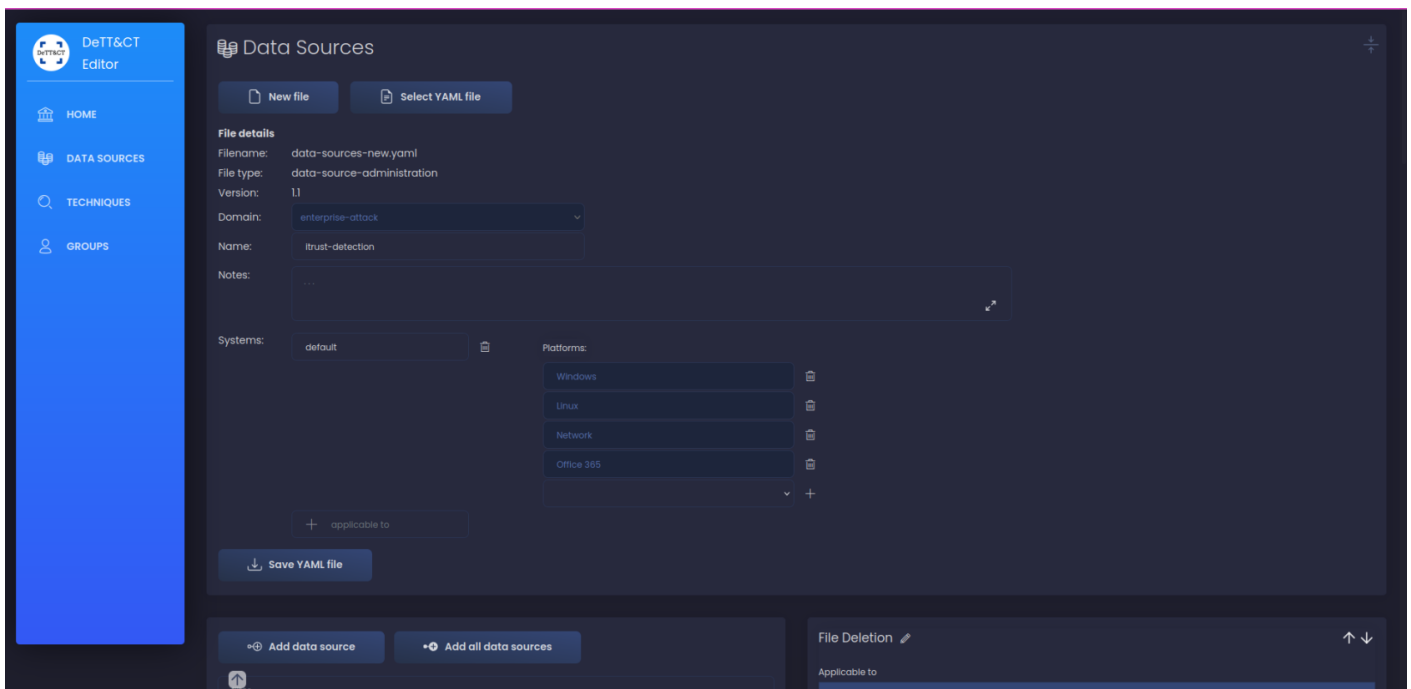


[SOC] Dettect

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
```

```
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 :

| Data sources <b>itrust-detection</b> +                 |                                   |                                       |                                       |                                       |                                             |                               |                                            |                                      |                                       |                                                        | Selection Controls                  |  | Layer Controls |  | Technique Controls |  | MITRE ATTACK® |  |   |  |
|--------------------------------------------------------|-----------------------------------|---------------------------------------|---------------------------------------|---------------------------------------|---------------------------------------------|-------------------------------|--------------------------------------------|--------------------------------------|---------------------------------------|--------------------------------------------------------|-------------------------------------|--|----------------|--|--------------------|--|---------------|--|---|--|
|                                                        |                                   |                                       |                                       |                                       |                                             |                               |                                            |                                      |                                       |                                                        | 🔍                                   |  | ✕              |  | 🔒                  |  | ⋮             |  | 🔧 |  |
| Initial Access<br>10 techniques                        | Execution<br>11 techniques        | Persistence<br>19 techniques          | Privilege Escalation<br>14 techniques | Defense Evasion<br>38 techniques      | Credential Access<br>17 techniques          | Discovery<br>29 techniques    | Lateral Movement<br>9 techniques           | Collection<br>17 techniques          | Command and Control<br>18 techniques  | Exfiltration<br>9 techniques                           | Impact<br>14 techniques             |  |                |  |                    |  |               |  |   |  |
| Content Injection                                      | Command and Scripting Interpreter | Account Manipulation Mechanisms       | Abuse Elevation Control Mechanisms    | Abuse Elevation Control Mechanisms    | Adversary-in-the-Middle (a1)                | Account Discovery (a6)        | Exploitation of Remote Services            | Adversary-in-the-Middle (a1)         | Application Layer Protocol (a4)       | Automated Exfiltration                                 | Account Access Removal              |  |                |  |                    |  |               |  |   |  |
| Driven by Compromise                                   |                                   | Additional Cloud Roles                |                                       |                                       |                                             |                               |                                            |                                      |                                       |                                                        |                                     |  |                |  |                    |  |               |  |   |  |
| Exploit Public-Facing Application                      | AutoHotKey & AutoIt               | Additional Email Delegate Permissions | Bypass User Account Control           | Bypass User Account Control           | ARP Cache Poisoning                         | Cloud Account                 | Internal Spearphishing                     | ARP Cache Poisoning                  | DNS                                   | Traffic Duplication                                    | Data Destruction                    |  |                |  |                    |  |               |  |   |  |
| External Remote Services                               | Cloud API                         | Device Registration                   | Setuid and Setgid                     | Setuid and Setgid                     | DHCP Spoofing                               | Domain Account                | Lateral Tool Transfer                      | DHCP Spoofing                        | File Transfer Protocols               | Data Transfer Size Limits                              | Data Encrypted for Impact           |  |                |  |                    |  |               |  |   |  |
| Hardware Additions                                     | JavaScript                        | SSH Authorized Keys                   | Sudo and Sudo Caching                 | Sudo and Sudo Caching                 | LLMNR/NBT-NS Poisoning and SMB Relay        | Email Account                 | Remote Service Session Hijacking           | LLMNR/NBT-NS Poisoning and SMB Relay | Mail Protocols                        | Exfiltration Over Alternative Protocol                 | Data Manipulation (a1)              |  |                |  |                    |  |               |  |   |  |
| Network Device CLI                                     |                                   |                                       | Temporary Elevated Cloud Access       | Temporary Elevated Cloud Access       |                                             | Local Account                 |                                            |                                      | Web Protocols                         |                                                        |                                     |  |                |  |                    |  |               |  |   |  |
| Phishing                                               | PowerShell                        | BITS Jobs                             | Access Token Manipulation             | Access Token Manipulation             | Brute Force (a2)                            | Application Window Discovery  | RDP Hijacking                              | Archive Collected Data               | Communication Through Removable Media | Exfiltration Over Asymmetric Encrypted Non-C2 Protocol | Runtime Data Manipulation           |  |                |  |                    |  |               |  |   |  |
| Spearphishing Attachment                               | Python                            | Boot or Logon Autostart Execution     | Create Process with Token             | Create Process with Token             | Credential Stuffing                         | Browser Information Discovery | SSH Hijacking                              | Archive via Custom Method            | Content Injection                     | Exfiltration Over Symmetric Encrypted Non-C2 Protocol  | Stored Data Manipulation            |  |                |  |                    |  |               |  |   |  |
| Spearphishing Link                                     | Unix Shell                        | Active Setup                          | Make and Impersonate Token            | Make and Impersonate Token            | Password Cracking                           | Cloud Service Dashboard       | Remote Services                            | Archive via Library                  | Data Encoding (a2)                    | Exfiltration Over Symmetric Encrypted Non-C2 Protocol  | Transmitted Data Manipulation       |  |                |  |                    |  |               |  |   |  |
| Spearphishing via Service                              | Visual Basic                      | Authentication Package                | Parent PID Spoofing                   | Parent PID Spoofing                   | Password Guessing                           | Cloud Service                 | Cloud Services                             | Audio Capture                        | Non-Standard Encoding                 | Exfiltration Over C2 Channel                           | Disk Wipe                           |  |                |  |                    |  |               |  |   |  |
| Spearphishing Voice                                    | Windows Command Shell             | Kernel Modules and Extensions         | SID-History Injection                 | SID-History Injection                 | Password Spraying                           | Debugger Evasion              | Distributed Component Object Model         | Automated Collection                 | Standard Encoding                     | Exfiltration Over C2 Channel                           | Disk Content Wipe                   |  |                |  |                    |  |               |  |   |  |
| Replication Through Removable Media                    | Evolution for Client Execution    | LSASS Driver                          | TOKEN Impersonation/Theft             | TOKEN Impersonation/Theft             | Windows Credential Manager                  | File and Directory Discovery  | Remote Desktop Protocol                    | Clipboard Data                       | Data Obfuscation (a3)                 | Exfiltration Over C2 Channel                           | Disk Structure Wipe                 |  |                |  |                    |  |               |  |   |  |
| Supply Chain Compromise (a1)                           | Inter-Process Communication (a2)  | Port Monitors                         | Account Manipulation                  | Account Manipulation                  | Credentials from Web Browsers               | Device Drive Discovery        | SMB/Windows Admin Shares                   | Browser Session Hijacking            | Junk Data                             | Exfiltration Over C2 Channel                           | Endpoint Mitigation of Service (a4) |  |                |  |                    |  |               |  |   |  |
| Compromise Hardware Supply Chain                       | Component Object Model            | Print Processors                      | Additional Cloud Roles                | Additional Cloud Roles                | Security Memory                             | Log Enumeration               | SSH                                        | Dynamic Resolution (a3)              | Protocol Impersonation                | Exfiltration Over C2 Channel                           | Application or System Exploitation  |  |                |  |                    |  |               |  |   |  |
| Compromise Software Dependencies and Development Tools | Dynamic Data Exchange             | Registry Run Keys / Startup Folder    | Additional Email Delegate Permissions | Additional Email Delegate Permissions | Windows Credential Manager                  | Group Policy Discovery        | VNC                                        | Steganography                        | Steganography                         | Exfiltration Over C2 Channel                           | OS Exhaustion Flood                 |  |                |  |                    |  |               |  |   |  |
| Compromise Software Dependencies and Development Tools | Native API                        | Security Support Provider             | SSH Authorized Keys                   | SSH Authorized Keys                   | Direct Volume Access                        | Network Service Discovery     | Windows Remote Management                  | Dynamic Resolution (a3)              | Steganography                         | Exfiltration Over C2 Channel                           | Service Exhaustion Flood            |  |                |  |                    |  |               |  |   |  |
| Compromise Software Dependencies and Development Tools | Scheduled Task/Job                | Shortcut Modification                 | Boot or Logon Autostart Execution     | Boot or Logon Autostart Execution     | Domain or Tenant Policy Modification        | Network Share Discovery       | Replication Through Removable Media        | Exfiltration Over C2 Channel         | Steganography                         | Exfiltration Over C2 Channel                           | Service Exhaustion Flood            |  |                |  |                    |  |               |  |   |  |
| Compromise Software Dependencies and Development Tools | At                                | XDG Autostart Entries                 | Active Setup                          | Active Setup                          | Group Policy Modification                   | Network Sniffing              | Software Deployment Tools                  | Exfiltration Over C2 Channel         | Steganography                         | Exfiltration Over C2 Channel                           | Service Exhaustion Flood            |  |                |  |                    |  |               |  |   |  |
| Trusted Relationship                                   | Cron                              | Boot or Logon Initialization Scripts  | Authentication Package                | Authentication Package                | Trust Modification                          | Peripheral Device Discovery   | Taint Shared Content                       | Exfiltration Over C2 Channel         | Steganography                         | Exfiltration Over C2 Channel                           | Service Exhaustion Flood            |  |                |  |                    |  |               |  |   |  |
| Valid Accounts (a4)                                    | Scheduled Task                    | Logon Script (Windows)                | Kernel Modules and Extensions         | Kernel Modules and Extensions         | Execution Guardrails (a4)                   | Web Cookies                   | Use Alternate Authentication Material (a4) | Exfiltration Over C2 Channel         | Steganography                         | Exfiltration Over C2 Channel                           | Service Exhaustion Flood            |  |                |  |                    |  |               |  |   |  |
| Cloud Accounts                                         | System Timers                     | Network Logon Script                  | Network Logon Script                  | Network Logon Script                  | Environmental Keying                        | Input Capture (a4)            | Application Access Token                   | Exfiltration Over C2 Channel         | Steganography                         | Exfiltration Over C2 Channel                           | Service Exhaustion Flood            |  |                |  |                    |  |               |  |   |  |
| Default Accounts                                       | Serverless Execution              | RC Scripts                            | LSASS Driver                          | LSASS Driver                          | Exploitation for Defense Evasion            | Credential API Hooking        | Data from Local                            | Exfiltration Over C2 Channel         | Steganography                         | Exfiltration Over C2 Channel                           | Service Exhaustion Flood            |  |                |  |                    |  |               |  |   |  |
|                                                        |                                   |                                       |                                       |                                       | File and Directory Permissions Modification |                               |                                            | Exfiltration Over C2 Channel         | Steganography                         | Exfiltration Over C2 Channel                           | Service Exhaustion Flood            |  |                |  |                    |  |               |  |   |  |
|                                                        |                                   |                                       |                                       |                                       | Linux and Mac File and Directory            |                               |                                            | Exfiltration Over C2 Channel         | Steganography                         | Exfiltration Over C2 Channel                           | Service Exhaustion Flood            |  |                |  |                    |  |               |  |   |  |

Revision #1

Created 21 October 2024 15:49:04 by Elieroc

Updated 21 October 2024 15:58:00 by Elieroc