 items	13 items	21 items	9 items	14 items
Drive-by Compromise	Control Panel Items	Security Support Provider	Access Token Manipulation	Access Token Manipulation	Input Capture	Password Policy Discovery	Logon Scripts	Input Capture	Domain Fronting	Data Compressed	Endpoint Denial of Service
Supply Chain Compromise	Service Execution	AppCert DLLs	Extra Window Memory Injection	Control Panel Items	Credential Dumping	Remote System Discovery	Pass the Hash	Data from Network Shared Drive	Uncommonly Used Port	Data Encrypted	Network Denial of Service
Spearphishing Attachment	PowerShell	Logon Scripts	Extra Window Memory Injection	Extra Window Memory Injection	Credentials in Registry	System Information Discovery	Application Deployment Software	Remote Access Tools	Exfiltration Over Command and Control Channel	Data Encrypted for Impact	
Exploit Public-Facing Application	Regsvr32	Image File Execution Options	Process Injection	Masquerading	LLMNR/NBT-NS Poisoning and Relay	System Owner/User Discovery	Distributed Component Object Model	Audio Capture	Commonly Used Port		
	Rundll32	Execution Options	AppCert DLLs	Process Injection	Process Injection	Account Discovery	Automated Collection	Clipboard Data	Data Obfuscation	Automated Exfiltration	Data Destruction
External Remote Services	Scripting	Injection	Regsvr32	Regsvr32	Account Manipulation	Process Discovery	Exploitation of Remote Services	Standard Application Layer Protocol	Data Transfer Size Limits	Data Transfer	Defacement
	Scheduled Task	Application Shimming	Rundll32	Rundll32	Brute Force	System Network Configuration Discovery	Pass the Ticket	Data from Information Repositories	Exfiltration Over Alternative Protocol	Exfiltration Over Wipe	Disk Content Wipe
Hardware Additions	User Execution	Scheduled Task	Scripting	Scripting	Credentials in Files	Application Window Discovery	Remote Desktop Protocol	Communication Through Removable Media	Disk Structure Wipe		
	CMSTP	Accessibility Features	Accessibility Features	Image File Execution Options	Exploitation for Credential Access	Browser Bookmark Discovery	Remote File Copy	Data from Local System	Exfiltration Over Other Network Medium	Exfiltration Over Firmware	Corruption
Replication Through Removable Media	Command-Line Interface	Account Manipulation	Account Shimming	Options Injection	Forced Authentication	Domain Trust Discovery	Remote Services	Data from Removable Media	Connection Proxy	Inhibit System Recovery	
	Compiled HTML File	Manipulation	Scheduled Task	Timestomp	Obfuscated Files or Information	File and Directory	Replication Through	Custom Command and Control Protocol	Exfiltration Over Physical Medium	Resource	
Spearphishing Link	Dynamic Data Exchange	Applnit DLLs	Accessibility Features	Information	Hooking			Data Staged			
Spearphishing via Service	Execution through API	Authentication Package	Applnit DLLs	Binary Padding							

# NEW FEATURES

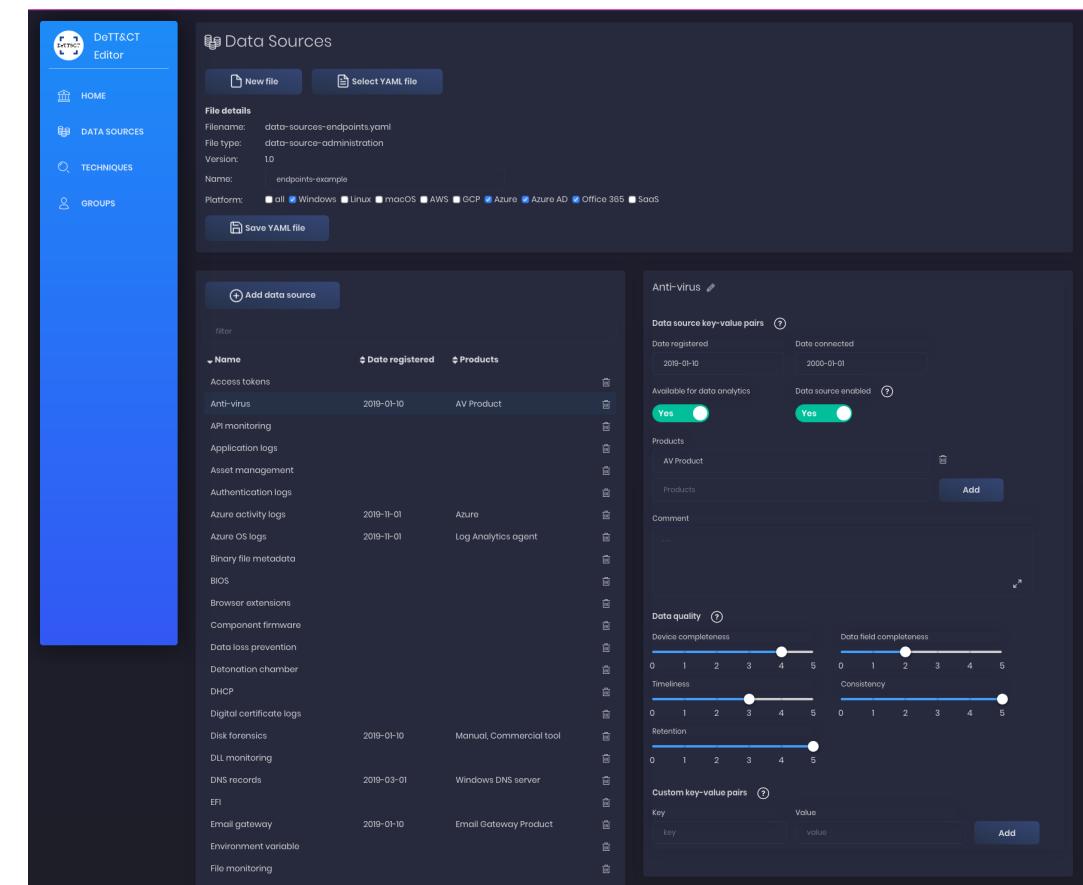
MAPPING YOUR BLUE TEAM

- DeTT&CT Editor
- Group YAML files with a count per technique
- Added support for cloud platforms
- EQL integration
- Score logbook for keeping track of historic data
- Updating visibility scores based on a updated data source admin. file

# DETT&CT EDITOR

- Editing big YAML files by hand is cumbersome and introduces errors
- Use it online: <https://rabobank-cdc.github.io/detectt-editor>
  - It's fully client side and developed in Vue JS
- Run it locally:

```
python detectt.py editor
```



# GROUP YAML FILES WITH A COUNT

```
1 %YAML 1.2
2 ---
3 # Source: https://www.crowdstrike.com/resources/reports/2020-crowdstrike-global-threat-report/
4 version: 1.0
5 file_type: group-administration
6 platform:
7   - Windows
8   - Linux
9   - macOS
10 groups:
11   - group_name: CrowdStrike Global Threat Report 2020
12     campaign:
13       technique_id:
14         T1059 : 70
15         T1078 : 65
16         T1064 : 56
17         T1016 : 54
18         T1105 : 53
19         T1003 : 52
20         T1086 : 52
21         T1033 : 51
22         T1087 : 50
23         T1076 : 48
24         T1082 : 48
25         T1049 : 46
26         T1018 : 45
27         T1057 : 43
28         T1083 : 42
29         T1089 : 40
30         T1047 : 39
31         T1043 : 37
32         T1027 : 34
33         T1100 : 33
34         T1486 : 32
```

# GROUP YAML FILES WITH A COUNT

## Red Canary Threat Detection Report 2020

### Top techniques 2019

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items	22 items	9 items	16 items
Spearphishing Attachment	Scheduled Task	Scheduled Task	Process Injection	Process Injection	Credential Dumping	Domain Trust Discovery	Windows Admin Shares	Audio Capture	Remote File Copy	Automated Exfiltration	Account Access Removal
Drive-by Compromise	PowerShell	DLL Search Order Hijacking	Scheduled Task	Masquerading	Account Manipulation	Account Discovery	Remote File Copy	Automated Collection	Commonly Used Port	Data Compressed	Data Destruction
Exploit Public-Facing Application	Scripting	Accessibility Features	DLL Search Order Hijacking	Disabling Security Tools	Bash History	Application Window Discovery	Clipboard Data	Communication Through Removable Media	Data Encrypted	Data Encrypted for Impact	Defacement
External Remote Services	Service Execution	Windows Management Instrumentation	Local Job Scheduling	DLL Search Order Hijacking	Brute Force	Browser Bookmark Discovery	AppleScript	Data from Information Repositories	Connection Proxy	Data Transfer Size Limits	Disk Content Wipe
Hardware Additions	Rundll32	.bash_profile and .bashrc	Accessibility Features	Scripting	Credentials from Web Browsers	File and Directory Discovery	Application Deployment Software	Custom Command and Control Protocol	Exfiltration Over Alternative Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Replication Through Removable Media	Local Job Scheduling	Account Manipulation	Rundll32	Deobfuscate/Decode Files or Information	Credentials in Files	Network Service Scanning	Component Object Model and Distributed COM	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Endpoint Denial of Service
Spearphishing Link	Mshta	AppCert DLLs	AppCert DLLs	Mshta	Credentials in Registry	Network Share Discovery	Exploitation of Remote Services	Data from Network Shared Drive	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Firmware Corruption
Spearphishing via Service	AppleScript	AppInit DLLs	AppInit DLLs	Process Hollowing	Exploitation for Credential Access	Network Sniffing	Exploitation of Remote Services	Data from Removable Media	Data Encoding	Data Obfuscation	Inhibit System Recovery
	CMSTP	Application Shimming	Application Shimming	Access Token Manipulation		Password Policy Discovery	Internal Spearphishing	Data Staged	Domain Fronting	Exfiltration Over Other Network	Network Denial of Service
	Command-Line Interface	Authentication Package	Bypass User Account Control	Binary Padding		Peripheral Device Discovery	Logon Scripts	Email	Domain Generation	Exfiltration Over Other Network	Network Denial of Service
				BITS Jobs							

# GROUP YAML FILES WITH A COUNT

## CrowdStrike Global Threat Report 2020

### Techniques OverWatch observed in targeted attacks in 2019

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items	22 items	9 items	16 items
Valid Accounts	Command-Line Interface	Valid Accounts	Valid Accounts	Valid Accounts	Credential Dumping	System Network Configuration Discovery	Remote File Copy	Data from Local System	Remote File Copy	Data Compressed	Data Encrypted for Impact
Exploit Public-Facing Application	Web Shell	Web Shell	Scripting	Brute Force	System Owner/User Discovery	Remote Desktop Protocol	Data Staged	Commonly Used Port	Exfiltration Over Command and Control Channel	Inhibit System Recovery	
PowerShell	Create Account	Scheduled Task	Disabling Security Tools	Credentials in Files	Account Discovery	Automated Collection	Uncommonly Used Port		Service Stop		
Spearphishing Attachment	Windows Management Instrumentation	Scheduled Task	Obfuscated Files or Information	New Service	Account Manipulation	Windows Admin Shares	Data from Network Shared Drive	Standard Application Layer Protocol	Resource Hijacking		
External Remote Services	Process Injection	New Service	Masquerading	Process Injection	Bash History	System Network Connections Discovery	Remote Services	Exfiltration Over Alternative Protocol	System Shutdown/Reboot		
Replication Through Removable Media	Rundll32	Account Manipulation	Modify Registry	Modify Registry	Credentials in Registry	Remote System Discovery	Data from Information Repositories	Remote Access Tools	Runtime Data Manipulation		
Spearphishing Link	Graphical User Interface	Modify Existing Service	Accessibility Features	Rundll32	Indicator Removal on Host	Input Capture	Process Discovery	Connection Proxy	Account Access Removal		
Service Execution	Scheduled Task	Registry Run Keys / Startup Folder	Image File Execution Options Injection	Image File Execution Options Injection	File Deletion	Private Keys	Windows Remote Management	Clipboard Data	Data Encrypted	Data Destruction	
Trusted Relationship	Regsvr32	Accessibility Features	Bypass User Account Control	Process Injection	Exploitation for Credential Access	File and Directory Discovery	Email Collection	Standard Cryptographic Protocol	Data Transfer Size Limits	Defacement	
Hardware Additions	Mshta	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	Exploitation for Privilege Escalation	Kerberoasting	Network Service Scanning	Logon Scripts	Web Service	Exfiltration Over Other Network Medium	Disk Content Wipe	
Exploitation for Client Execution	Exploitation for Client Execution	Redundant Access	Exploitation for Privilege Escalation	Access Token Modification	Network Sniffing	Network Share Discovery	Third-party Software	Screen Capture	Custom Command and Control Protocol	Disk Structure Wipe	
Drive-by Compromise	Local Job Scheduling	Redundant Access	Redundant Access	Access Token Modification	Network Sniffing	Permission Groups Discovery	AppleScript	Audio Capture	Exfiltration Over Physical Medium	Endpoint Denial of Service	
Spearphishing via Service	Windows Remote Management	External Remote Services	External Remote Services	Connection Proxy	Two-Factor Authentication Interception	Domain Trust Discovery	Application Deployment Software	Data from Removable Media	Custom Cryptographic Protocol	Firmware Corruption	
Supply Chain Compromise	BITS Jobs	DLL Search Order Hijacking	DLL Side-Loading	DLL Side-Loading	Credentials from Web Browsers	Query Registry	Component Object Model and Distributed COM	Man in the Browser	Data Encoding	Scheduled Transfer	
	CMSTP	DLL Search Order Hijacking	Regsvr32	Setuid and Setgid	Image File Execution Options Injection	System Service Discovery	Video Capture	Standard Non-Application Layer Protocol			
	Control Panel Items	Hidden Files and Directories	Setuid and Setgid	Sudo	Forced Authentication	System Time Discovery	Exploitation of Remote Services				
	Execution through API	Hidden Files and Directories	Sudo	Mshta	Forced Authentication	System Time Discovery	Multiband Communication				
	InstallUtil	Local Job Scheduling	Sudo	AppInit DLLs	Redundant Access	System Time Discovery	Internal Spearphishing				
	Third-party Software	Setuid and Setgid	AppInit DLLs	Redundant Access	Hooking	Security Software Discovery	Multilayer Encryption				
	Trusted Developer Utilities	Windows Management Instrumentation Event	Setuid and Setgid	Service Registry Permissions Weakness	Input Prompt	Network Sniffing	Pass the Hash				
	User Execution	Startup Items	Clear Command History	Keychain	LLMNR/NBT-NS Poisoning and Relay	Pass the Hash	Communication Through Removable Media				
	XSL Script Processing	Subscription	Timestamp	Startup Items	LLMNR/NBT-NS Poisoning and Relay	Pass the Ticket	Pass the Ticket				
		AppCert DLLs	Web Service	AppCert DLLs	Input Prompt	Peripheral Device Discovery	Shared Webroot				
		Application Shimming	Access Token Manipulation	AppCert DLLs	Input Prompt	Software Discovery	Domain Fronting				
		Security DLL	Security DLL	Security DLL	Security DLL	Software Discovery	SSH Hijacking				
		Application Window	Application Window	Security DLL	Security DLL	Software Discovery	Taint Shared				

# CLOUD PLATFORMS

- Allow the use of cloud platforms
- Mapping data sources to platforms
  - <https://github.com/rabobank-cdc/DeTTECT/wiki/Data-sources-per-platform>

# ENDGAME'S EQL INTEGRATION IN DETT&CT

- Use EQL to filter your YAML data in DeTT&CT



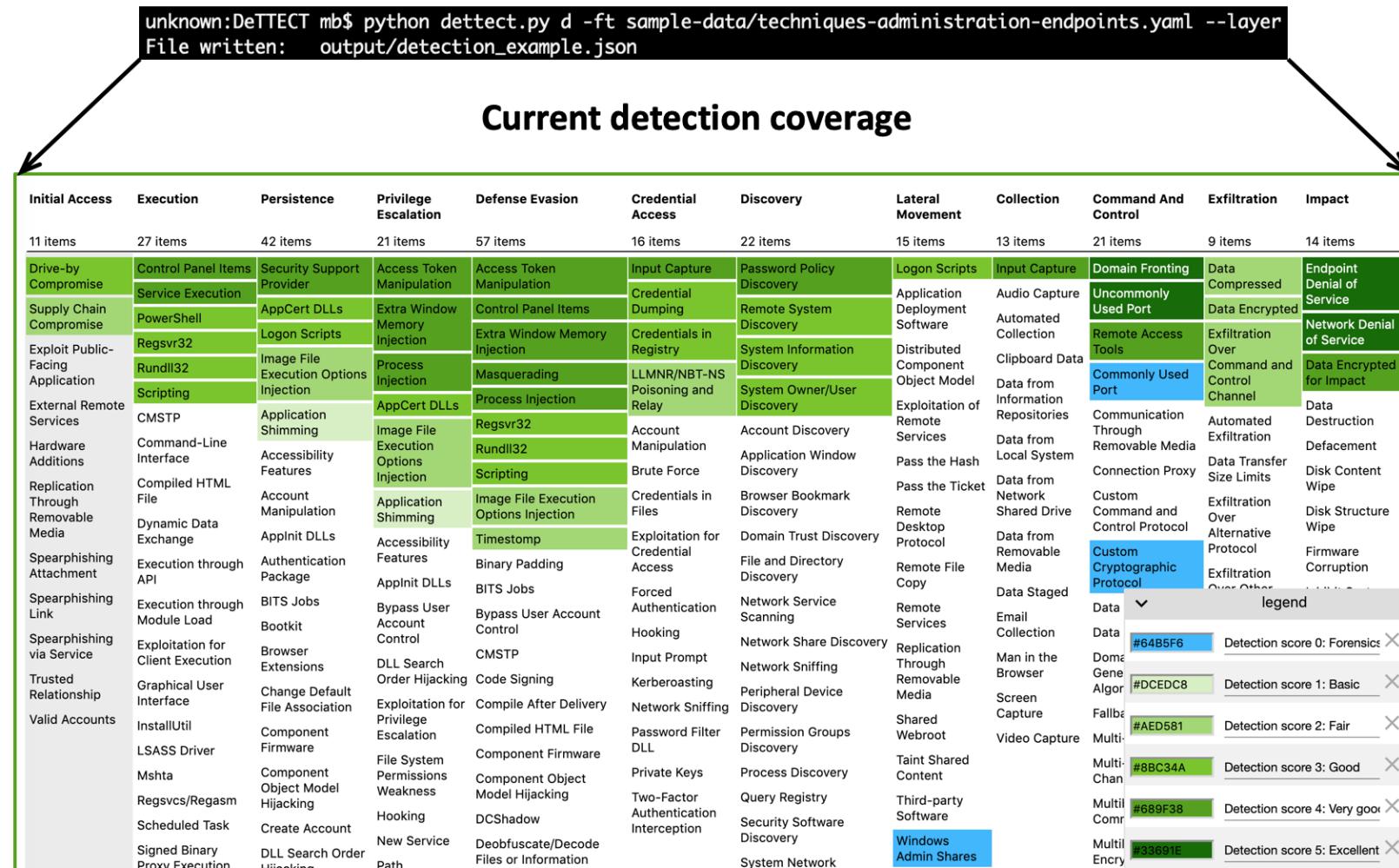
- Example use case: how did our detection coverage look like X time ago?

```
python dettect.py d -ft sample-data/techniques-admin.yaml --layer  
--search-detection "techniques where detection.score_logbook.date <  
'2017-11-01'" --all-scores
```

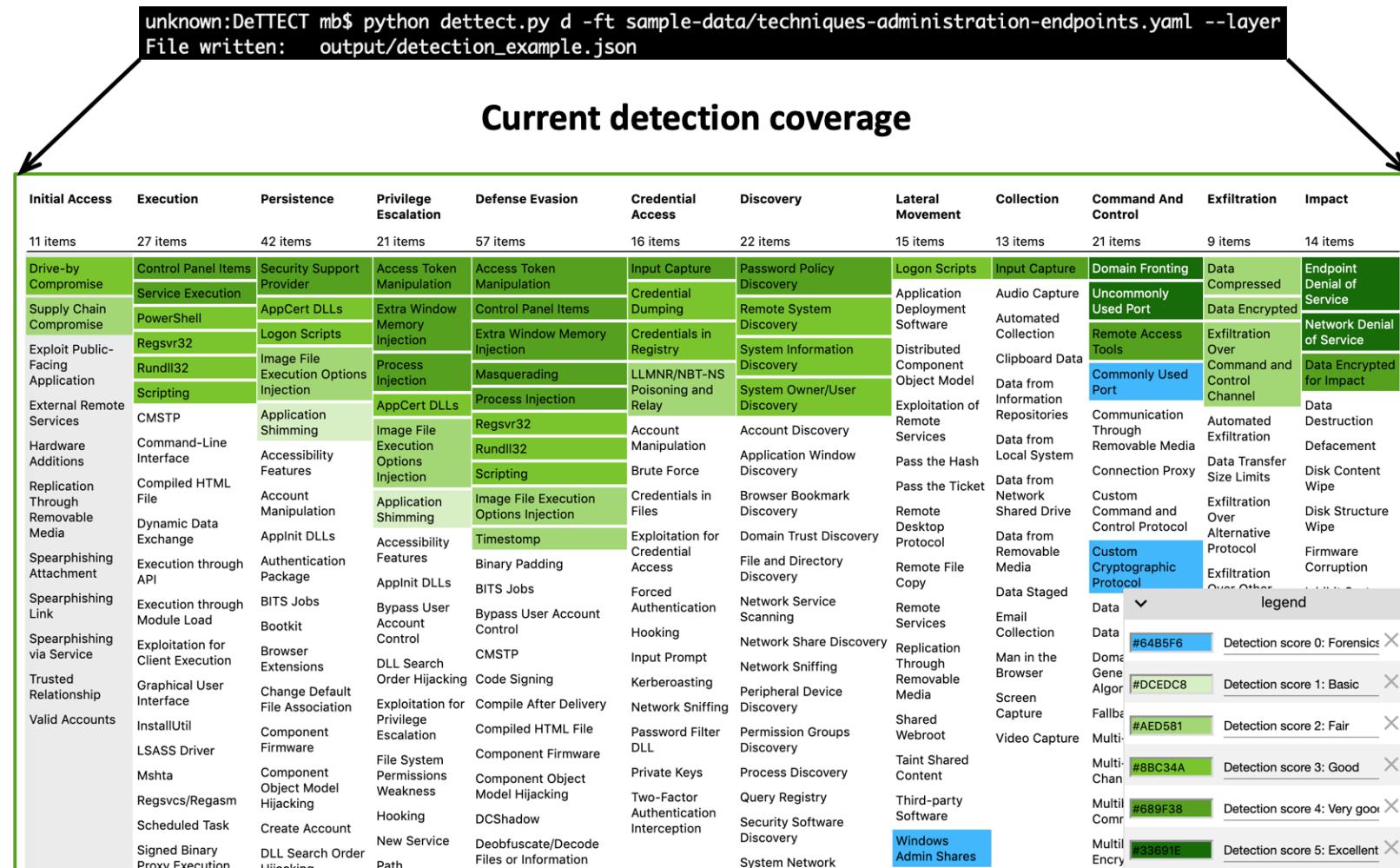
- Only include data sources which can be used in data analytics:

```
python dettect.py ds -fd sample-data/data-sources-endpoints.yaml -l  
--search "data_sources where available_for_data_analytics = true"
```

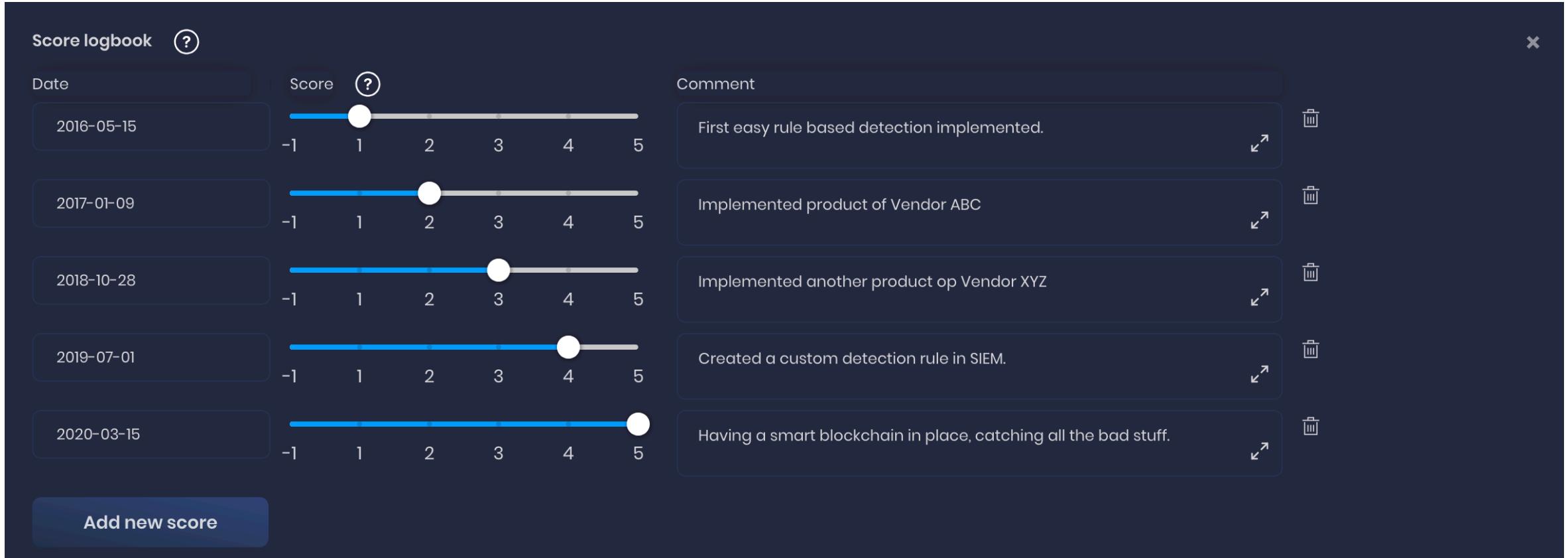
- Detection coverage over time



- Detection coverage over time



# SCORE LOGBOOK



# UPDATING VISIBILITY SCORES

- Update visibility scores (automatically) based on changes in your data sources file
- Update when MITRE released a new ATT&CK version

# UPDATING VISIBILITY SCORES

```
python dettect.py ds -fd ~/Downloads/data-sources-new.yaml -u -ft output/techniques-administration-myexample-windows.yaml
```

Do you want to fill in the visibility comment for the updated scores?

```
>> y(yes) / n(no): y
```

```
>> Visibility comment for in the new 'score' object: Update Q2
```

# UPDATING VISIBILITY SCORES

The following new technique IDs are added to the technique administration file with a visibility score derived from the nr. of data sources:

- T1192
- T1194
- T1195
- T1534

A total of 1 visibility scores are eligible for an update.

For all most recent visibility score objects that are eligible for an update, the key-value pair 'auto-generated' is set to 'true'.

This implies that these scores are auto-generated. How do you want to proceed?:

- 1) Update all visibility scores that have changed.
- 2) Decide per visibility score, that has changed if you want to update or not.  
Both the current and new visibility score will be printed.
- 3) Cancel.

# UPDATING VISIBILITY SCORES

[updates remaining: 1]

Visibility object:

- ATT&CK ID/name T1189 / Credential Dumping
- Applicable to: all
- Technique comment:

OLD score object:

- Date: 2020-05-15
- Score: 0
- Visibility comment:
- Auto generated: True

NEW score object:

- Date: 2020-05-15
- Score: 1
- Visibility comment: Update Q2
- Auto generated: True

Update the score?

>> y(yes) / n(no): yes

# UPDATING VISIBILITY SCORES

```
- Updated a score in technique ID: T1189    (applicable to: all)
```

```
Written backup file:  output/techniques-administration-myexample-windows_backup_3.yaml
```

```
File written:  output/techniques-administration-myexample-windows.yaml
```

# FUTURE PLANS

MAPPING YOUR BLUE TEAM

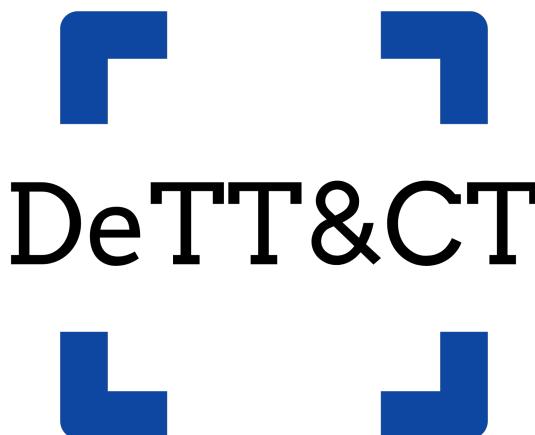
- Support for sub-techniques
  - Including conversion function
- DeTT&CT:
  - Score logbook for data sources
  - Applicable to field for data sources
- DeTT&CT Editor improvements:
  - Better searching
  - Edit YAML comment and exceptions section
  - Better navigation through data sources / techniques
  - Multiple UX improvements

The complete list: <https://github.com/rabobank-cdc/DeTTECT/wiki/Future-dev>

END

**MB SECURE**

Sirius  Security

  
DeTT&CT

[github.com/rabobank-cdc/DeTECT](https://github.com/rabobank-cdc/DeTECT)

Questions?



@Bakk3rM

@RubenB\_2