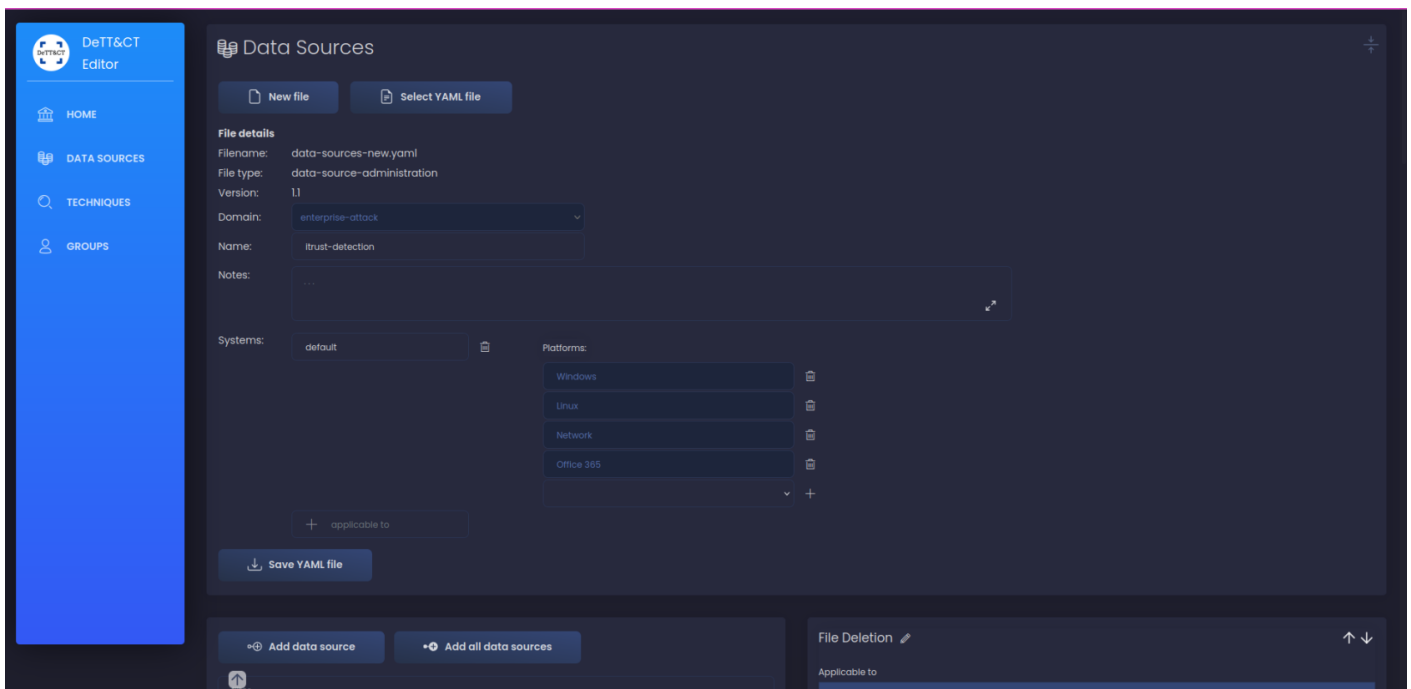


[SOC] Dettect

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 iftrust-detection																							
												Selection Controls		Layer Controls		Technique Controls							
														Search		Close		Lock		More		Help	
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 Drive-by Compromise Exploit Public-Facing Application External Remote Services Hardware Additions Phishing Spearphishing Attachment Spearphishing Link Spearphishing via Service Spearphishing Voice Replication Through Removable Media Supply Chain Compromise (3/3) Compromise Hardware Supply Chain Compromise Software Dependencies and Development Tools Compromise Software Supply Chain Trusted Relationship Valid Accounts (4/4) Cloud Accounts Default Accounts	Command and Scripting Interpreter AutoHotKey & AutoIT Cloud API JavaScript Network Device CLI PowerShell Python Unix Shell Visual Basic Windows Command Shell Exploitation for Client Execution Inter-Process Communication (2/2) Component Object Model Dynamic Data Exchange Native API Scheduled Task/Job At Cron Scheduled Task Systemd Timers Serverless Execution	Account Manipulation Additional Cloud Roles Additional Email Delegate Permissions Device Registration SSH Authorized Keys BITS Jobs Boot or Logon Autostart Execution Active Setup Authentication Package Kernel Modules and Extensions LSASS Driver Port Monitors Print Processors Registry Run Keys / Startup Folder Security Support Provider Shortcut Modification Time Providers Winlogon Helper DLL XDG Autostart Entries Boot or Logon Initialization Scripts Logon Script (Windows) Network Logon Script RC Scripts	Abuse Elevation Control Mechanism Bypass User Account Control Setuid and Setgid Sudo and Sudo Caching Temporary Elevated Cloud Access Access Token Manipulation Create Process with Token Make and Impersonate Token Parent PID Spoofing SID-History Injection Token Impersonation/Theft Token Impersonation/Theft BITS Jobs Debugger Evasion Deobfuscate/Decode Files or Information Direct Volume Access Domain or Tenant Policy Modification Group Policy Modification Trust Modification Execution Guardrails (1/1) Environmental Keying Exploitation for Defense Evasion File and Directory Permissions Modification Linux and Mac File and Directory	Abuse Elevation Control Mechanism Bypass User Account Control Setuid and Setgid Sudo and Sudo Caching Temporary Elevated Cloud Access Access Token Manipulation Create Process with Token Make and Impersonate Token Parent PID Spoofing SID-History Injection Token Impersonation/Theft BITS Jobs Debugger Evasion Deobfuscate/Decode Files or Information Direct Volume Access Domain or Tenant Policy Modification Group Policy Modification Trust Modification Execution Guardrails (1/1) Environmental Keying Exploitation for Defense Evasion File and Directory Permissions Modification Linux and Mac File and Directory	Adversary-in-the-Middle (2/3) ARP Cache Poisoning DHCP Spoofing LLMNR/NBT-NS Poisoning and SMB Relay Brute Force (1/1) Credential Stuffing Password Cracking Password Guessing Password Spraying Credentials from Password Stores Credentials from Web Browsers Password Managers SecurityId Memory Windows Credential Manager Exploitation for Credential Access Forced Authentication Forge Web Credentials (2/2) SAML Tokens Web Cookies Input Capture (4/4) Credential API Hooking	Account Discovery (1/1) Cloud Account Domain Account Email Account Local Account Application Window Discovery Browser Information Discovery Cloud Service Dashboard Cloud Service Discovery Debugger Evasion Device Driver Discovery Domain Trust Discovery File and Directory Discovery Group Policy Discovery Log Enumeration Network Service Discovery Network Share Discovery Network Sniffing Password Policy Discovery Peripheral Device Discovery Application Access Token	Exploitation of Remote Services Internal Spearphishing Lateral Tool Transfer Remote Service Session Hijacking RDP Hijacking SSH Hijacking Remote Services Cloud Services Distributed Component Object Model Remote Desktop Protocol SMB/Windows Admin Shares SSH VNC Windows Remote Management Replication Through Removable Media Software Deployment Tools Taint Shared Content Use Alternate Authentication Material (4/4) Sharepoint Data from Local	Adversary-in-the-Middle (2/3) ARP Cache Poisoning DHCP Spoofing LLMNR/NBT-NS Poisoning and SMB Relay Archive Collected Data (1/1) Archive via Custom Method Archive via Library Archive via Utility Audio Capture Automated Collection Browser Session Hijacking Clipboard Data Data from Cloud Storage Data from Configuration Repository (2/2) Network Device Configuration Dump SNMP (MIB Dump) Data from Information Repositories (1/1) Sharepoint Data from Local	Application Layer Protocol (4/4) DNS File Transfer Protocols Mail Protocols Web Protocols Communication Through Removable Media Content Injection Non-Standard Encoding Data Obfuscation (2/2) Junk Data Protocol Impersonation Steganography Dynamic Resolution (1/3) DNS Calculation Domain Generation Algorithms Fast Flux DNS Encrypted Channel (2/2) Asymmetric Cryptography Symmetric Cryptography	Automated Exfiltration (1/1) Traffic Duplication Data Transfer Size Limits Exfiltration Over Alternative Protocol Exfiltration Over Asymmetric Encrypted Non-C2 Protocol Exfiltration Over Symmetric Encrypted Non-C2 Protocol Exfiltration Over Encrypted Non-C2 Protocol Exfiltration Over C2 Channel Exfiltration Over Other Network Medium Exfiltration Over Physical Medium Exfiltration over USB Exfiltration over Web Service (4/4) Exfiltration Over Webhook	Account Access Removal Data Destruction Data Encrypted for Impact Data Manipulation Runtime Data Manipulation Stored Data Manipulation Transmitted Data Manipulation Defacement External Defacement Internal Defacement Disk Wipe (1/1) Disk Content Wipe Disk Structure Wipe Endpoint Denial of Service (4/4) Application or System Exhaustion Flood OS Exhaustion Flood Service Exhaustion Flood												

Revision #1

Created 21 October 2024 15:49:04 by Elieroc

Updated 21 October 2024 15:58:00 by Elieroc