> “IF YOU KNOW THE **ENEMY**
> AND KNOW **YOURSELF,**
> YOU DO **NOT** NEED TO **FEAR**
> THE **RESULT** OF A
> **HUNDERED BATTLES.**”

~ Sun Tzu | The Art of War

Robbe Van den Daele

Security Operations Incident Responder

Security Consultant

@ The Collective

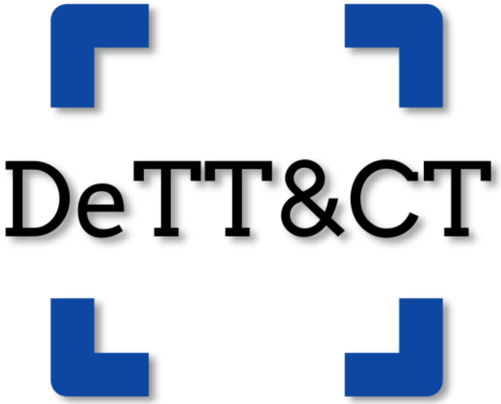
Security Technology and Procedures

Microsoft Sentinel and Defender

MITRE ATT&CK Gap Analysis

Hybrid Brothers
(https://hybridbrothers.com)

MITRE Frameworks



The Frameworks

ATT&CK, DEFEND, DeTT&CT

MITRE Frameworks - MITRE ATT&CK

- Knowledge base of adversary tactics and techniques based on real-world observations.
- Use cases
  - Adversary emulations
  - Read and purple teaming
  - Detection development
  - Defensive gap analysis
  - SOC maturity assessment
  - Cyber Threat Intelligence
- Biannual update releases (mostly in October and April)
- Three domains
  - Enterprise
  - Mobile
  - ICS

MITRE Frameworks - DeTT&CT

- Score and compare log source quality, visibility coverage, detection coverage and threat hunting behaviors
- Administering done via GUI
- Conversions done via Python
- Dettectinator used for SOC automation tooling

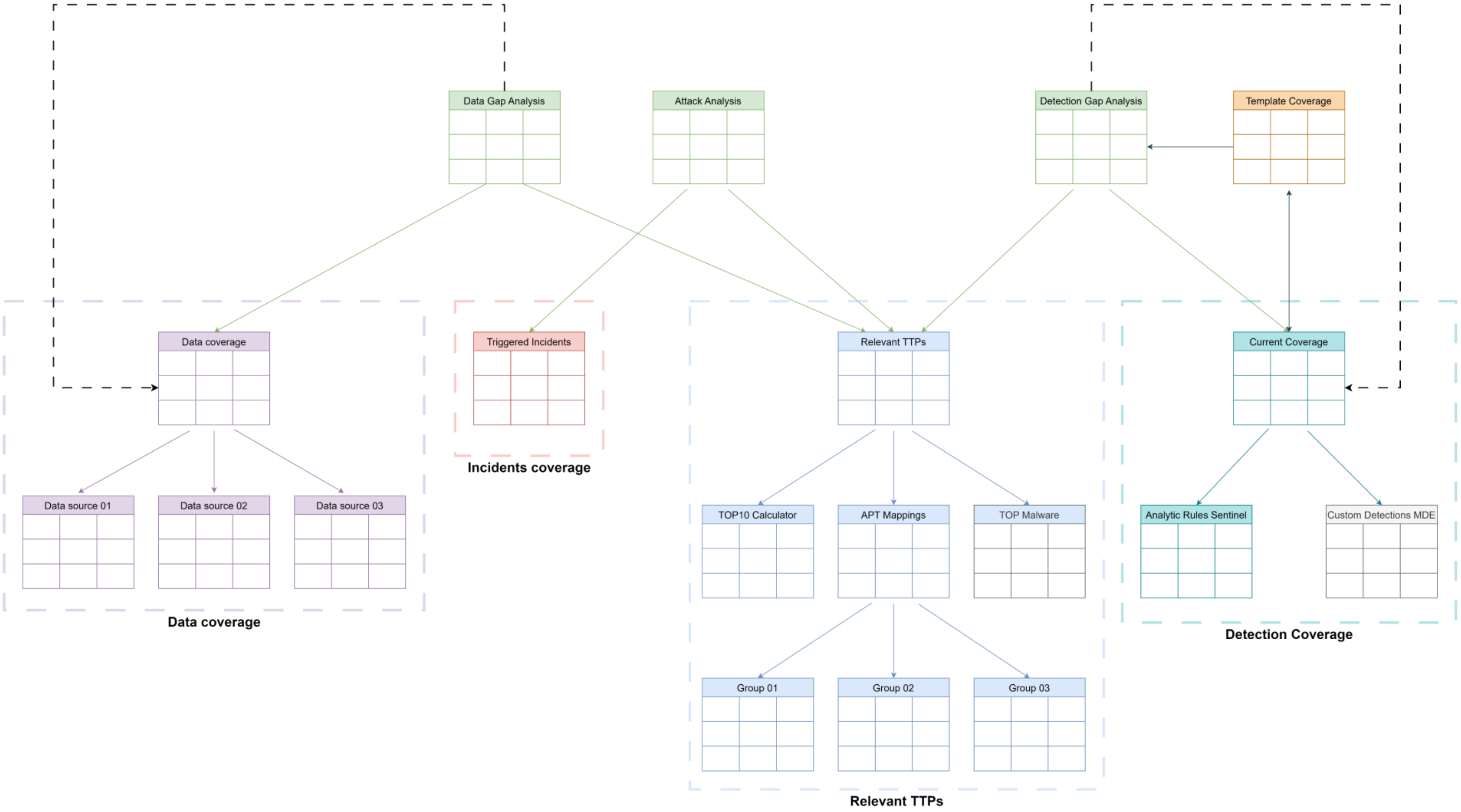
MITRE Frameworks - MITRE D3FEND

- Knowledge graph of Cyber Security countermeasure techniques, with relationships to offensive/adversary techniques in ATT&CK
- Use cases
    - Identify product differences and detection gaps relative to desired functionality
    - Suggest potential testing scope for defensive techniques in terms of relevant offensive techniques
- Still in Beta, stable release expected in 2024

Performing assessments

Data gap analysis, attack analysis, detection gap analysis

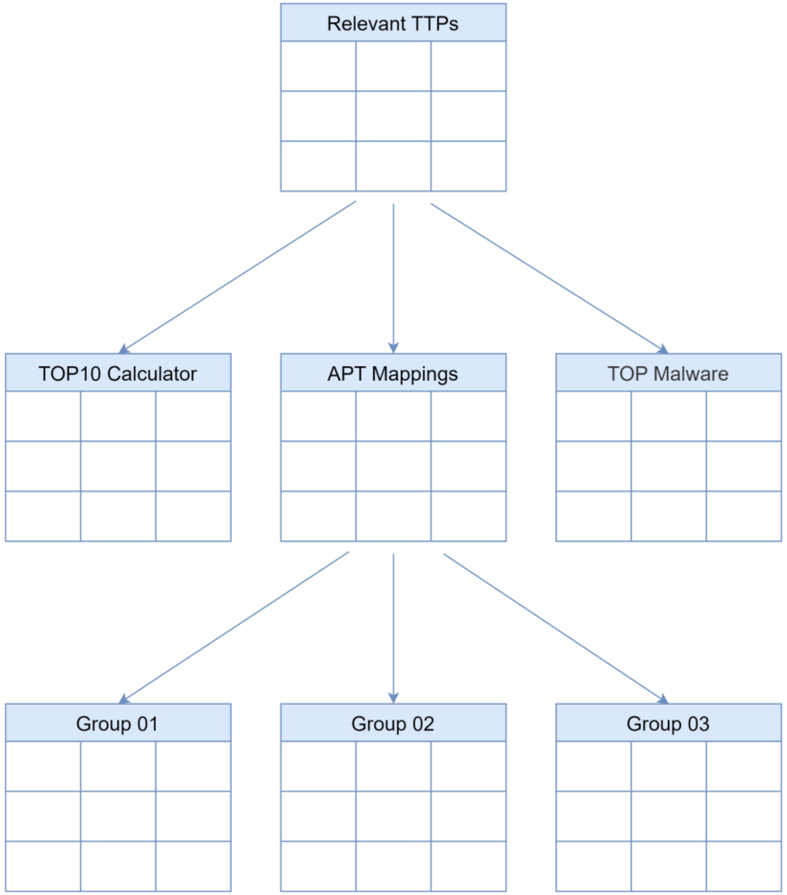
The assessment



Knowing your enemy

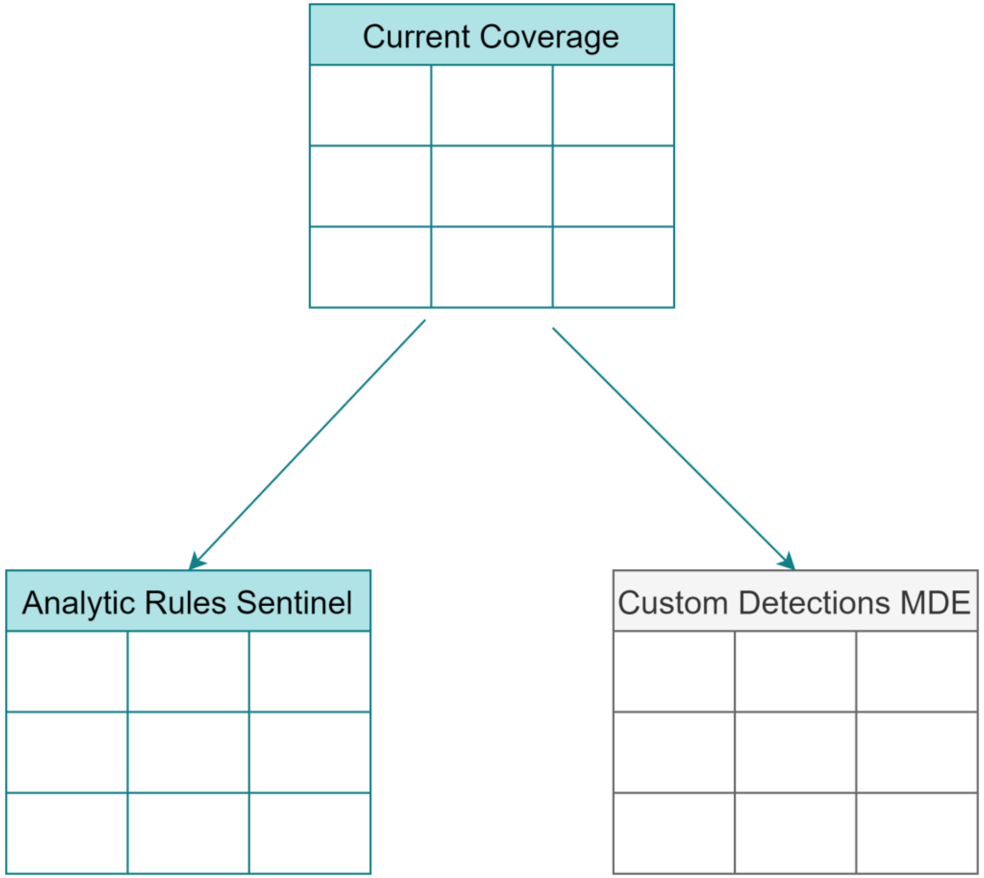
- TOP 10 most exploited techniques, based on your environment
- APT mappings for your industry
- Most used malware and tools

Demo



Detection coverage – Assessment types

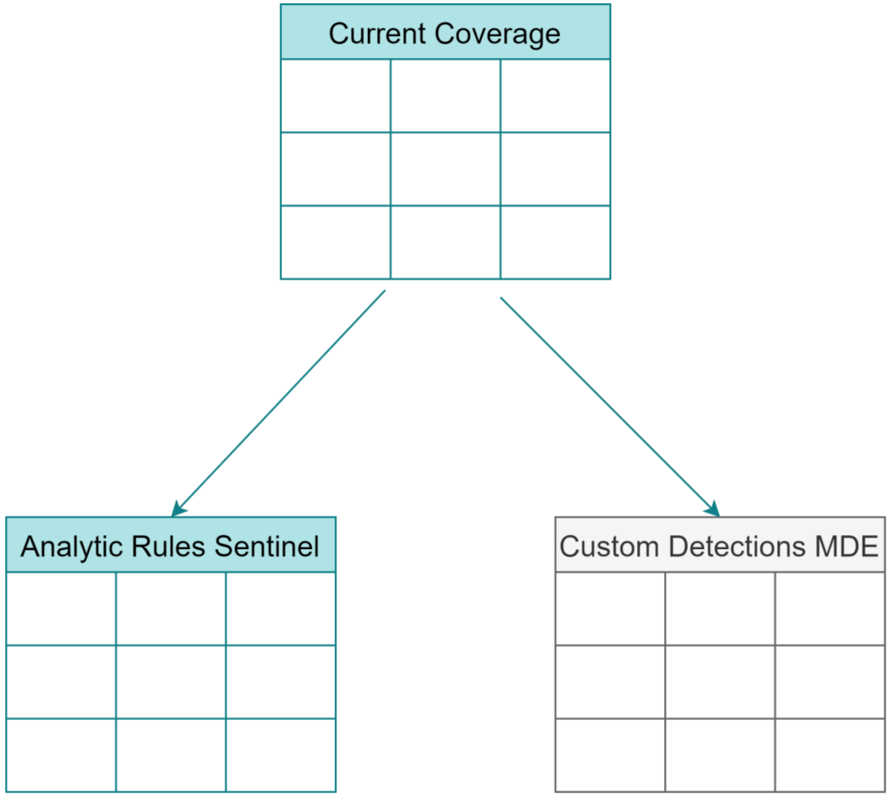
- Hands-on
  - Small-scoped
  - Pinpoint accuracy
  - Analytic rule refinement
  - Time consuming
- Hands-off
  - Broad strokes of coverage
  - Fast turnaround
  - High-level architecture and engineering
  - Going further, we talk about Hands-off assessments



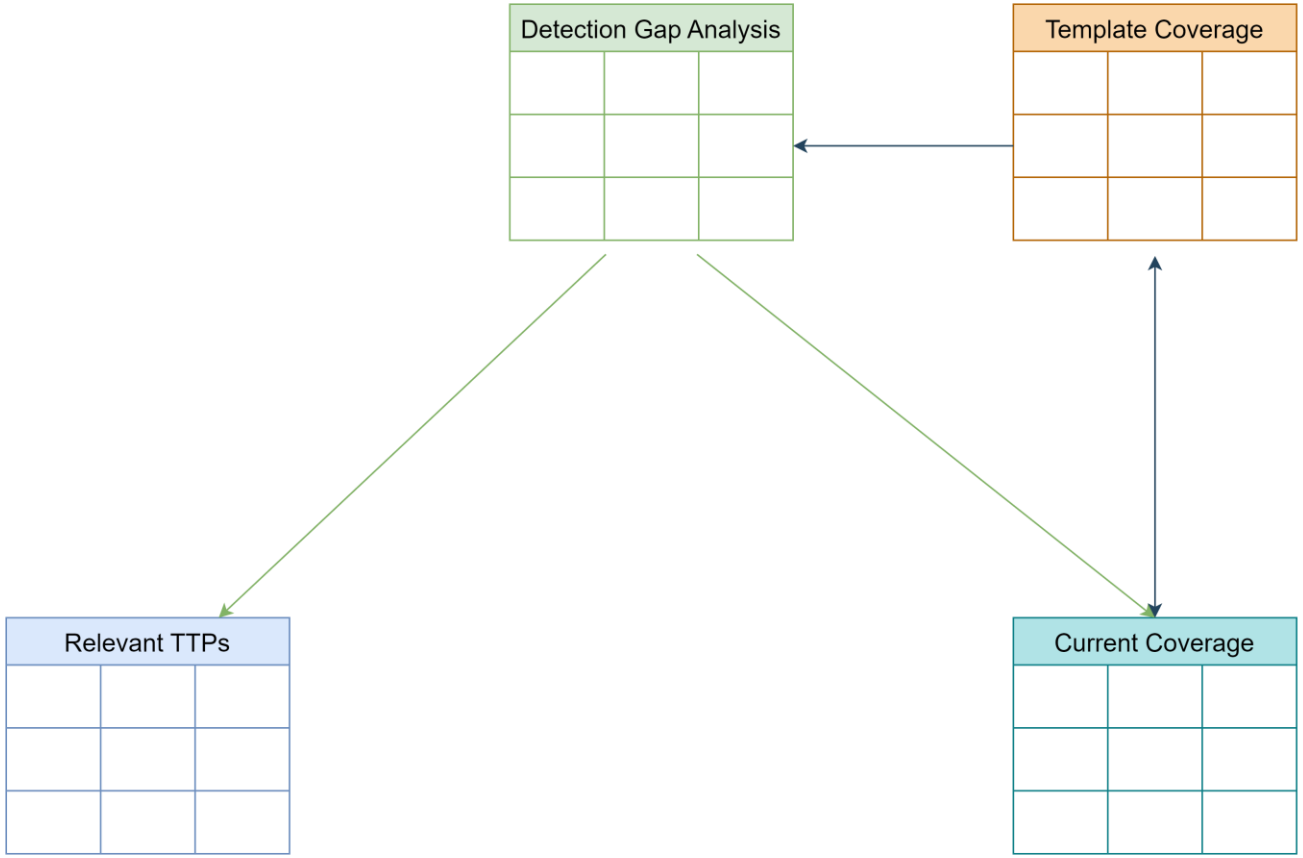
Detection coverage – Tools

- Analytic and Incidents Mapping project (HybridBrothers)
  - To ATT&CK
  - Score calculation based on sum
- Dettectinator
  - To DETT&CT
  - Score based on confidence level

Demo

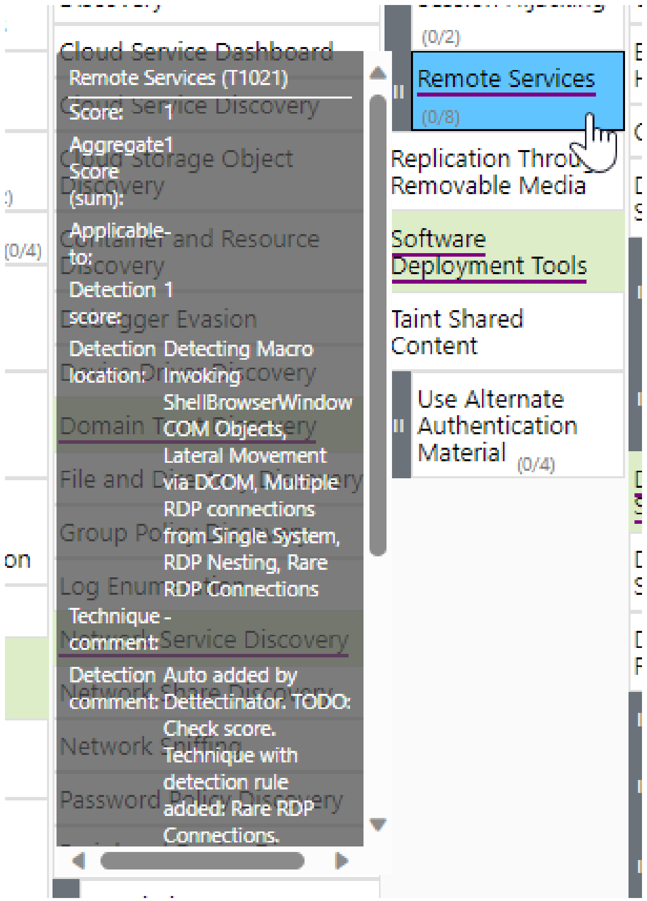


Detection Gap Analysis – Demo



Detection Gap Analysis – Missing Parts

- Missing Data Source context
  - Good Remote Service detections for FortiGate
  - Bad Remote Service detections for CheckPoint
- Score does not represent accurate average of different data source detections



Remote Services (T1021)

Score: 1

Aggregate Score (sum): 1

Applicable-to:

Detection score: 1

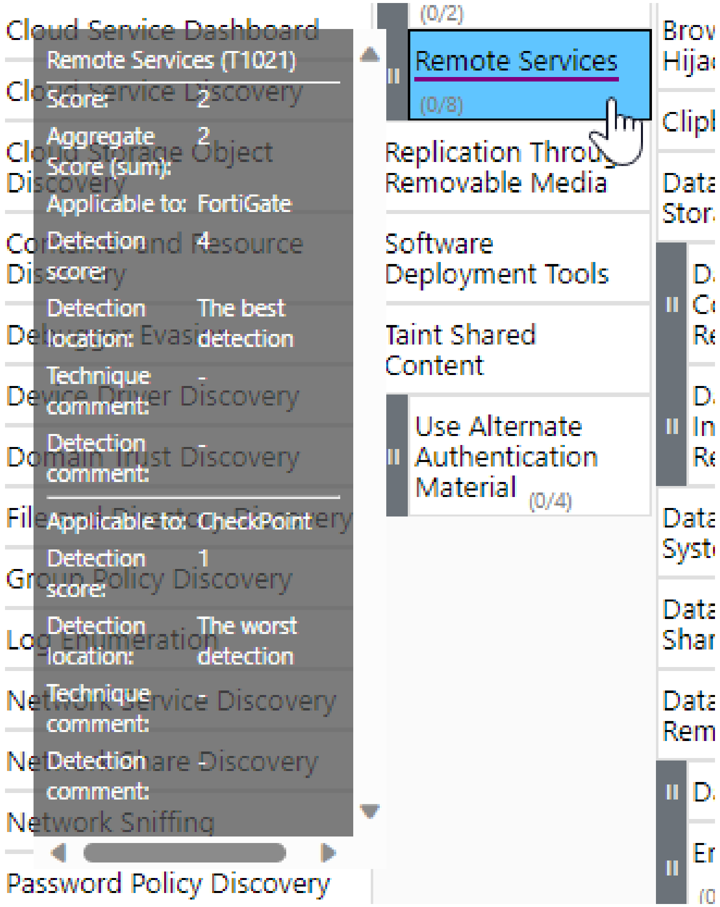
Detection location: Detecting Macro Invoking ShellBrowserWindow COM Objects, Lateral Movement via DCOM, Multiple RDP connections from Single System, RDP Nesting, Rare RDP Connections

Technique-comment:

Detection comment: Auto added by Dettectinator. TODO: Check score. Technique with detection rule added: Rare RDP Connections.

Detection Gap Analysis – Missing Parts Fix

- Using the applicable_to field for data source mapping
  - FortiGate has a score of 4
  - CheckPoint has a score of 1
- Total detection coverage score is an average of both
- Data source aware detection mapping → Provide important context



Remote Services (T1021)

Score: 2

Aggregate Score (sum): 2

Applicable to: FortiGate

Detection score: 4

Detection location: The best detection

Technique comment: -

Detection comment: -

Applicable to: CheckPoint

Detection score: 1

Detection location: The worst detection

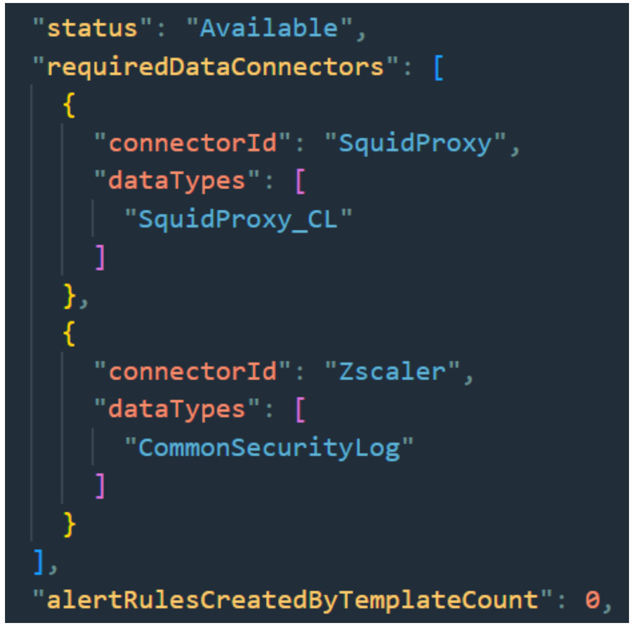
Technique comment: -

Detection comment: -

Cloud Service Dashboard
Cloud Service Discovery
Cloud Storage Object Discovery
Container and Resource 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
(0/2)
Remote Services
(0/8)
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication Material
(0/4)

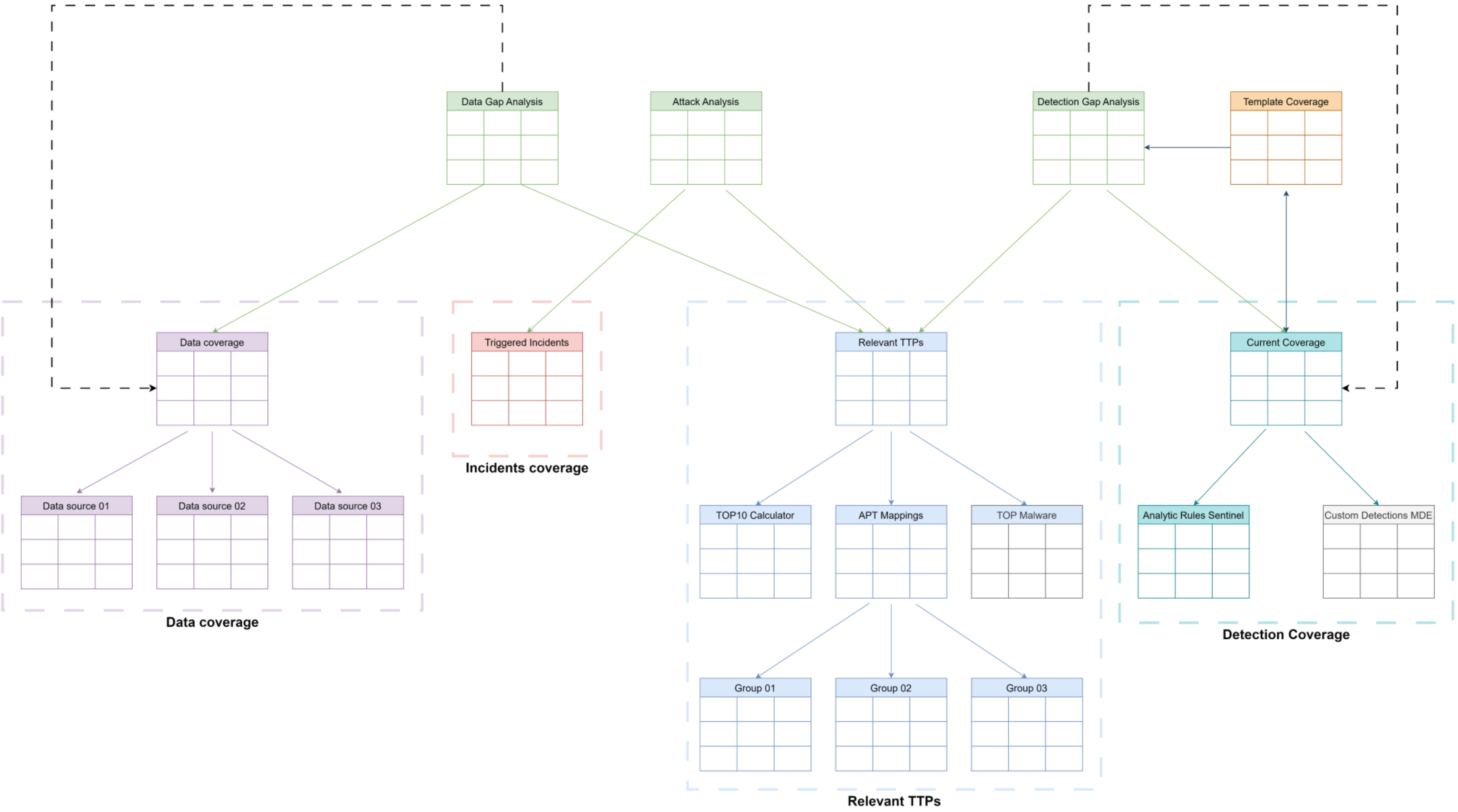
Detection Gap Analysis – Missing Parts Fix

- Using Sentinel to automate this fix
  - Mapping the connectorId of Sentinel to applicable_to of Dett&ct
- Building a custom plugin on Dettectinator
- Only manual task, is to assign the correct scores



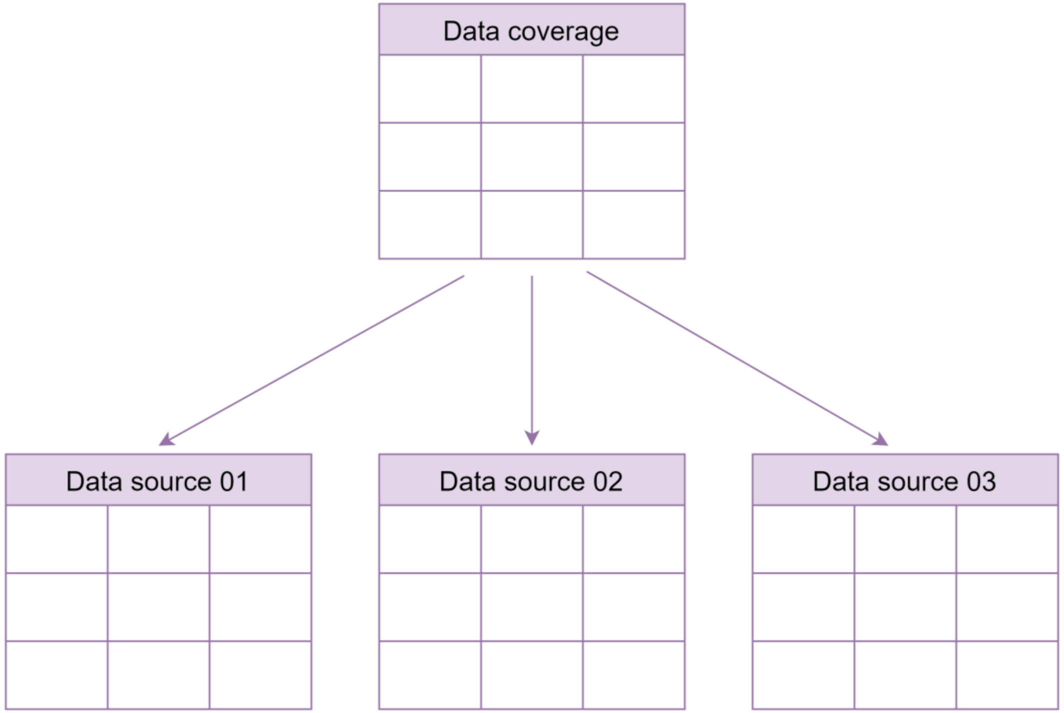
```
"status": "Available",
"requiredDataConnectors": [
  {
    "connectorId": "SquidProxy",
    "dataTypes": [
      "SquidProxy_CL"
    ]
  },
  {
    "connectorId": "Zscaler",
    "dataTypes": [
      "CommonSecurityLog"
    ]
  }
],
"alertRulesCreatedByTemplateCount": 0,
```

The assessment

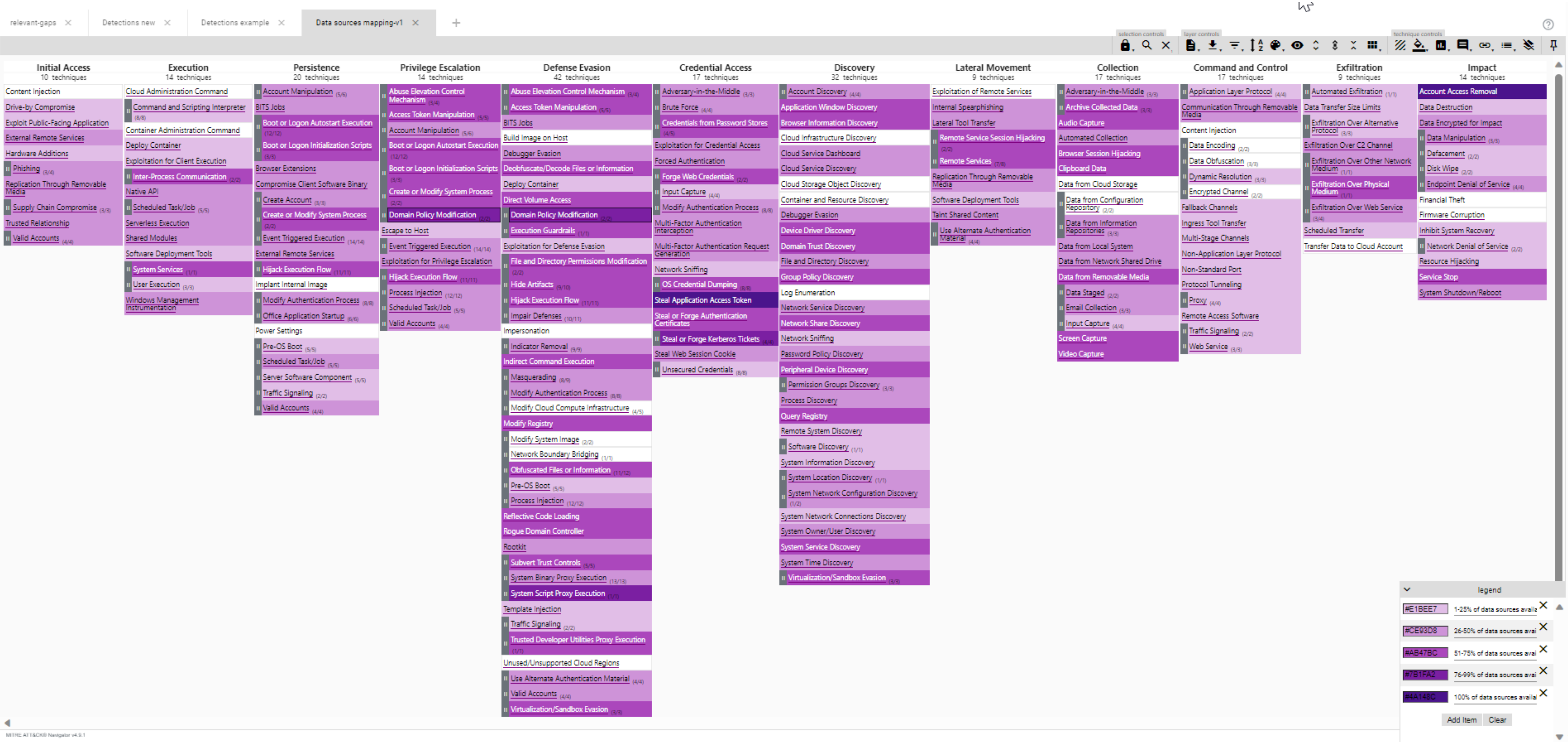


Data coverage

- Two flavors
  - Mapping Data Sources to techniques
  - Mapping Data Events to techniques
- Both very extensive, although less frequent
- Dett&ct framework



Data coverage – Data source mapping demo



Initial Access 10 techniques
- Content Injection
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (3/4)
- Replication Through Removable Media
- Supply Chain Compromise (3/3)
- Trusted Relationship
- Valid Accounts (4/4)

Execution 14 techniques
- Cloud Administration Command
- Command and Scripting Interpreter (8/8)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (2/2)
- Native API
- Scheduled Task/Job (5/5)
- Serverless Execution
- Shared Modules
- Software Deployment Tools
- System Services (1/1)
- User Execution (3/3)
- Windows Management Instrumentation

Persistence 20 techniques
- Account Manipulation (5/6)
- BITS Jobs
- Boot or Logon Autostart Execution (12/12)
- Boot or Logon Initialization Scripts (3/3)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (3/3)
- Create or Modify System Process (2/2)
- Event Triggered Execution (14/14)
- External Remote Services
- Hijack Execution Flow (11/11)
- Implant Internal Image
- Modify Authentication Process (8/8)
- Office Application Startup (6/6)
- Power Settings
- Pre-OS Boot (5/5)
- Scheduled Task/Job (5/5)
- Server Software Component (5/5)
- Traffic Signaling (2/2)
- Valid Accounts (4/4)

Privilege Escalation 14 techniques
- Abuse Elevation Control Mechanism (3/4)
- Access Token Manipulation (5/5)
- Account Manipulation (5/6)
- Boot or Logon Autostart Execution (12/12)
- Boot or Logon Initialization Scripts (3/3)
- Create or Modify System Process (2/2)
- Domain Policy Modification (2/2)
- Escape to Host
- Event Triggered Execution (14/14)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (11/11)
- Process Injection (12/12)
- Scheduled Task/Job (5/5)
- Valid Accounts (4/4)

Defense Evasion 42 techniques
- Abuse Elevation Control Mechanism (3/4)
- Access Token Manipulation (5/5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (2/2)
- Execution Guardrails (1/1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (2/2)
- Hide Artifacts (9/10)
- Hijack Execution Flow (11/11)
- Impair Defenses (10/11)
- Impersonation
- Indicator Removal (9/9)
- Indirect Command Execution
- Masquerading (8/9)
- Modify Authentication Process (8/8)
- Modify Cloud Compute Infrastructure (4/5)
- Modify Registry
- Modify System Image (2/2)
- Network Boundary Bridging (1/1)
- Obfuscated Files or Information (11/12)
- Pre-OS Boot (5/5)
- Process Injection (12/12)
- Reflective Code Loading
- Rogue Domain Controller
- Rootkit
- Subvert Trust Controls (5/5)
- System Binary Proxy Execution (13/13)
- System Script Proxy Execution (1/1)
- Template Injection
- Traffic Signaling (2/2)
- Trusted Developer Utilities Proxy Execution (1/1)
- Unused/Unsupported Cloud Regions
- Use Alternate Authentication Material (4/4)
- Valid Accounts (4/4)
- Virtualization/Sandbox Evasion (3/3)

Credential Access 17 techniques
- Adversary-in-the-Middle (3/3)
- Brute Force (4/4)
- Credentials from Password Stores (4/5)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (2/2)
- Input Capture (4/4)
- Modify Authentication Process (8/8)
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- Network Sniffing
- OS Credential Dumping (8/8)
- Steal Application Access Token
- Steal or Forge Authentication Certificates
- Steal or Forge Kerberos Tickets (4/4)
- Steal Web Session Cookie
- Unsecured Credentials (8/8)

Discovery 32 techniques
- Account Discovery (4/4)
- Application Window Discovery
- Browser Information Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource 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
- Permission Groups Discovery (3/3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (1/1)
- System Information Discovery
- System Location Discovery (1/1)
- System Network Configuration Discovery (1/2)
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion (3/3)

Lateral Movement 9 techniques
- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (2/2)
- Remote Services (7/8)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (4/4)

Collection 17 techniques
- Adversary-in-the-Middle (3/3)
- Archive Collected Data (3/3)
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage
- Data from Configuration Repository (2/2)
- Data from Information Repositories (3/3)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (2/2)
- Email Collection (3/3)
- Input Capture (4/4)
- Screen Capture
- Video Capture

Command and Control 17 techniques
- Application Layer Protocol (4/4)
- Communication Through Removable Media
- Content Injection
- Data Encoding (2/2)
- Data Obfuscation (3/3)
- Dynamic Resolution (3/3)
- Encrypted Channel (2/2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (4/4)
- Remote Access Software
- Traffic Signaling (2/2)
- Web Service (3/3)

Exfiltration 9 techniques
- Automated Exfiltration (1/1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (3/3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (1/1)
- Exfiltration Over Physical Medium (1/1)
- Exfiltration Over Web Service (3/4)
- Scheduled Transfer
- Transfer Data to Cloud Account

Impact 14 techniques
- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation (3/3)
- Defacement (2/2)
- Disk Wipe (2/2)
- Endpoint Denial of Service (4/4)
- Financial Theft
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service (2/2)
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

legend

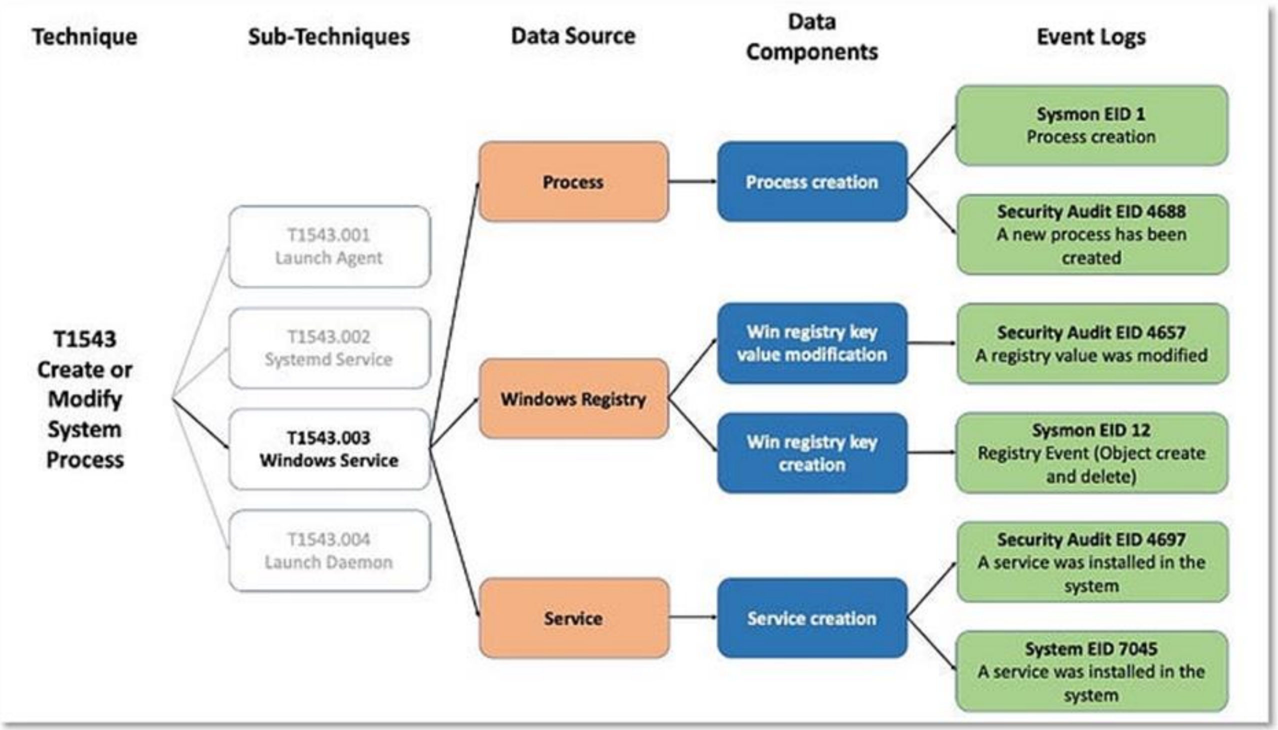
#E1BEE7	1-25% of data sources availa	×
#CE93D8	26-50% of data sources avai	×
#AB47BC	51-75% of data sources avai	×
#7B1FA2	76-99% of data sources avai	×
#4A148C	100% of data sources availal	×

Add Item Clear

MITRE ATT&CK® Navigator v4.9.1

Data coverage – Data event mapping

- Open-source tools exists
- OSSIM model
- MDE, Windows Events, and Sysmon to ATT&CK
- Example



Technique

Sub-Techniques

Data Source

Data Components

Event Logs

T1543 Create or Modify System Process

T1543.001 Launch Agent

T1543.002 Systemd Service

T1543.003 Windows Service

T1543.004 Launch Daemon

Process

Windows Registry

Service

Process creation

Win registry key value modification

Win registry key creation

Service creation

Sysmon EID 1 Process creation

Security Audit EID 4688 A new process has been created

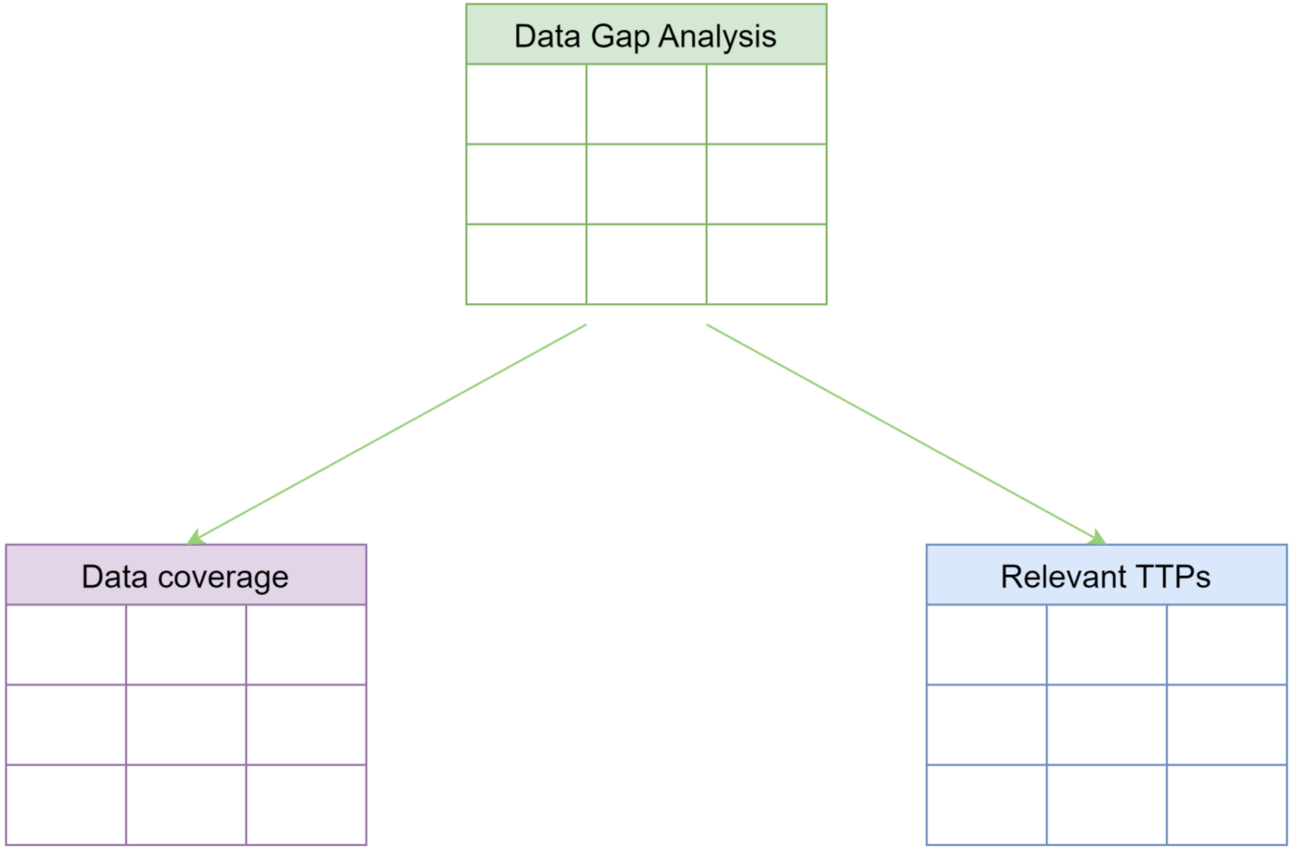
Security Audit EID 4657 A registry value was modified

Sysmon EID 12 Registry Event (Object create and delete)

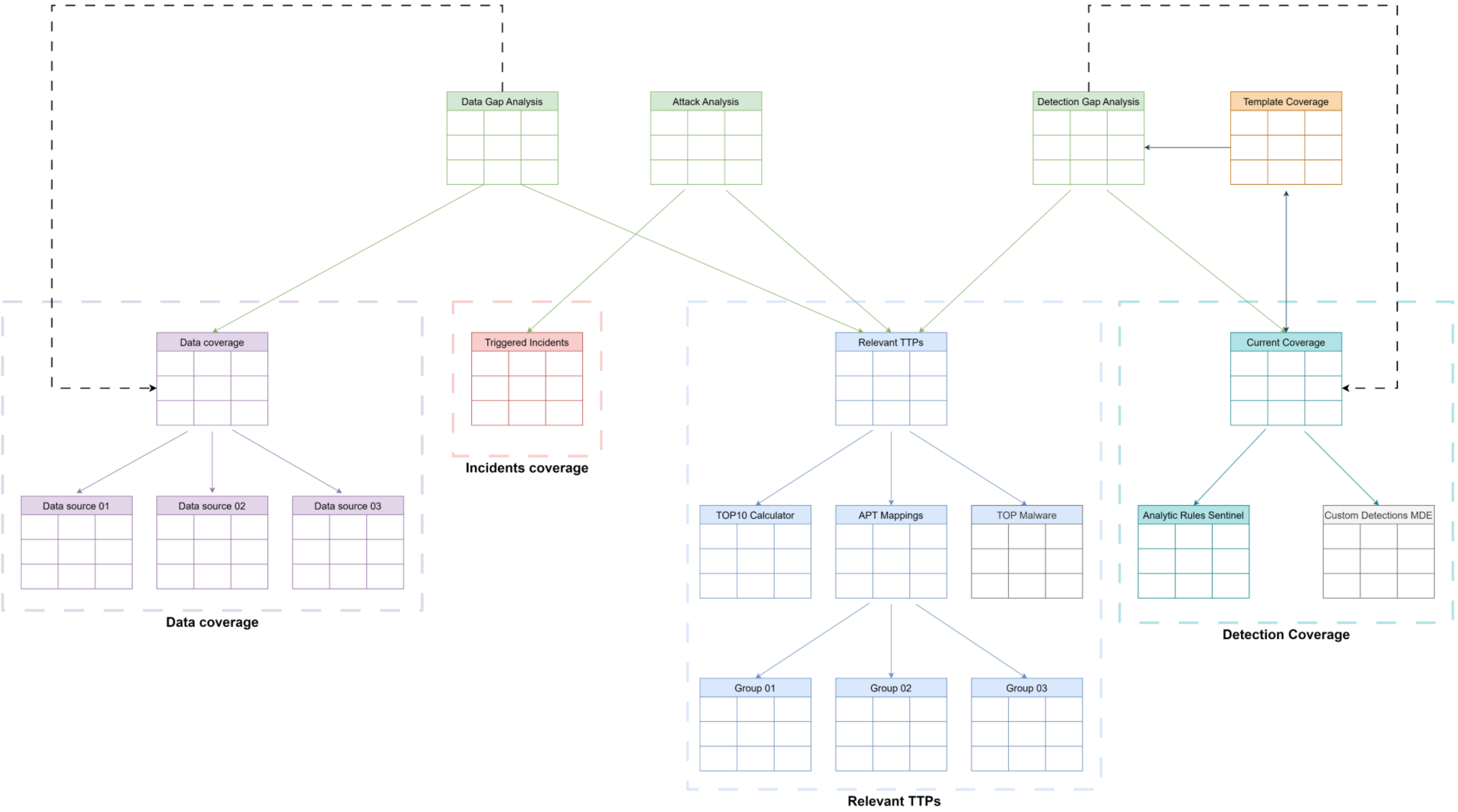
Security Audit EID 4697 A service was installed in the system

System EID 7045 A service was installed in the system

Detection Gap Analysis – Demo

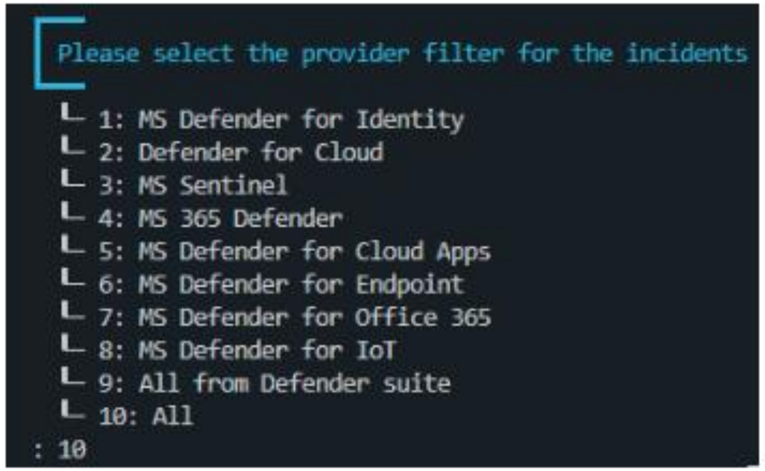


The assessment

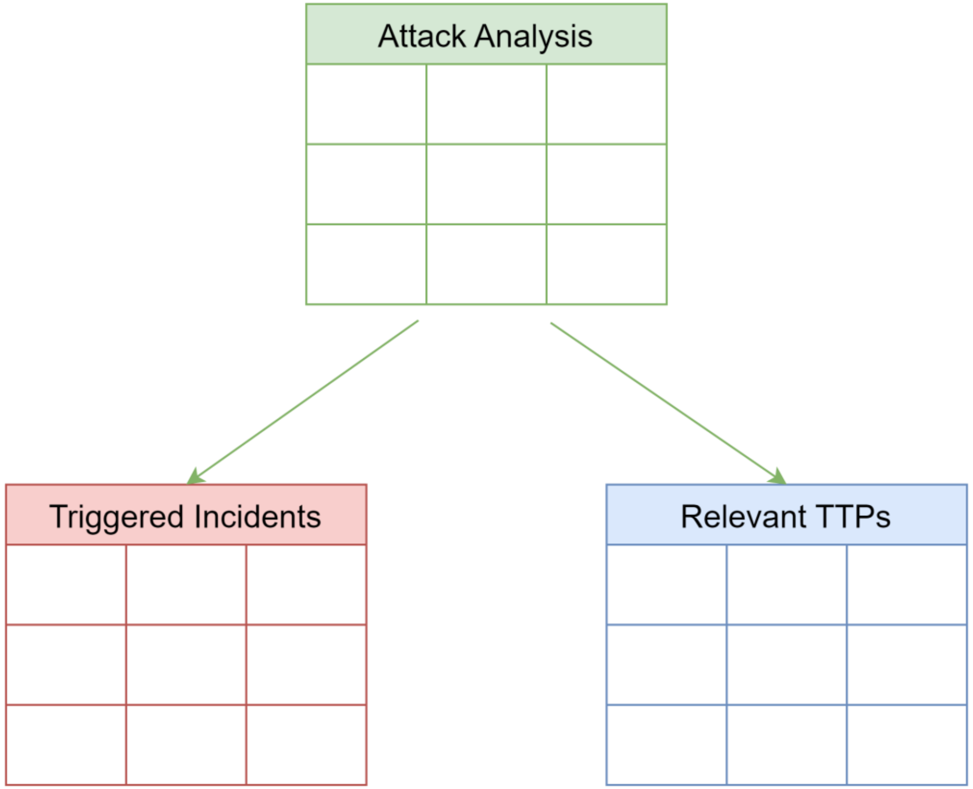


Incident mapping

- Analytic and Incidents Mapping project (HybridBrothers)
  - To ATT&CK
  - Score calculation based on sum



```
Please select the provider filter for the incidents
  └ 1: MS Defender for Identity
  └ 2: Defender for Cloud
  └ 3: MS Sentinel
  └ 4: MS 365 Defender
  └ 5: MS Defender for Cloud Apps
  └ 6: MS Defender for Endpoint
  └ 7: MS Defender for Office 365
  └ 8: MS Defender for IoT
  └ 9: All from Defender suite
  └ 10: All
: 10
```

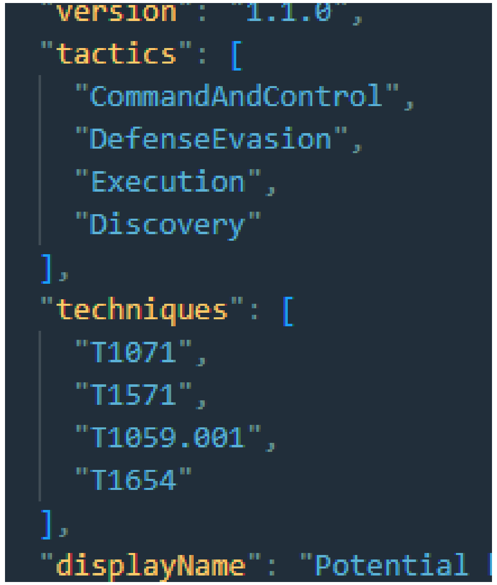


Microsoft MITRE support

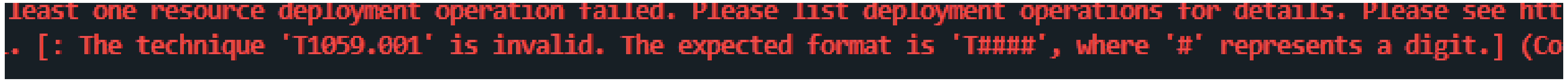
Limits and challenges

Microsoft Sentinel MITRE support

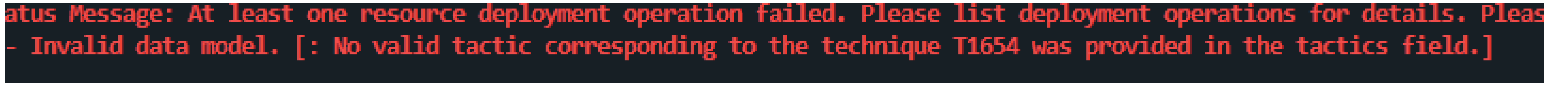
- No sub-technique support
  - Hands-on assessment hard to perform
- Limited ATT&CK version support
  - As of now ATT&CK v13 (v14 is out)
  - Docs even say ATT&CK v11



```
"version": "1.1.0",
"tactics": [
  "CommandAndControl",
  "DefenseEvasion",
  "Execution",
  "Discovery"
],
"techniques": [
  "T1071",
  "T1571",
  "T1059.001",
  "T1654"
],
"displayName": "Potential
```



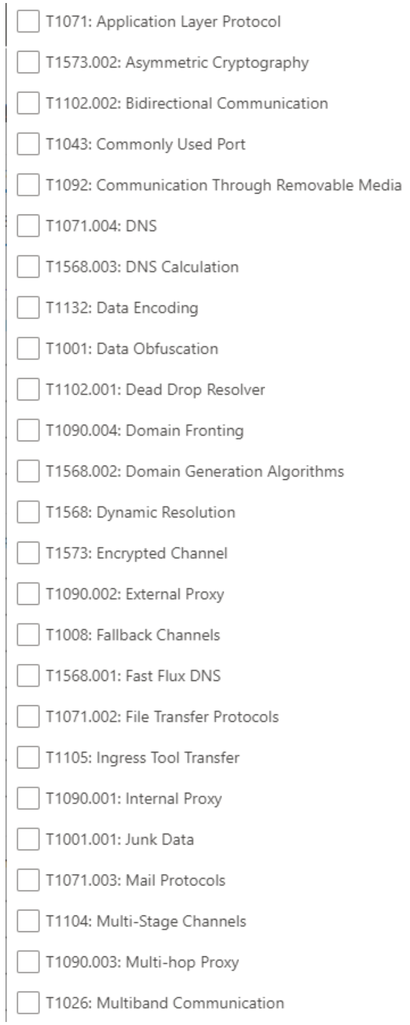
```
least one resource deployment operation failed. Please list deployment operations for details. Please see htt
. [: The technique 'T1059.001' is invalid. The expected format is 'T####', where '#' represents a digit.] (Co
```



```
atus Message: At least one resource deployment operation failed. Please list deployment operations for details. Pleas
- Invalid data model. [: No valid tactic corresponding to the technique T1654 was provided in the tactics field.]
```

MDE custom detections MITRE support

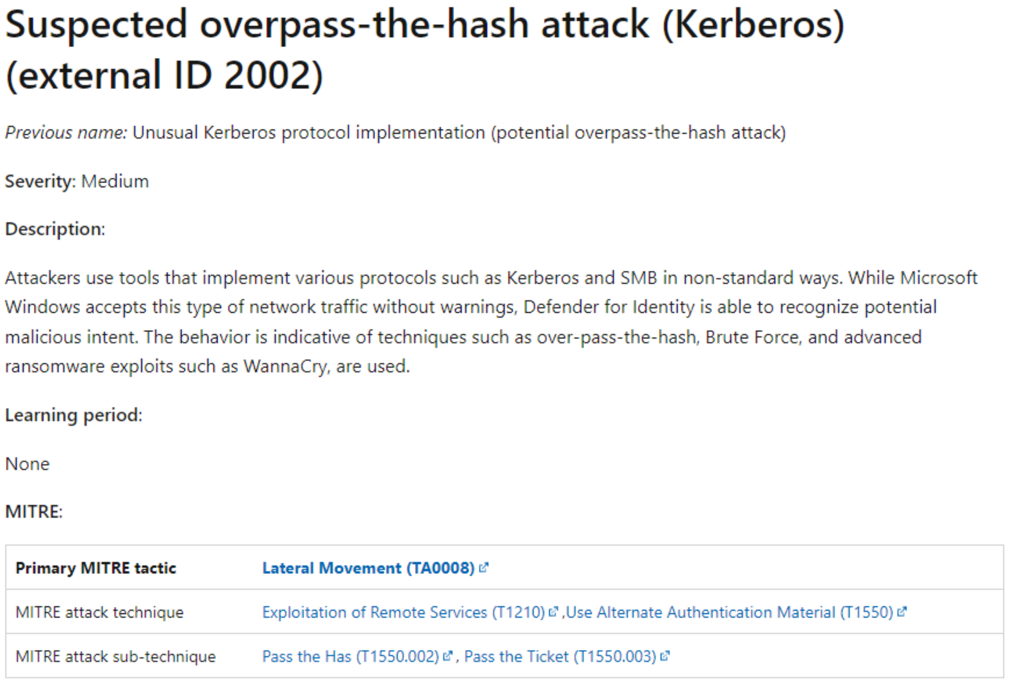
- Sub-technique support
  - Sub-technique lost when enumerated via Sentinel
- Limited ATT&CK version support
  - As of now ATT&CK v13 (v14 is out)



□ T1071: Application Layer Protocol
□ T1573.002: Asymmetric Cryptography
□ T1102.002: Bidirectional Communication
□ T1043: Commonly Used Port
□ T1092: Communication Through Removable Media
□ T1071.004: DNS
□ T1568.003: DNS Calculation
□ T1132: Data Encoding
□ T1001: Data Obfuscation
□ T1102.001: Dead Drop Resolver
□ T1090.004: Domain Fronting
□ T1568.002: Domain Generation Algorithms
□ T1568: Dynamic Resolution
□ T1573: Encrypted Channel
□ T1090.002: External Proxy
□ T1008: Fallback Channels
□ T1568.001: Fast Flux DNS
□ T1071.002: File Transfer Protocols
□ T1105: Ingress Tool Transfer
□ T1090.001: Internal Proxy
□ T1001.001: Junk Data
□ T1071.003: Mail Protocols
□ T1104: Multi-Stage Channels
□ T1090.003: Multi-hop Proxy
□ T1026: Multiband Communication

Defender for Identity MITRE support

- Alert name with MITRE mappings available in MS Learn
  - [Security alerts - Microsoft Defender for Identity | Microsoft Learn]
- Tactic, Technique, and Sub-Technique support → Hands-on assessments



Suspected overpass-the-hash attack (Kerberos) (external ID 2002)

Previous name: Unusual Kerberos protocol implementation (potential overpass-the-hash attack)

Severity: Medium

Description:

Attackers use tools that implement various protocols such as Kerberos and SMB in non-standard ways. While Microsoft Windows accepts this type of network traffic without warnings, Defender for Identity is able to recognize potential malicious intent. The behavior is indicative of techniques such as over-pass-the-hash, Brute Force, and advanced ransomware exploits such as WannaCry, are used.

Learning period:

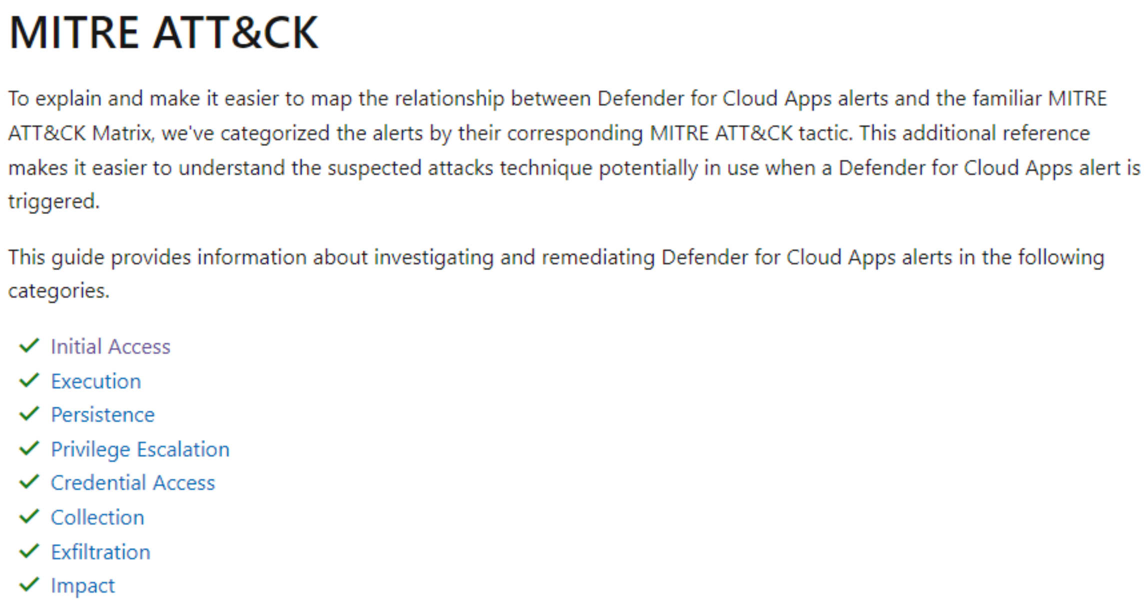
None

MITRE:

Primary MITRE tactic	**Lateral Movement (TA0008)**
MITRE attack technique	Exploitation of Remote Services (T1210) ,Use Alternate Authentication Material (T1550)
MITRE attack sub-technique	Pass the Has (T1550.002) , Pass the Ticket (T1550.003)

Defender for Cloud Apps MITRE support

- Alert name with MITRE mappings available in MS Learn
  - How to investigate anomaly detection alerts - Microsoft Defender for Cloud Apps | Microsoft Learn
- Only Tactic support → Hands-off assessments



MITRE ATT&CK

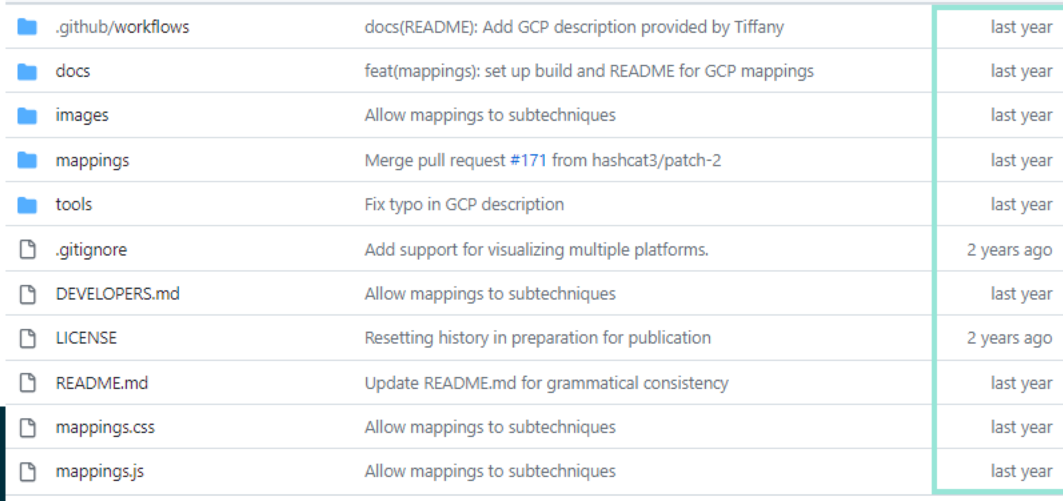
To explain and make it easier to map the relationship between Defender for Cloud Apps alerts and the familiar MITRE ATT&CK Matrix, we've categorized the alerts by their corresponding MITRE ATT&CK tactic. This additional reference makes it easier to understand the suspected attacks technique potentially in use when a Defender for Cloud Apps alert is triggered.

This guide provides information about investigating and remediating Defender for Cloud Apps alerts in the following categories.

- ✓ Initial Access
- ✓ Execution
- ✓ Persistence
- ✓ Privilege Escalation
- ✓ Credential Access
- ✓ Collection
- ✓ Exfiltration
- ✓ Impact

Defender for Endpoint MITRE support

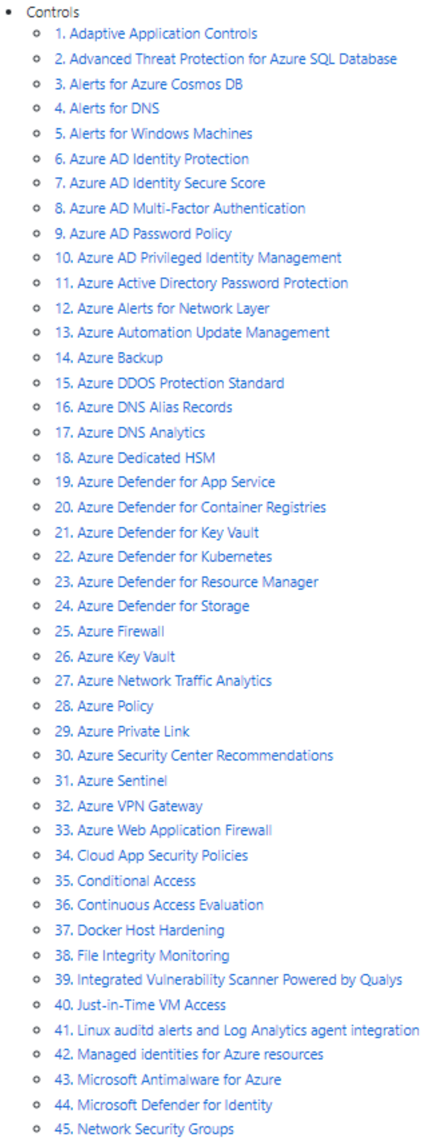
- No Documentation
- Work arounds
    - Mapping incidents
    - BAS – Breach and Attack simulation
        - Caldera / Atomic Red Team
        - AttackIQ Evaluations
    - MS Azure Security control mapping [Microsoft Azure Security Control Mappings to MITRE ATT&CK® (center-for-threat-informed-defense.github.io)]



.github/workflows	docs(README): Add GCP description provided by Tiffany	last year
docs	feat(mappings): set up build and README for GCP mappings	last year
images	Allow mappings to subtechniques	last year
mappings	Merge pull request #171 from hashcat3/patch-2	last year
tools	Fix typo in GCP description	last year
.gitignore	Add support for visualizing multiple platforms.	2 years ago
DEVELOPERS.md	Allow mappings to subtechniques	last year
LICENSE	Resetting history in preparation for publication	2 years ago
README.md	Update README.md for grammatical consistency	last year
mappings.css	Allow mappings to subtechniques	last year
mappings.js	Allow mappings to subtechniques	last year

Azure Stack MITRE Support

- MS Azure Security control mapping Microsoft Azure Security Control Mappings to MITRE ATT&CK® (center-for-threat-defense.github.io)
  - A little outdated
  - Not always complete



- Controls
  - 1. Adaptive Application Controls
  - 2. Advanced Threat Protection for Azure SQL Database
  - 3. Alerts for Azure Cosmos DB
  - 4. Alerts for DNS
  - 5. Alerts for Windows Machines
  - 6. Azure AD Identity Protection
  - 7. Azure AD Identity Secure Score
  - 8. Azure AD Multi-Factor Authentication
  - 9. Azure AD Password Policy
  - 10. Azure AD Privileged Identity Management
  - 11. Azure Active Directory Password Protection
  - 12. Azure Alerts for Network Layer
  - 13. Azure Automation Update Management
  - 14. Azure Backup
  - 15. Azure DDOS Protection Standard
  - 16. Azure DNS Alias Records
  - 17. Azure DNS Analytics
  - 18. Azure Dedicated HSM
  - 19. Azure Defender for App Service
  - 20. Azure Defender for Container Registries
  - 21. Azure Defender for Key Vault
  - 22. Azure Defender for Kubernetes
  - 23. Azure Defender for Resource Manager
  - 24. Azure Defender for Storage
  - 25. Azure Firewall
  - 26. Azure Key Vault
  - 27. Azure Network Traffic Analytics
  - 28. Azure Policy
  - 29. Azure Private Link
  - 30. Azure Security Center Recommendations
  - 31. Azure Sentinel
  - 32. Azure VPN Gateway
  - 33. Azure Web Application Firewall
  - 34. Cloud App Security Policies
  - 35. Conditional Access
  - 36. Continuous Access Evaluation
  - 37. Docker Host Hardening
  - 38. File Integrity Monitoring
  - 39. Integrated Vulnerability Scanner Powered by Qualys
  - 40. Just-in-Time VM Access
  - 41. Linux auditd alerts and Log Analytics agent integration
  - 42. Managed identities for Azure resources
  - 43. Microsoft Antimalware for Azure
  - 44. Microsoft Defender for Identity
  - 45. Network Security Groups

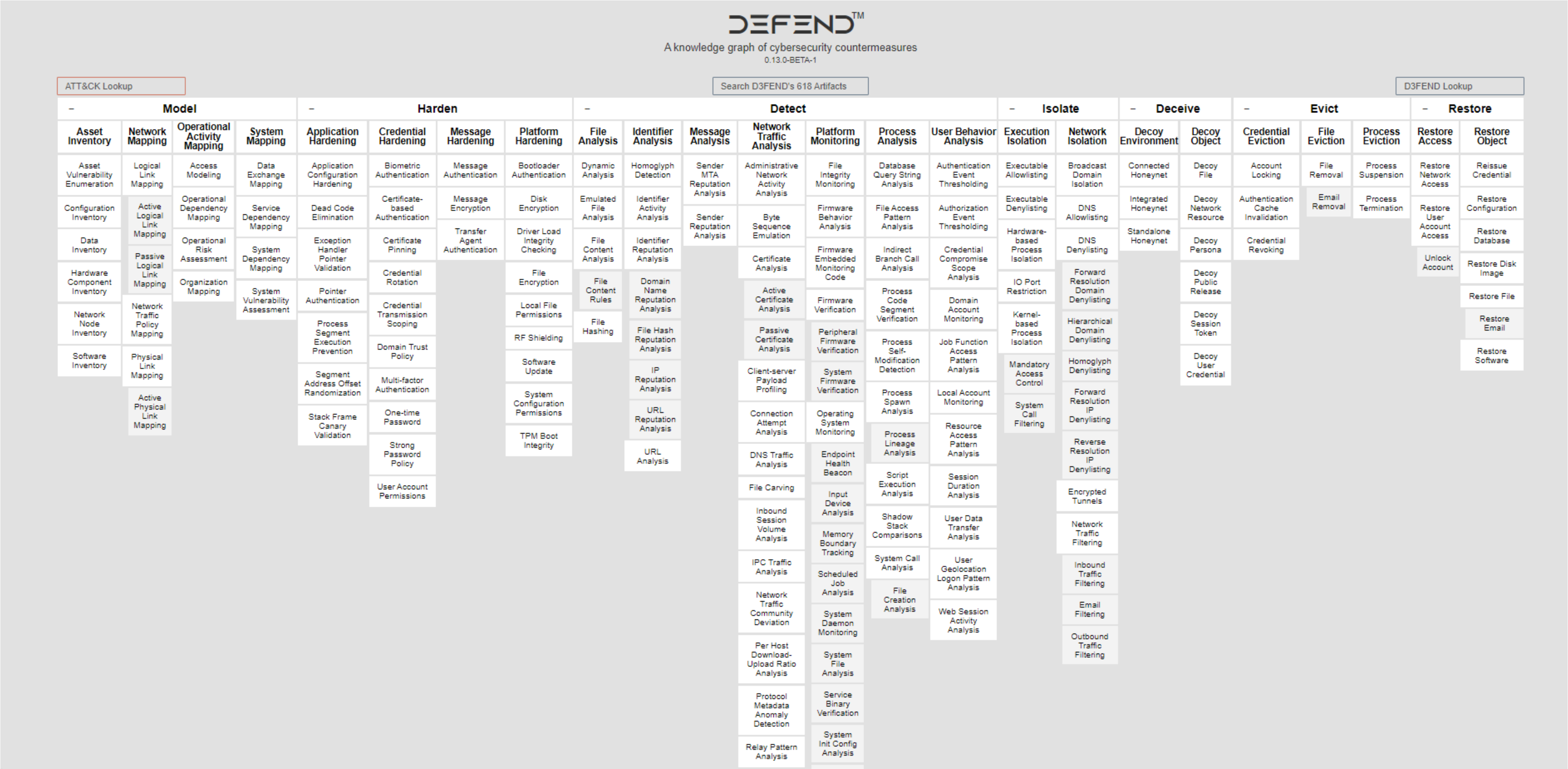
How do I improve

Detective and preventive controls

Improving

1. Map your relevant TTPs
2. Create data and detection mappings
3. Perform data and detection gap analysis
4. Add data sources for important missing techniques
5. Create detections for weakly covered techniques

Improving using DEFEND



D3FEND™

A knowledge graph of cybersecurity countermeasures

0.13.0-BETA-1

– Model

- **Asset Inventory**
  - Asset Vulnerability Enumeration
  - Configuration Inventory
  - Data Inventory
  - Hardware Component Inventory
  - Network Node Inventory
  - Software Inventory
- **Network Mapping**
  - Logical Link Mapping
  - Active Logical Link Mapping
  - Passive Logical Link Mapping
  - Network Traffic Policy Mapping
  - Physical Link Mapping
  - Active Physical Link Mapping
- **Operational Activity Mapping**
  - Access Modeling
  - Operational Dependency Mapping
  - Operational Risk Assessment
  - Organization Mapping
- **System Mapping**
  - Data Exchange Mapping
  - Service Dependency Mapping
  - System Dependency Mapping
  - System Vulnerability Assessment

– Harden

- **Application Hardening**
  - Application Configuration Hardening
  - Dead Code Elimination
  - Exception Handler Pointer Validation
  - Pointer Authentication
  - Process Segment Execution Prevention
  - Segment Address Offset Randomization
  - Stack Frame Canary Validation
- **Credential Hardening**
  - Biometric Authentication
  - Certificate-based Authentication
  - Certificate Pinning
  - Credential Rotation
  - Credential Transmission Scoping
  - Domain Trust Policy
  - Multi-factor Authentication
  - One-time Password
  - Strong Password Policy
  - User Account Permissions
- **Message Hardening**
  - Message Authentication
  - Message Encryption
  - Transfer Agent Authentication
- **Platform Hardening**
  - Bootloader Authentication
  - Disk Encryption
  - Driver Load Integrity Checking
  - File Encryption
  - Local File Permissions
  - RF Shielding
  - Software Update
  - System Configuration Permissions
  - TPM Boot Integrity

– Detect

- **File Analysis**
  - Dynamic Analysis
  - Emulated File Analysis
  - File Content Analysis
  - File Content Rules
  - File Hashing
- **Identifier Analysis**
  - Homoglyph Detection
  - Identifier Activity Analysis
  - Identifier Reputation Analysis
  - Domain Name Reputation Analysis
  - File Hash Reputation Analysis
  - IP Reputation Analysis
  - URL Reputation Analysis
  - URL Analysis
- **Message Analysis**
  - Sender MTA Reputation Analysis
  - Sender Reputation Analysis
- **Network Traffic Analysis**
  - Administrative Network Activity Analysis
  - Byte Sequence Emulation
  - Certificate Analysis
  - Active Certificate Analysis
  - Passive Certificate Analysis
  - Client-server Payload Profiling
  - Connection Attempt Analysis
  - DNS Traffic Analysis
  - File Carving
  - Inbound Session Volume Analysis
  - IPC Traffic Analysis
  - Network Traffic Community Deviation
  - Per Host Download-Upload Ratio Analysis
  - Protocol Metadata Anomaly Detection
  - Relay Pattern Analysis
- **Platform Monitoring**
  - File Integrity Monitoring
  - Firmware Behavior Analysis
  - Firmware Embedded Monitoring Code
  - Firmware Verification
  - Peripheral Firmware Verification
  - System Firmware Verification
  - Operating System Monitoring
  - Endpoint Health Beacon
  - Input Device Analysis
  - Memory Boundary Tracking
  - Scheduled Job Analysis
  - System Daemon Monitoring
  - System File Analysis
  - Service Binary Verification
  - System Init Config Analysis
- **Process Analysis**
  - Database Query String Analysis
  - File Access Pattern Analysis
  - Indirect Branch Call Analysis
  - Process Code Segment Verification
  - Process Self-Modification Detection
  - Process Spawn Analysis
  - Process Lineage Analysis
  - Script Execution Analysis
  - Shadow Stack Comparisons
  - System Call Analysis
  - File Creation Analysis
- **User Behavior Analysis**
  - Authentication Event Thresholding
  - Authorization Event Thresholding
  - Credential Compromise Scope Analysis
  - Domain Account Monitoring
  - Job Function Access Pattern Analysis
  - Local Account Monitoring
  - Resource Access Pattern Analysis
  - Session Duration Analysis
  - User Data Transfer Analysis
  - User Geolocation Logon Pattern Analysis
  - Web Session Activity Analysis

– Isolate

- **Execution Isolation**
  - Executable Allowlisting
  - Executable Denylisting
  - Hardware-based Process Isolation
  - IO Port Restriction
  - Kernel-based Process Isolation
  - Mandatory Access Control
  - System Call Filtering
- **Network Isolation**
  - Broadcast Domain Isolation
  - DNS Allowlisting
  - DNS Denylisting
  - Forward Resolution Domain Denylisting
  - Hierarchical Domain Denylisting
  - Homoglyph Denylisting
  - Forward Resolution IP Denylisting
  - Reverse Resolution IP Denylisting
  - Encrypted Tunnels
  - Network Traffic Filtering
  - Inbound Traffic Filtering
  - Email Filtering
  - Outbound Traffic Filtering

– Deceive

- **Decoy Environment**
  - Connected Honeynet
  - Integrated Honeynet
  - Standalone Honeynet
- **Decoy Object**
  - Decoy File
  - Decoy Network Resource
  - Decoy Persona
  - Decoy Public Release
  - Decoy Session Token
  - Decoy User Credential

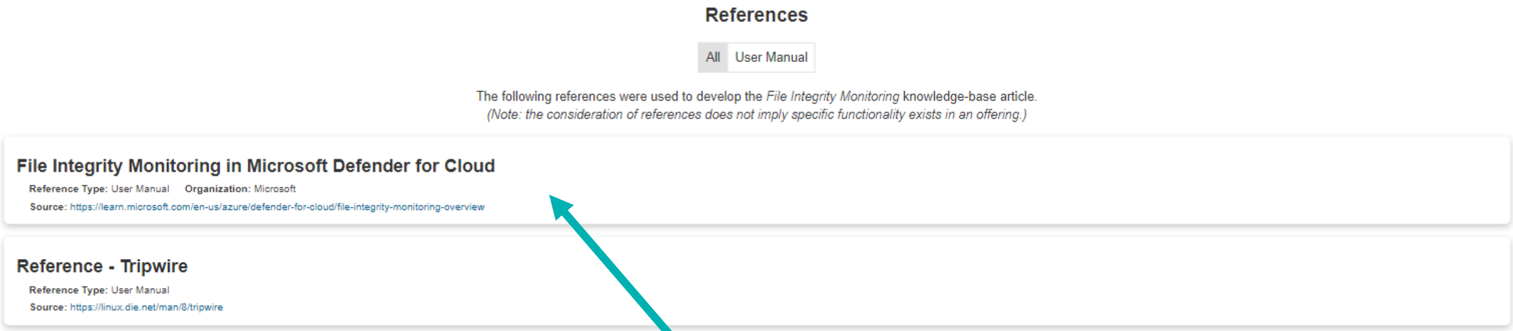
– Evict

- **Credential Eviction**
  - Account Locking
  - Authentication Cache Invalidation
  - Credential Revoking
- **File Eviction**
  - File Removal
  - Email Removal
- **Process Eviction**
  - Process Suspension
  - Process Termination

– Restore

- **Restore Access**
  - Restore Network Access
  - Restore User Account Access
  - Unlock Account
- **Restore Object**
  - Reissue Credential
  - Restore Configuration
  - Restore Database
  - Restore Disk Image
  - Restore File
  - Restore Email
  - Restore Software

Improving using DEFEND



References

All | User Manual

The following references were used to develop the *File Integrity Monitoring* knowledge-base article.
(Note: the consideration of references does not imply specific functionality exists in an offering.)

File Integrity Monitoring in Microsoft Defender for Cloud

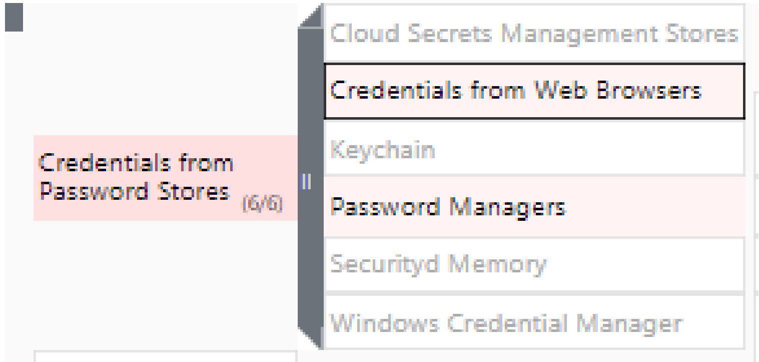
Reference Type: User Manual **Organization:** Microsoft

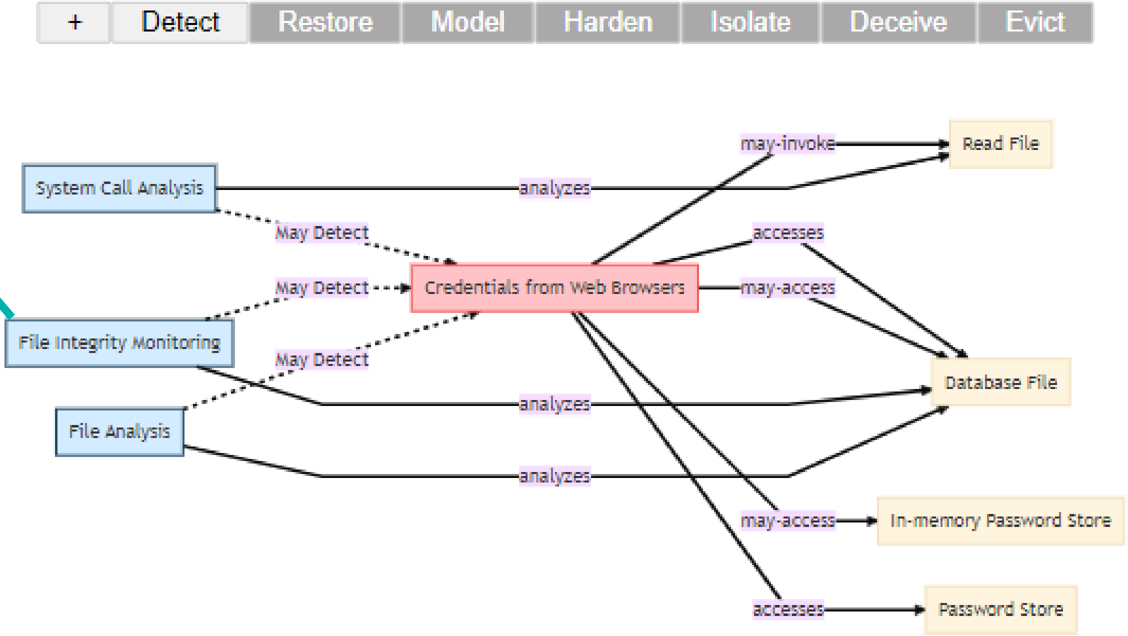
Source: https://learn.microsoft.com/en-us/azure/defender-for-cloud/file-integrity-monitoring-overview

Reference - Tripwire

Reference Type: User Manual

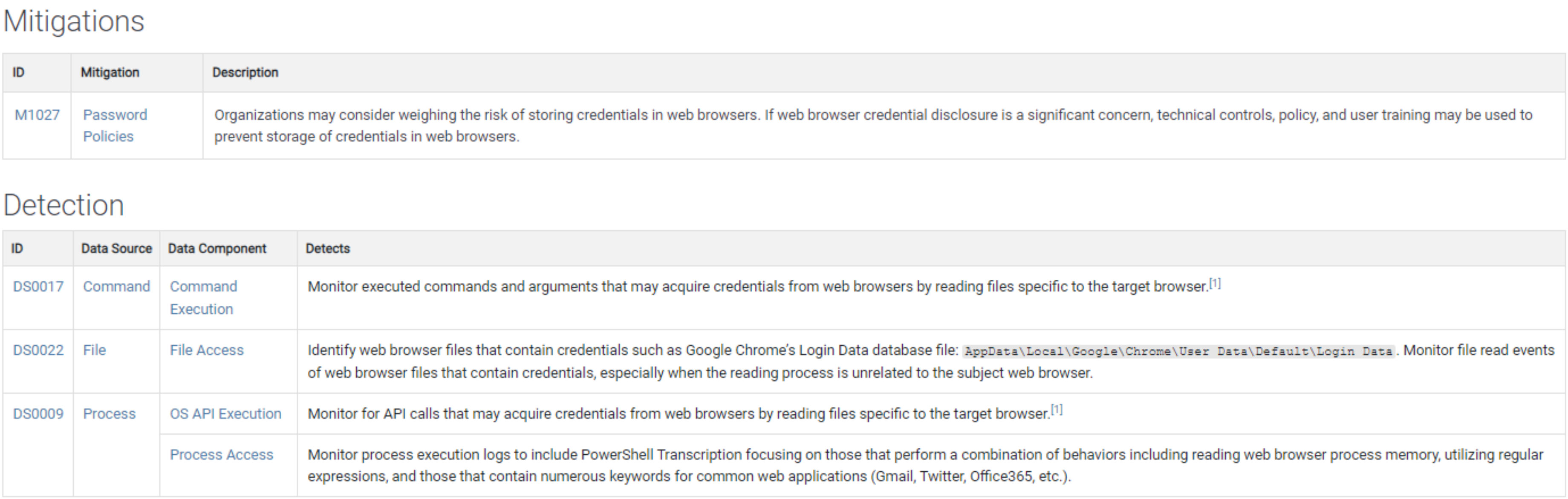
Source: https://linux.die.net/man/8/tripwire


Credentials from Password Stores (6/6)
Cloud Secrets Management Stores
Credentials from Web Browsers
Keychain
Password Managers
Securityd Memory
Windows Credential Manager



Improving using ATT&CK

- Credentials from Password Stores: Credentials from Web Browsers, Sub-technique T1555.003 - Enterprise | MITRE ATT&CK®



Mitigations

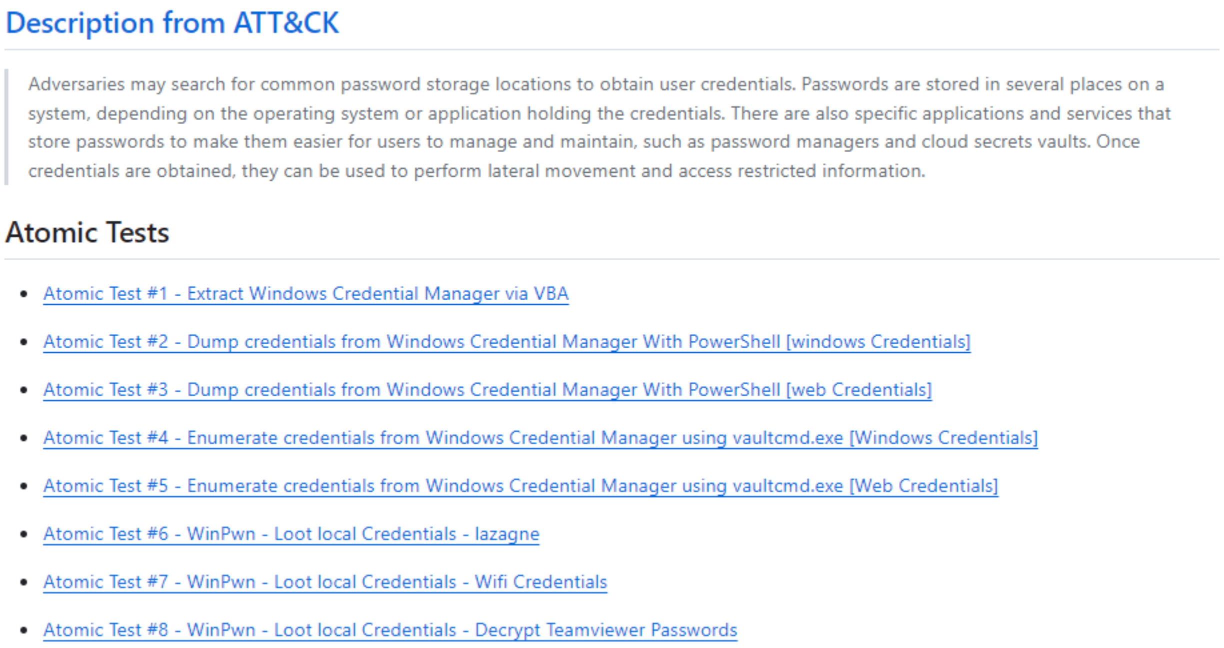
ID	Mitigation	Description
M1027	Password Policies	Organizations may consider weighing the risk of storing credentials in web browsers. If web browser credential disclosure is a significant concern, technical controls, policy, and user training may be used to prevent storage of credentials in web browsers.

Detection

ID	Data Source	Data Component	Detects
DS0017	Command	Command Execution	Monitor executed commands and arguments that may acquire credentials from web browsers by reading files specific to the target browser.[1]
DS0022	File	File Access	Identify web browser files that contain credentials such as Google Chrome's Login Data database file: `AppData\Local\Google\Chrome\User Data\Default\Login Data`. Monitor file read events of web browser files that contain credentials, especially when the reading process is unrelated to the subject web browser.
DS0009	Process	OS API Execution	Monitor for API calls that may acquire credentials from web browsers by reading files specific to the target browser.[1]
		Process Access	Monitor process execution logs to include PowerShell Transcription focusing on those that perform a combination of behaviors including reading web browser process memory, utilizing regular expressions, and those that contain numerous keywords for common web applications (Gmail, Twitter, Office365, etc.).

Improving using BAS tool documentation

- atomic-red-team/atomics/T1555/T1555.md at master · redcanaryco/atomic-red-team (github.com)



Description from ATT&CK

> Adversaries may search for common password storage locations to obtain user credentials. Passwords are stored in several places on a system, depending on the operating system or application holding the credentials. There are also specific applications and services that store passwords to make them easier for users to manage and maintain, such as password managers and cloud secrets vaults. Once credentials are obtained, they can be used to perform lateral movement and access restricted information.

Atomic Tests

- Atomic Test #1 - Extract Windows Credential Manager via VBA
- Atomic Test #2 - Dump credentials from Windows Credential Manager With PowerShell [windows Credentials]
- Atomic Test #3 - Dump credentials from Windows Credential Manager With PowerShell [web Credentials]
- Atomic Test #4 - Enumerate credentials from Windows Credential Manager using vaultcmd.exe [Windows Credentials]
- Atomic Test #5 - Enumerate credentials from Windows Credential Manager using vaultcmd.exe [Web Credentials]
- Atomic Test #6 - WinPwn - Loot local Credentials - lazagne
- Atomic Test #7 - WinPwn - Loot local Credentials - Wifi Credentials
- Atomic Test #8 - WinPwn - Loot local Credentials - Decrypt Teamviewer Passwords

Pitfalls

Learn from my mistakes, so you don’t have to

Pitfalls

Limiting yourself to the Matrix

Trying to achieve 100% coverage

Shouting "Bingo" when you have one technique

Not taking data source context into account

> “IF YOU KNOW THE **ENEMY**
> AND KNOW **YOURSELF,**
> YOU DO **NOT** NEED TO **FEAR**
> THE **RESULT** OF A
> **HUNDERED BATTLES.**”

~ Sun Tzu | The Art of War