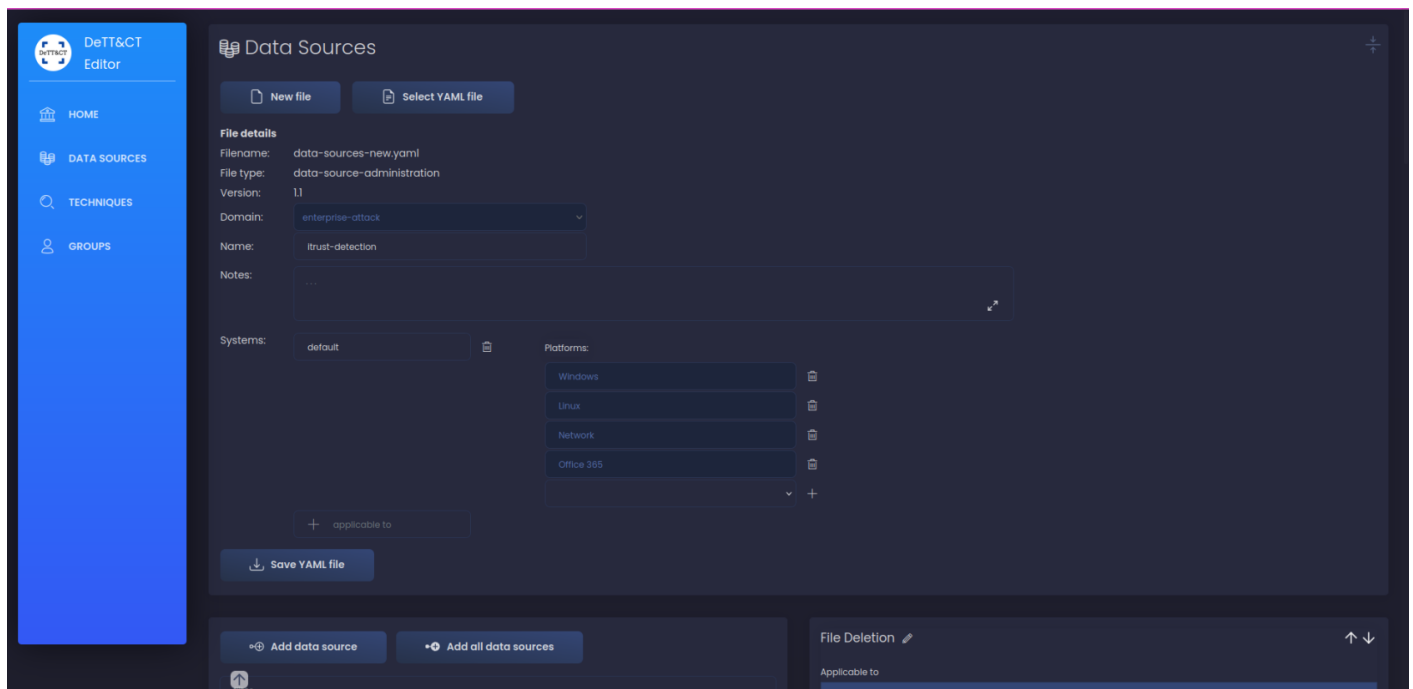


[SOC] Dettect

Introduction

Le projet Dettect a pour objectif d'identifier les TTPs couvertes (et non-couvertes) par vos règles de détection.

Le projet vous aidera à générer un fichier avec vos datasources couvertes et à convertir ce fichier en un fichier importable dans le MITRE Navigator afin d'afficher les TTPs.



DeTT&CT

Voici le lien du projet :

- <https://github.com/rabobank-cdc/DeTTECT>

Lancez le conteneur :

```
docker run -p 8080:8080 -v $(pwd)/output:/opt/DeTTECT/output -v $(pwd)/input:/opt/DeTTECT/input --name  
dettect -it rabobankcdc/dettect:latest /bin/bash
```

Puis lancez le serveur web en écoute :

```
python3 dettect.py e
```

Vous pouvez ouvrir un navigateur web et vous rendre sur <http://localhost:8080> .

- Après avoir créer vos datasources et télécharger votre configuration, déplacez-le dans le dossier input du projet.
- Ensuite ouvrez un shell dans le conteneur :

```
docker exec -it dettect bash
```

Puis convertissez pour obtenir un fichier de configuration importable dans le MITRE Navigator :

```
python3 dettect.py ds -fd input/data-sources-new.yaml -l
```

Et importez dans le MITRE Navigator :

ATT&CKcon 5.0 returns October 22-23, 2024 in McLean, VA. [Register here today!](#) MITRE ATT&CK®

Data sources [trust-detection] x												Selection Controls	Layer Controls	Technique Controls
												🔍 ✕ 🔒 ⋮ ⚙		
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact			
10 techniques	11 techniques	19 techniques	14 techniques	38 techniques	17 techniques	29 techniques	9 techniques	17 techniques	18 techniques	9 techniques	14 techniques			
Content Injection (1.3)	Command and Scripting Interpreter (1.3)	Account Manipulation (1.3)	Abuse Elevation Control Mechanism (1.3)	Abuse Elevation Control Mechanism (1.3)	Adversary-in-the-Middle (1.3)	Account Discovery (1.3)	Exploitation of Remote Services (1.3)	Adversary-in-the-Middle (1.3)	Application Layer Protocol (1.3)	Automated Exfiltration (1.3)	Account Access Removal (1.3)			
Drive-by Compromise (1.3)	AutoHotKey & AutoIT (1.3)	Additional Cloud Roles (1.3)	Bypass User Account Control (1.3)	Bypass User Account Control (1.3)	ARP Cache Poisoning (1.3)	Cloud Account (1.3)	Internal Spearphishing (1.3)	ARP Cache Poisoning (1.3)	DNS (1.3)	Traffic Duplication (1.3)	Data Destruction (1.3)			
Exploit Public-Facing Application (1.3)	Cloud API (1.3)	Additional Email Delegate Permissions (1.3)	Setuid and Setgid (1.3)	Setuid and Setgid (1.3)	DHCP Spoofing (1.3)	Domain Account (1.3)	Lateral Tool Transfer (1.3)	DHCP Spoofing (1.3)	File Transfer Protocols (1.3)	Data Transfer Size Limits (1.3)	Data Encrypted for Impact (1.3)			
External Remote Services (1.3)	JavaScript (1.3)	Device Registration (1.3)	Sudo and Sudo Caching (1.3)	Sudo and Sudo Caching (1.3)	LLMNR/NBT-NS Poisoning and SMB Relay (1.3)	Email Account (1.3)	Remote Service Session Hijacking (1.3)	LLMNR/NBT-NS Poisoning and SMB Relay (1.3)	Mail Protocols (1.3)	Exfiltration Over Alternative Protocol (1.3)	Data Manipulation (1.3)			
Hardware Additions (1.3)	Network Device CLI (1.3)	SSH Authorized Keys (1.3)	Temporary Elevated Cloud Access (1.3)	Temporary Elevated Cloud Access (1.3)	Local Account (1.3)	Local Account (1.3)	RDP Hijacking (1.3)	Archive Collected Data (1.3)	Web Protocols (1.3)	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol (1.3)	Runtime Data Manipulation (1.3)			
Phishing (1.3)	PowerShell (1.3)	BITS Jobs (1.3)	Access Token Manipulation (1.3)	Access Token Manipulation (1.3)	Brute Force (1.3)	Application Window Discovery (1.3)	SSH Hijacking (1.3)	Archive via Custom Method (1.3)	Communication Through Removable Media (1.3)	Exfiltration Over Symmetric Encrypted Non-C2 Protocol (1.3)	Stored Data Manipulation (1.3)			
Spearphishing Attachment (1.3)	Python (1.3)	Boot or Logon Autostart Execution (1.3)	Create Process with Token (1.3)	Create Process with Token (1.3)	Credential Stuffing (1.3)	Browser Information Discovery (1.3)	Remote Services (1.3)	Archive via Library (1.3)	Content Injection (1.3)	Exfiltration Over Encrypted Non-C2 Protocol (1.3)	Transmitted Data Manipulation (1.3)			
Spearphishing Link (1.3)	Unix Shell (1.3)	Active Setup (1.3)	Make and Impersonate Token (1.3)	Make and Impersonate Token (1.3)	Password Cracking (1.3)	Cloud Service Dashboard (1.3)	Cloud Services (1.3)	Archive via Utility (1.3)	Non-Standard Encoding (1.3)	Exfiltration Over Encrypted Non-C2 Protocol (1.3)	Defacement (1.3)			
Spearphishing via Service (1.3)	Visual Basic (1.3)	Authentication Package (1.3)	Parent PID Spoofing (1.3)	Parent PID Spoofing (1.3)	Password Guessing (1.3)	Cloud Service Discovery (1.3)	Distributed Component Object Model (1.3)	Audio Capture (1.3)	Standard Encoding (1.3)	Exfiltration Over Unencrypted Non-C2 Protocol (1.3)	External Defacement (1.3)			
Spearphishing Voice (1.3)	Windows Command Shell (1.3)	Kernel Modules and Extensions (1.3)	Parent PID Spoofing (1.3)	SID-History Injection (1.3)	Password Spraying (1.3)	Debugger Evasion (1.3)	Remote Desktop Protocol (1.3)	Automated Collection (1.3)	Data Obfuscation (1.3)	Exfiltration Over Unencrypted Non-C2 Protocol (1.3)	Internal Defacement (1.3)			
Replication Through Removable Media (1.3)	Exploitation for Client Execution (1.3)	LSASS Driver (1.3)	SID-History Injection (1.3)	SID-History Injection (1.3)	Credentials from Password Stores (1.3)	Device Driver Discovery (1.3)	SMB/Windows Admin Shares (1.3)	Browser Session Hijacking (1.3)	Junk Data (1.3)	Exfiltration Over C2 Channel (1.3)	Disk Wipe (1.3)			
Supply Chain Compromise (1.3)	Inter-Process Communication (1.3)	Port Monitors (1.3)	Token Impersonation/Theft (1.3)	Token Impersonation/Theft (1.3)	Credentials from Web Browsers (1.3)	Device Driver Discovery (1.3)	SSH (1.3)	Clipboard Data (1.3)	Data from Cloud Storage (1.3)	Exfiltration Over Other Network Medium (1.3)	Disk Content Wipe (1.3)			
Compromise Hardware Supply Chain (1.3)	Component Object Model (1.3)	Print Processors (1.3)	Account Manipulation (1.3)	Account Manipulation (1.3)	Password Managers (1.3)	Domain Trust Discovery (1.3)	VNC (1.3)	Data from Configuration Repository (1.3)	Steganography (1.3)	Exfiltration Over Physical Medium (1.3)	Disk Structure Wipe (1.3)			
Compromise Software Supply Chain (1.3)	Dynamic Data Exchange (1.3)	Registry Run Keys / Startup Folder (1.3)	Additional Cloud Roles Permissions (1.3)	Direct Volume Access (1.3)	Securityd Memory (1.3)	File and Directory Discovery (1.3)	Windows Remote Management (1.3)	Data from Information Repositories (1.3)	Dynamic Resolution (1.3)	Exfiltration Over USB (1.3)	Endpoint Denial of Service (1.3)			
Compromise Software Dependencies and Development Tools (1.3)	Native API (1.3)	Shortcut Modification (1.3)	Device Registration (1.3)	Domain or Tenant Policy Modification (1.3)	Windows Credential Manager (1.3)	Group Policy Discovery (1.3)	Replication Through Removable Media (1.3)	SNMP (MIB Dump) (1.3)	DNS Calculation (1.3)	Exfiltration Over Web Service (1.3)	Application or System Exhaustion Flood (1.3)			
Compromise Software Supply Chain (1.3)	Scheduled Task/Job (1.3)	Time Providers (1.3)	SSH Authorized Keys (1.3)	Trust Modification (1.3)	Exploitation for Credential Access (1.3)	Log Enumeration (1.3)	Software Deployment Tools (1.3)	Sharepoint (1.3)	Domain Generation Algorithms (1.3)	Exfiltration Over Webhook (1.3)	OS Exhaustion Flood (1.3)			
Trusted Relationship (1.3)	At (1.3)	Winlogon Helper DLL (1.3)	Boot or Logon Autostart Execution (1.3)	Execution Guardrails (1.3)	Forced Authentication (1.3)	Network Service Discovery (1.3)	Taint Shared Content (1.3)		Fast Flux DNS (1.3)		Service Exhaustion Flood (1.3)			
Valid Accounts (1.3)	Cron (1.3)	XDG Autostart Entries (1.3)	Active Setup (1.3)	Environmental Keying (1.3)	Forge Web Credentials (1.3)	Network Share Discovery (1.3)	Use Alternate Authentication Material (1.3)		Encrypted Channel (1.3)					
Cloud Accounts (1.3)	Scheduled Task (1.3)	Boot or Logon Initialization Scripts (1.3)	Authentication Package (1.3)	Exploitation for Defense Evasion (1.3)	SAML Tokens (1.3)	Network Sniffing (1.3)	Application Access Token (1.3)		Asymmetric Cryptography (1.3)					
Default Accounts (1.3)	Systemd Timers (1.3)	Logon Script (Windows) (1.3)	Kernel Modules and Extensions (1.3)	File and Directory Permissions Modification (1.3)	Web Cookies (1.3)	Password Policy Discovery (1.3)			Symmetric Cryptography (1.3)					
	Serverless Execution (1.3)	Network Logon Script (1.3)	LSASS Driver (1.3)	Linux and Mac File and Directory Hooking (1.3)	Input Capture (1.3)	Peripheral Device Discovery (1.3)								

Legend

Revision #1

Created 21 October 2024 15:49:04 by Elieroc

Updated 21 October 2024 15:58:00 by Elieroc