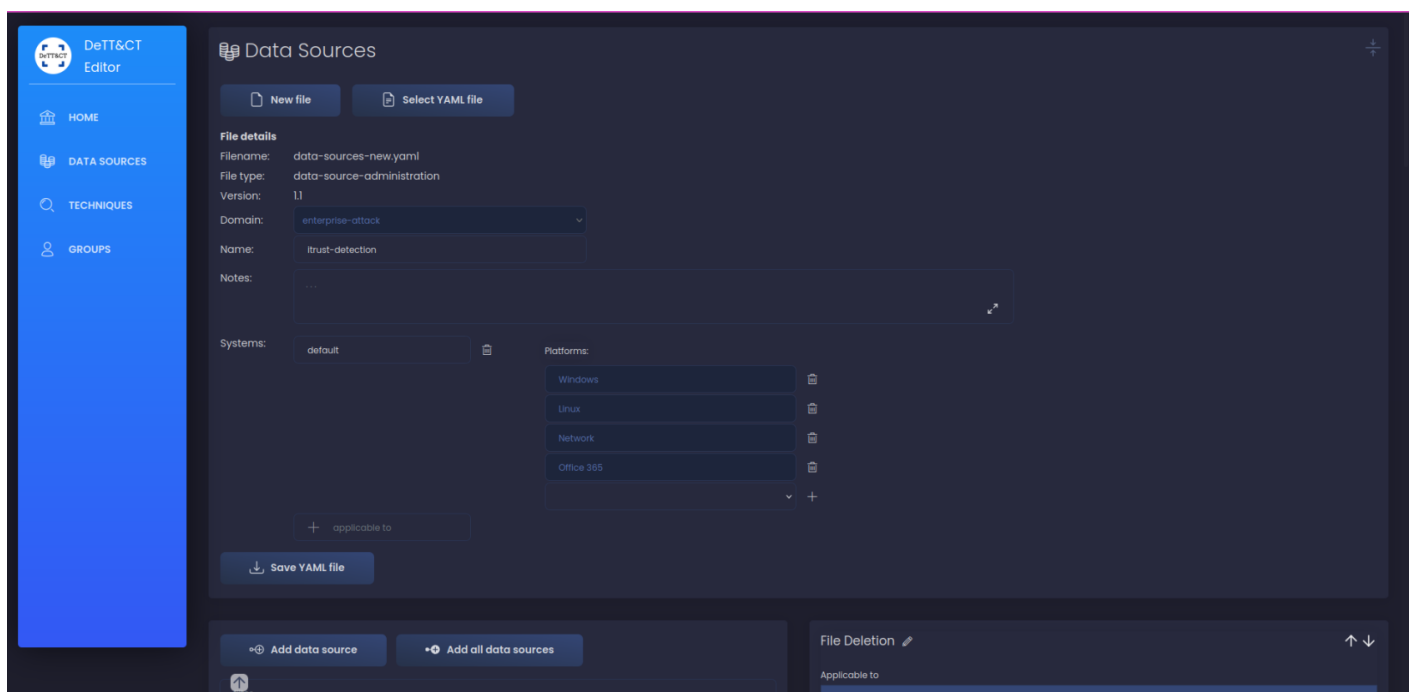


[SOC] Dettect

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 ifrust-detection

Selection Controls

Layer Controls

Technique Controls

Q

X

⌵

⋮

⌵

Initial Access 10 techniques	Execution 11 techniques	Persistence 19 techniques	Privilege Escalation 14 techniques	Defense Evasion 38 techniques	Credential Access 17 techniques	Discovery 29 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 14 techniques
<div>Content Injection</div> <div>Drive-by Compromise</div> <div>Exploit Public-Facing Application</div> <div>External Remote Services</div> <div>Hardware Additions</div> <div>Phishing</div> <div>Spearphishing Attachment</div> <div>Spearphishing Link</div> <div>Spearphishing via Service</div> <div>Spearphishing Voice</div> <div>Replication Through Removable Media</div> <div>Supply Chain Compromise (3/3)</div> <div>Compromise Hardware Supply Chain</div> <div>Compromise Software Dependencies and Development Tools</div> <div>Compromise Software Supply Chain</div> <div>Trusted Relationship</div> <div>Valid Accounts (4/4)</div> <div>Cloud Accounts</div> <div>Default Accounts</div>	<div>Command and Scripting Interpreter</div> <div>AutoHotKey & AutoIt</div> <div>Cloud API</div> <div>JavaScript</div> <div>Network Device CLI</div> <div>PowerShell</div> <div>Python</div> <div>Unix Shell</div> <div>Visual Basic</div> <div>Windows Command Shell</div> <div>Exploitation for Client Execution</div> <div>Inter-Process Communication (2/2)</div> <div>Component Object Model</div> <div>Dynamic Data Exchange</div> <div>Native API</div> <div>Scheduled Task/Job</div> <div>At</div> <div>Cron</div> <div>Scheduled Task</div> <div>Systemd Timers</div> <div>Serverless Execution</div>	<div>Account Manipulation</div> <div>Additional Cloud Roles</div> <div>Additional Email Delegate Permissions</div> <div>Device Registration</div> <div>SSH Authorized Keys</div> <div>BITS Jobs</div> <div>Boot or Logon Autostart Execution</div> <div>Active Setup</div> <div>Authentication Package</div> <div>Kernel Modules and Extensions</div> <div>LSASS Driver</div> <div>Port Monitors</div> <div>Print Processors</div> <div>Registry Run Keys / Startup Folder</div> <div>Security Support Provider</div> <div>Shortcut Modification</div> <div>Time Providers</div> <div>Winlogon Helper DLL</div> <div>XDG Autostart Entries</div> <div>Boot or Logon Initialization Scripts (3/3)</div> <div>Logon Script (Windows)</div> <div>Network Logon Script</div> <div>RC Scripts</div>	<div>Abuse Elevation Control Mechanism</div> <div>Bypass User Account Control</div> <div>Setuid and Setgid</div> <div>Sudo and Sudo Caching</div> <div>Temporary Elevated Cloud Access</div> <div>Access Token Manipulation</div> <div>Create Process with Token</div> <div>Make and Impersonate Token</div> <div>Parent PID Spoofing</div> <div>SID-History Injection</div> <div>Token Impersonation/Theft</div> <div>BITS Jobs</div> <div>Debugger Evasion</div> <div>Deobfuscate/Decode Files or Information</div> <div>Direct Volume Access</div> <div>Domain or Tenant Policy Modification</div> <div>Group Policy Modification</div> <div>Trust Modification</div> <div>Execution Guardrails (1/1)</div> <div>Environmental Keying</div> <div>Exploitation for Defense Evasion</div> <div>File and Directory Permissions Modification</div> <div>Linux and Mac File and Directory</div>	<div>Abuse Elevation Control Mechanism</div> <div>Bypass User Account Control</div> <div>Setuid and Setgid</div> <div>Sudo and Sudo Caching</div> <div>Temporary Elevated Cloud Access</div> <div>Access Token Manipulation</div> <div>Create Process with Token</div> <div>Make and Impersonate Token</div> <div>Parent PID Spoofing</div> <div>SID-History Injection</div> <div>Token Impersonation/Theft</div> <div>BITS Jobs</div> <div>Debugger Evasion</div> <div>Deobfuscate/Decode Files or Information</div> <div>Direct Volume Access</div> <div>Domain or Tenant Policy Modification</div> <div>Group Policy Modification</div> <div>Trust Modification</div> <div>Execution Guardrails (1/1)</div> <div>Environmental Keying</div> <div>Exploitation for Defense Evasion</div> <div>File and Directory Permissions Modification</div> <div>Linux and Mac File and Directory</div>	<div>Adversary-in-the-Middle (2/3)</div> <div>ARP Cache Poisoning</div> <div>DHCP Spoofing</div> <div>LLMNR/NBT-NS Poisoning and SMB Relay</div> <div>Brute Force (1/1)</div> <div>Credential Stuffing</div> <div>Password Cracking</div> <div>Password Guessing</div> <div>Password Spraying</div> <div>Credentials from Password Stores</div> <div>Credentials from Web Browsers</div> <div>Password Managers</div> <div>SecurityId Memory</div> <div>Windows Credential Manager</div> <div>Exploitation for Credential Access</div> <div>Forced Authentication</div> <div>Forge Web Credentials (2/2)</div> <div>SAML Tokens</div> <div>Web Cookies</div> <div>Input Capture (4/4)</div> <div>Credential API Hooking</div>	<div>Account Discovery (1/1)</div> <div>Cloud Account</div> <div>Domain Account</div> <div>Email Account</div> <div>Local Account</div> <div>Application Window Discovery</div> <div>Browser Information Discovery</div> <div>Cloud Service Dashboard</div> <div>Cloud Service Discovery</div> <div>Debugger Evasion</div> <div>Device Driver Discovery</div> <div>Domain Trust Discovery</div> <div>File and Directory Discovery</div> <div>Group Policy Discovery</div> <div>Log Enumeration</div> <div>Network Service Discovery</div> <div>Network Share Discovery</div> <div>Network Sniffing</div> <div>Password Policy Discovery</div> <div>Peripheral Device Discovery</div> <div>Application Access</div>	<div>Exploitation of Remote Services</div> <div>Internal Spearphishing</div> <div>Lateral Tool Transfer</div> <div>Remote Service Session Hijacking</div> <div>RDP Hijacking</div> <div>SSH Hijacking</div> <div>Remote Services</div> <div>Cloud Services</div> <div>Distributed Component Object Model</div> <div>Remote Desktop Protocol</div> <div>SMB/Windows Admin Shares</div> <div>SSH</div> <div>VNC</div> <div>Windows Remote Management</div> <div>Replication Through Removable Media</div> <div>Software Deployment Tools</div> <div>Taint Shared Content</div> <div>Use Alternate Authentication Material (4/4)</div> <div>Sharepoint</div> <div>Application Access</div>	<div>Adversary-in-the-Middle (3/3)</div> <div>ARP Cache Poisoning</div> <div>DHCP Spoofing</div> <div>LLMNR/NBT-NS Poisoning and SMB Relay</div> <div>Archive Collected Data (3/3)</div> <div>Archive via Custom Method</div> <div>Archive via Library</div> <div>Archive via Utility</div> <div>Audio Capture</div> <div>Automated Collection</div> <div>Browser Session Hijacking</div> <div>Clipboard Data</div> <div>Data from Cloud Storage</div> <div>Data from Configuration Repository (2/2)</div> <div>Network Device Configuration Dump</div> <div>SNMP (MIB Dump)</div> <div>Data from Information Repositories (1/1)</div> <div>Sharepoint</div> <div>Data from Local</div>	<div>Application Layer Protocol (4/4)</div> <div>DNS</div> <div>File Transfer Protocols</div> <div>Mail Protocols</div> <div>Web Protocols</div> <div>Communication Through Removable Media</div> <div>Content Injection</div> <div>Non-Standard Encoding</div> <div>Data Obfuscation (3/3)</div> <div>Protocol Impersonation</div> <div>Steganography</div> <div>Dynamic Resolution (3/3)</div> <div>DNS Calculation</div> <div>Domain Generation Algorithms</div> <div>Fast Flux DNS</div> <div>Encrypted Channel (2/2)</div> <div>Asymmetric Cryptography</div> <div>Symmetric Cryptography</div>	<div>Automated Exfiltration</div> <div>Traffic Duplication</div> <div>Data Transfer Size Limits</div> <div>Exfiltration Over Alternative Protocol</div> <div>Exfiltration Over Asymmetric Encrypted Non-C2 Protocol</div> <div>Exfiltration Over Symmetric Encrypted Non-C2 Protocol</div> <div>Exfiltration Over Encrypted Non-C2 Protocol</div> <div>Exfiltration Over C2 Channel</div> <div>Exfiltration Over Other Network Medium</div> <div>Exfiltration Over Physical Medium</div> <div>Exfiltration over USB</div> <div>Exfiltration Over Web Service (4/4)</div> <div>Exfiltration Over Webhook</div>	<div>Account Access Removal</div> <div>Data Destruction</div> <div>Data Encrypted for Impact</div> <div>Data Manipulation</div> <div>Runtime Data Manipulation</div> <div>Stored Data Manipulation</div> <div>Transmitted Data Manipulation</div> <div>Defacement</div> <div>External Defacement</div> <div>Internal Defacement</div> <div>Disk Wipe (1/1)</div> <div>Disk Content Wipe</div> <div>Disk Structure Wipe</div> <div>Endpoint Denial of Service (4/4)</div> <div>Application or System Exhaustion Flood</div> <div>OS Exhaustion Flood</div> <div>Service Exhaustion Flood</div>

⬆️⬇️

Revision #1

Created 21 October 2024 15:49:04 by Elieroc

Updated 21 October 2024 15:58:00 by Elieroc