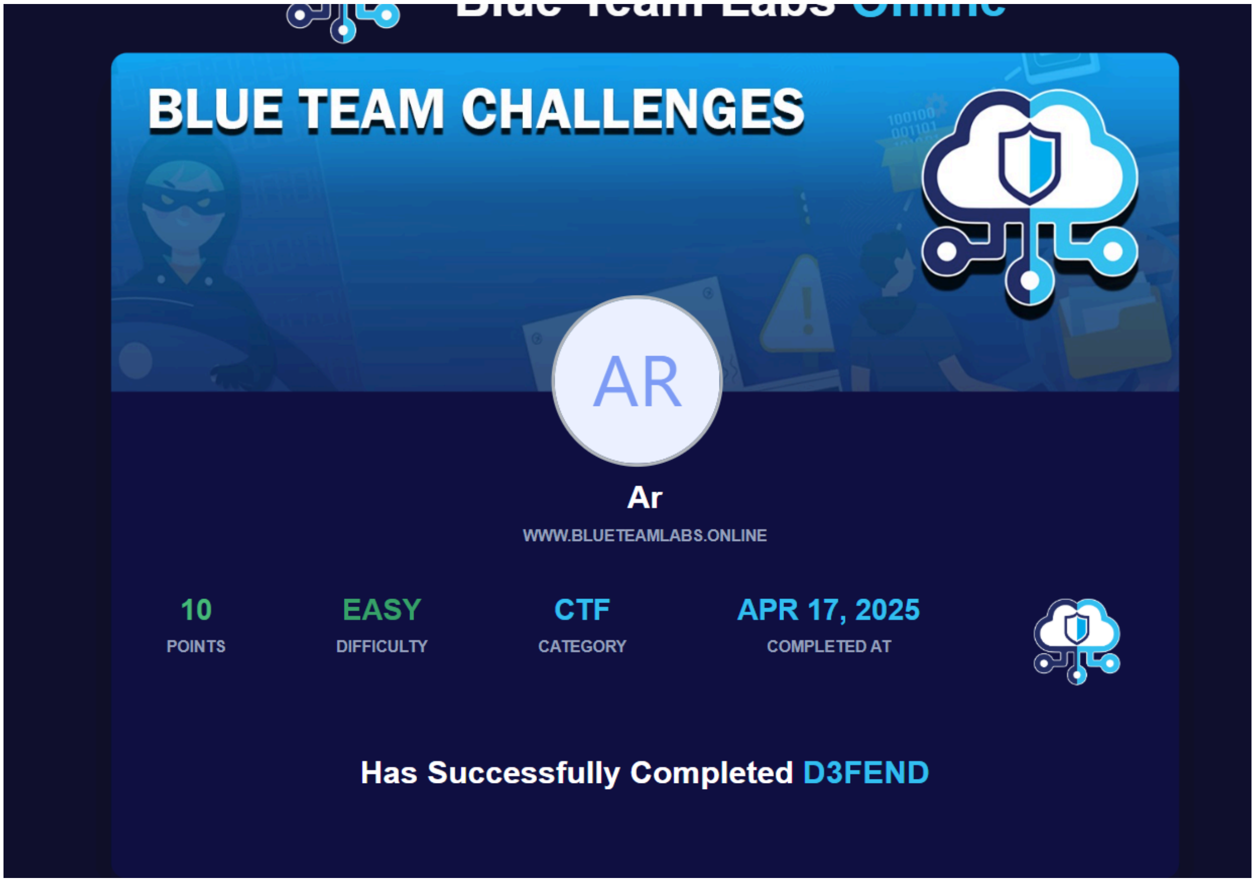
BTLO Challenge Documentation

Investigation Title: D3FEND Investigation

Summary:

This investigation focuses on understanding the defensive cybersecurity techniques cataloged in the MITRE D3FEND framework. The challenge required exploring various IDs, concepts, and associated tools that relate to defensive strategies against offensive cyber threats

Introduction



Blue Team Labs Online

BLUE TEAM CHALLENGES

AR

Ar

WWW.BLUETEAMLABS.ONLINE

10	EASY	CTF	APR 17, 2025
POINTS	DIFFICULTY	CATEGORY	COMPLETED AT

Has Successfully Completed D3FEND

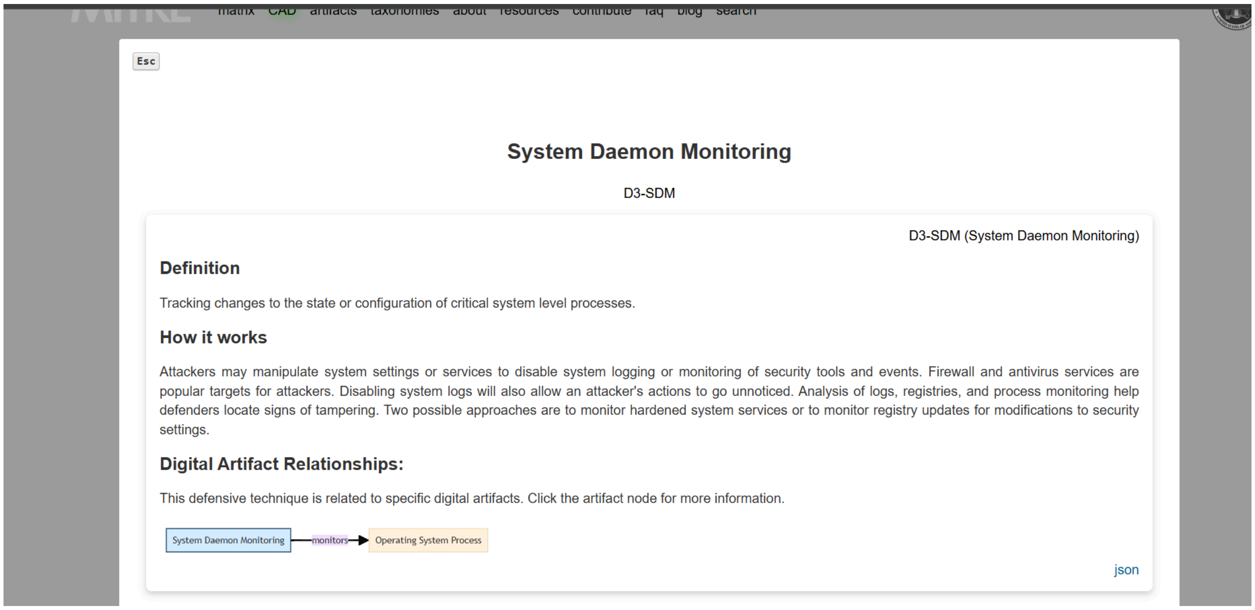
Questions and Answers:

1️⃣Question:

What is the corresponding name for the ID ‘D3-SDM’?

Answer: System Daemon Monitoring

Source: SystemDaemonMonitoring – MITRE D3FEND


matrix CAD artifacts taxonomies about resources contribute faq blog search
Esc

System Daemon Monitoring

D3-SDM

D3-SDM (System Daemon Monitoring)

Definition

Tracking changes to the state or configuration of critical system level processes.

How it works

Attackers may manipulate system settings or services to disable system logging or monitoring of security tools and events. Firewall and antivirus services are popular targets for attackers. Disabling system logs will also allow an attacker's actions to go unnoticed. Analysis of logs, registries, and process monitoring help defenders locate signs of tampering. Two possible approaches are to monitor hardened system services or to monitor registry updates for modifications to security settings.

Digital Artifact Relationships:

This defensive technique is related to specific digital artifacts. Click the artifact node for more information.

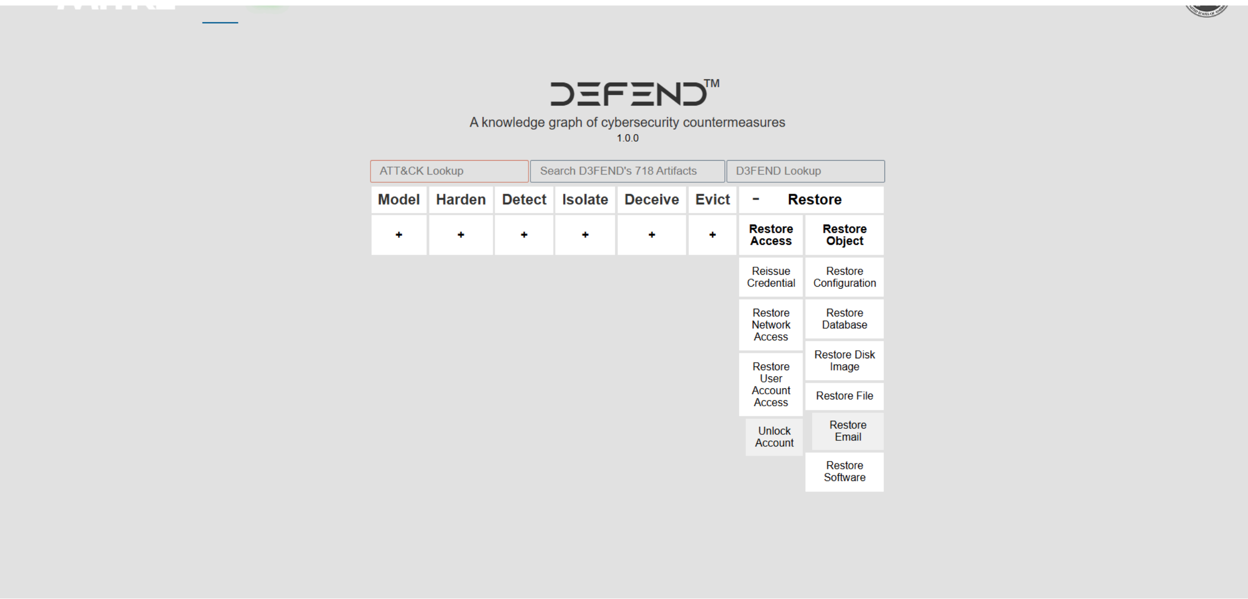
2️⃣Question:

What are the five general tactics used to classify each defensive method? (In the order they appear)

Answer:

- Deceive
- Detect
- Evict
- Harden
- Isolate

- **Source:** D3FEND Framework Homepage



D3FEND™

A knowledge graph of cybersecurity countermeasures

1.0.0

ATT&CK Lookup	Search D3FEND's 718 Artifacts	D3FEND Lookup

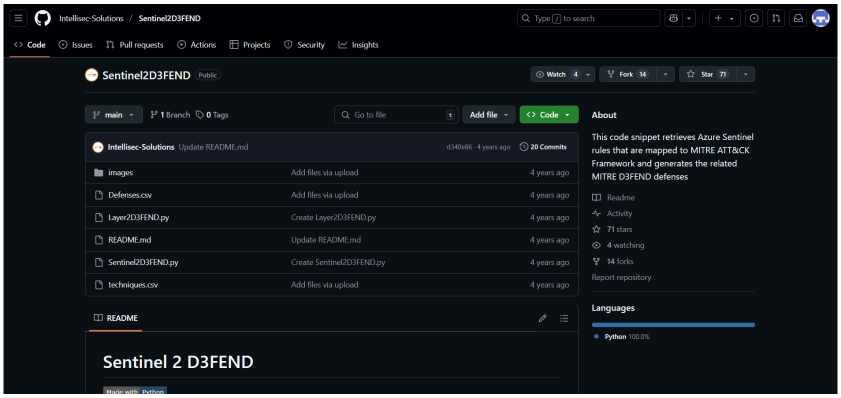
Model	Harden	Detect	Isolate	Deceive	Evict	- Restore	
+	+	+	+	+	+	**Restore Access**	**Restore Object**
						Reissue Credential	Restore Configuration
						Restore Network Access	Restore Database
						Restore User Account Access	Restore Disk Image
							Restore File
						Unlock Account	Restore Email
							Restore Software

3️⃣ Question:

What open-source project retrieves Azure Sentinel rules that are mapped to MITRE ATT&CK Framework and generates the related MITRE D3FEND defenses?

Answer: Sentinel 2 D3FEND

Source: GitHub Repository - Sentinel2D3FEND



Sentinel2D3FEND Public

Intellisec-Solutions Update README.md d340e86 · 4 years ago 20 Commits

images	Add files via upload	4 years ago
Defenses.csv	Add files via upload	4 years ago
Layer2D3FEND.py	Create Layer2D3FEND.py	4 years ago
README.md	Update README.md	4 years ago
Sentinel2D3FEND.py	Create Sentinel2D3FEND.py	4 years ago
techniques.csv	Add files via upload	4 years ago

README

Sentinel 2 D3FEND

Made with Python

About

This code snippet retrieves Azure Sentinel rules that are mapped to MITRE ATT&CK Framework and generates the related MITRE D3FEND defenses

Readme

Activity

71 stars

4 watching

14 forks

Report repository

Languages

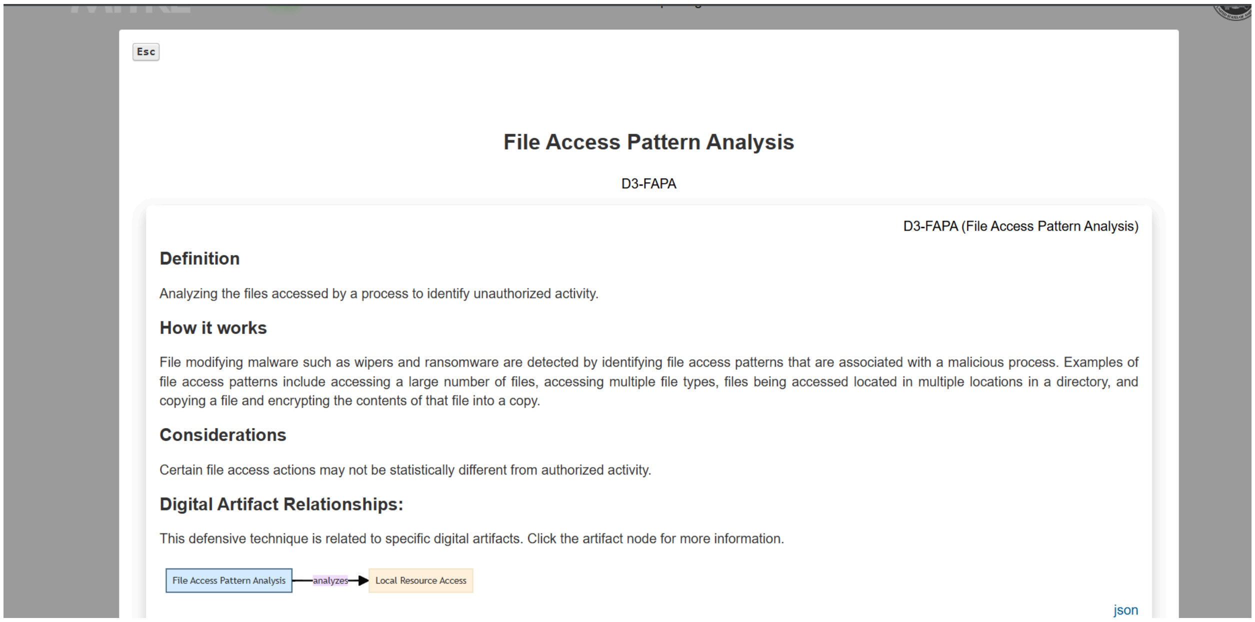
Python 100.0%

4️⃣Question:

What does ‘File Access Pattern Analysis’ mean?

Answer: Analyzing the files accessed by a process to identify unauthorized activity.

Source: [FileAccessPatternAnalysis – MITRE D3FEND]()



File Access Pattern Analysis

D3-FAPA

D3-FAPA (File Access Pattern Analysis)

Definition

Analyzing the files accessed by a process to identify unauthorized activity.

How it works

File modifying malware such as wipers and ransomware are detected by identifying file access patterns that are associated with a malicious process. Examples of file access patterns include accessing a large number of files, accessing multiple file types, files being accessed located in multiple locations in a directory, and copying a file and encrypting the contents of that file into a copy.

Considerations

Certain file access actions may not be statistically different from authorized activity.

Digital Artifact Relationships:

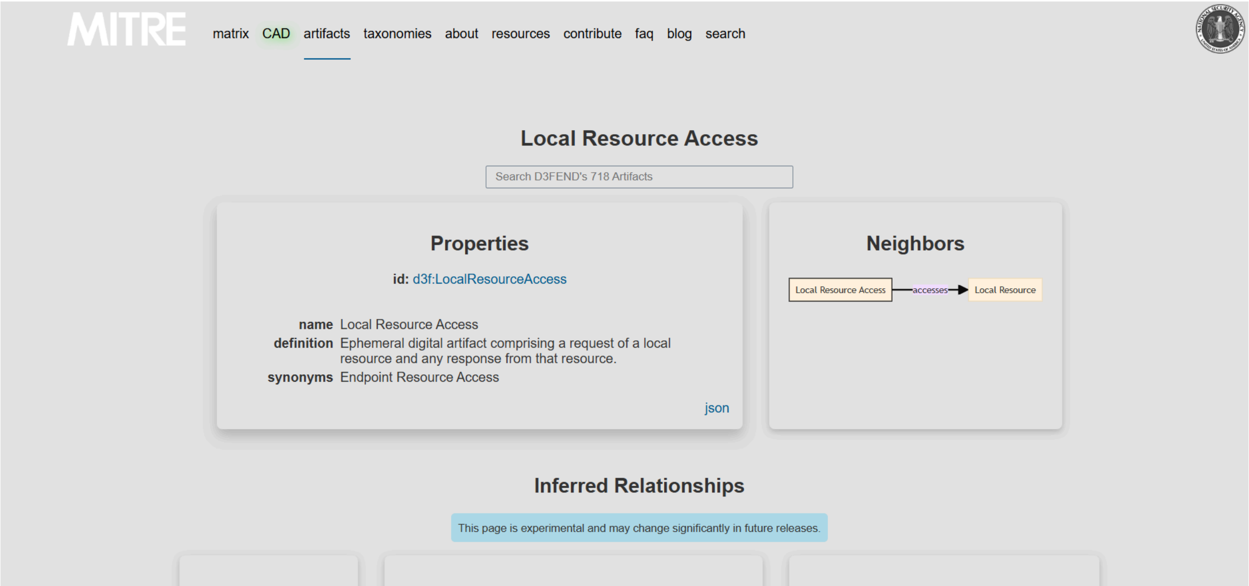
This defensive technique is related to specific digital artifacts. Click the artifact node for more information.

5️⃣Question:

What does ‘Local Resource Access’ artifact mean?

Answer: Ephemeral digital artifact comprising a request of a local resource and any response from that resource.

Source: [LocalResourceAccess – MITRE D3FEND]()



Local Resource Access

Search D3FEND's 718 Artifacts

Properties

id: d3f:LocalResourceAccess

name Local Resource Access

definition Ephemeral digital artifact comprising a request of a local resource and any response from that resource.

synonyms Endpoint Resource Access

json

Neighbors

Inferred Relationships

This page is experimental and may change significantly in future releases.

✅ Tools Used:

- Google Search (for OSINT)
- MITRE D3FEND website
- GitHub for open-source tool research

📌 Notes:

This documentation reflects my exploration and learning of D3FEND techniques, useful for building strong cyber defense understanding. It is part of my BTLO portfolio.