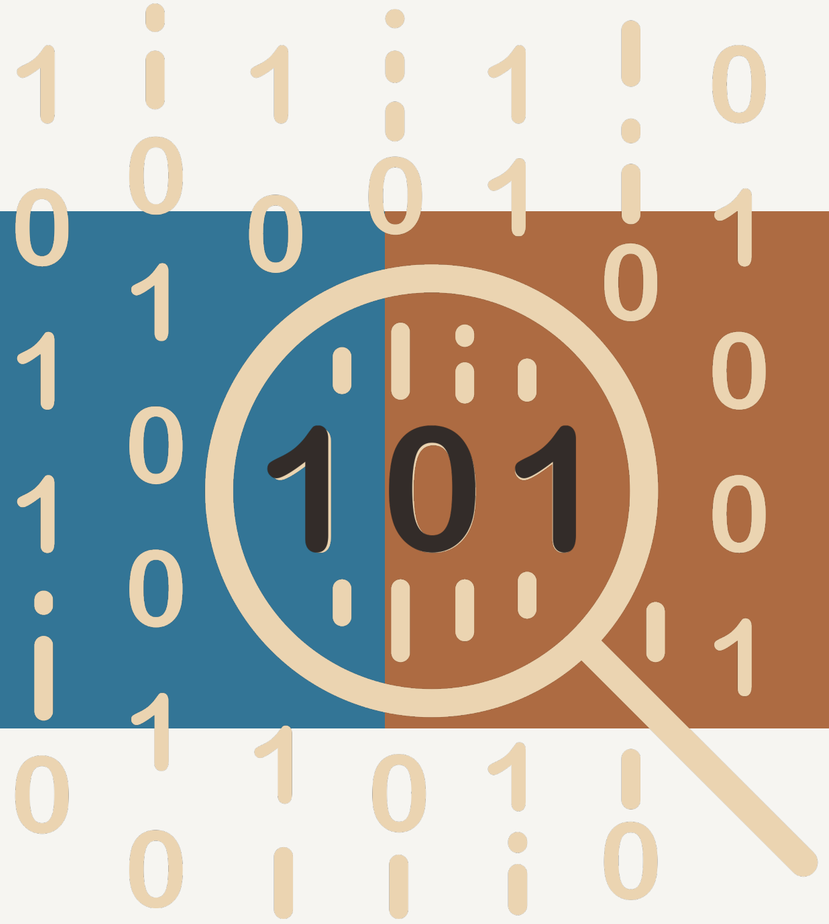
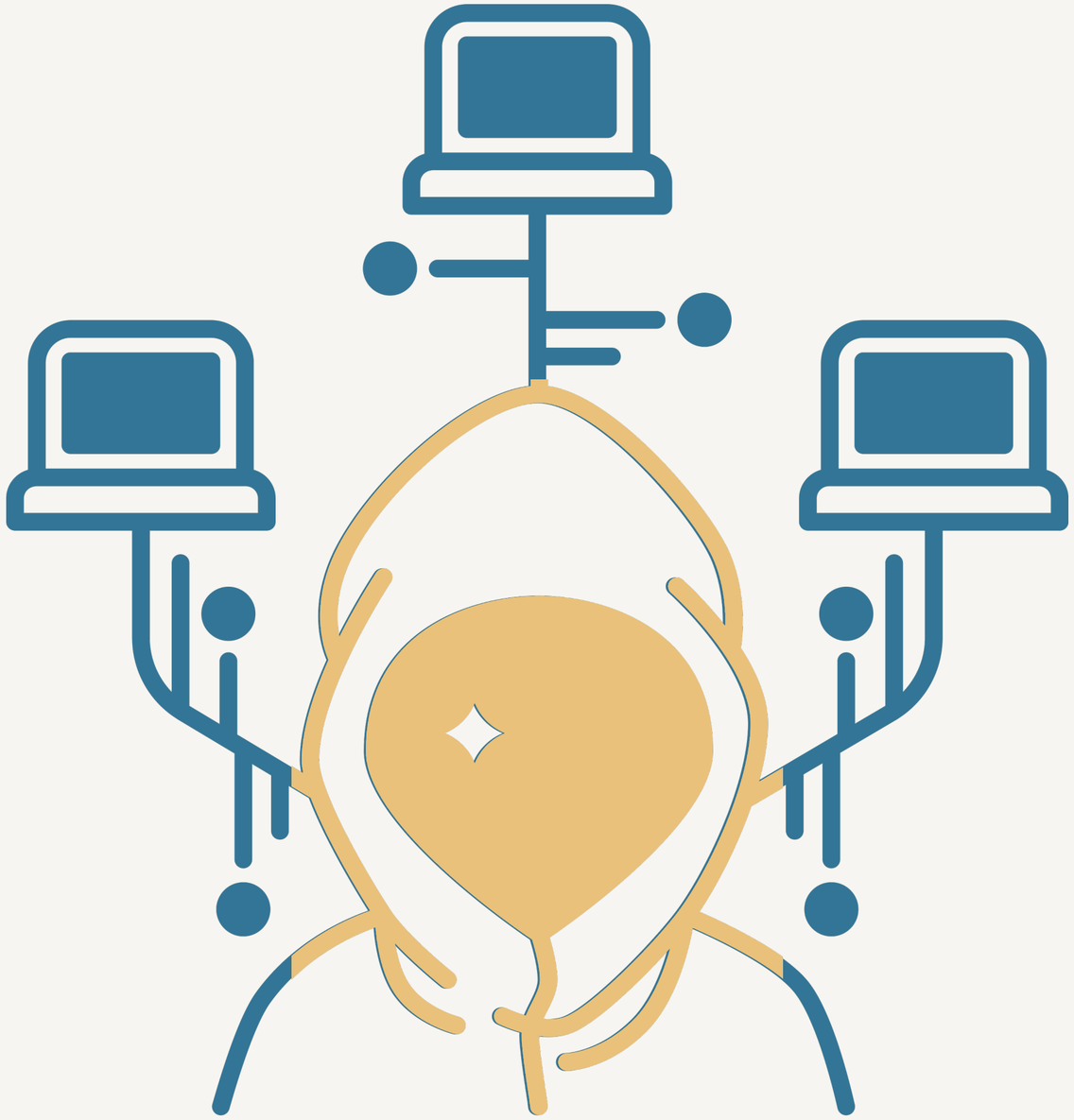
Nicole Stewart
Olga Spillane

Threat Modeling 101



2026

SECURITY
DAYS



Threat Modelling

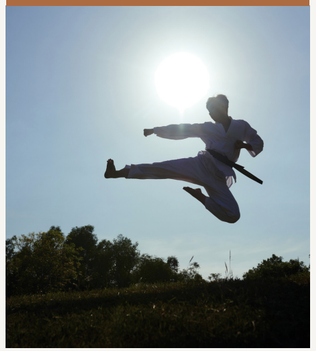
What is it?

Structured way to decode

WHO

WHY

HOW



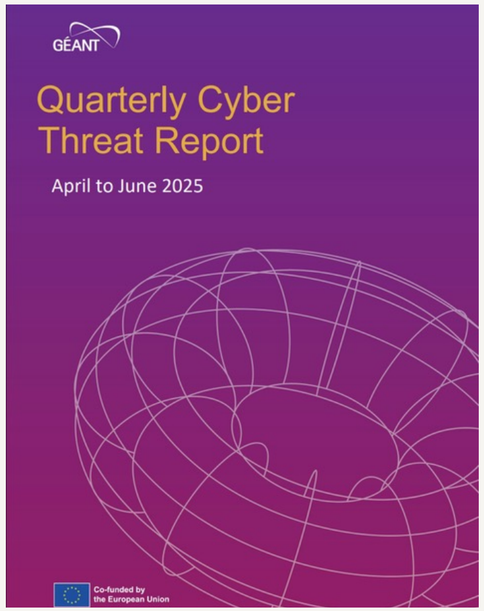
Used to

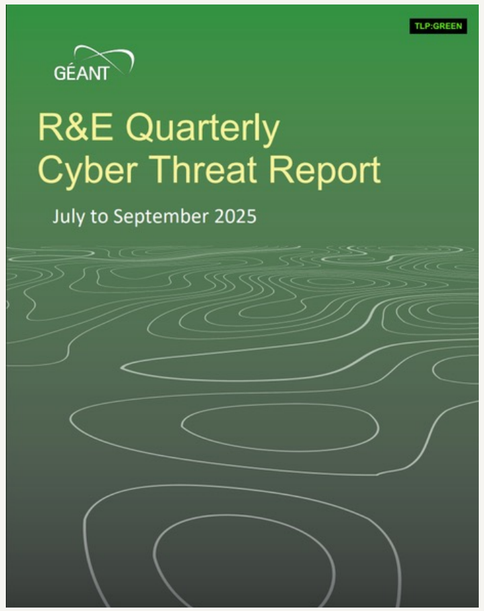
identify security threats to applications, systems, or environments

understand potential impacts on operations and security

implement controls for protection, detection, and response

Our Context – GN5-2 CTI Reports

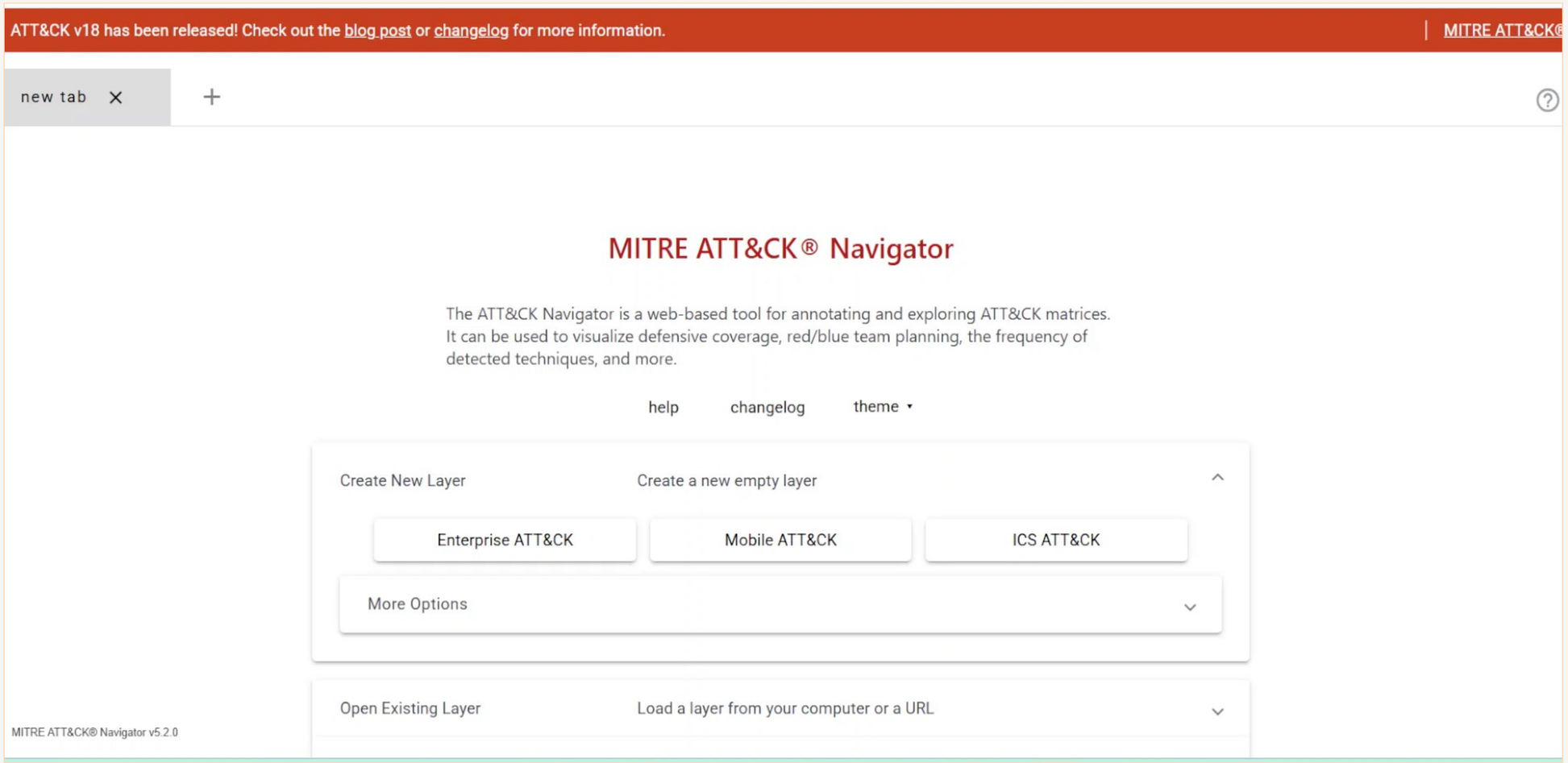




$120

ATT&CK Navigator

overlaying TTP layers



ATT&CK Navigator

threat actors targeting HE TTP mapping

TA0004: Privilege Escalation	TA0005: Defense Evasion	TA0006: Credential Access	TA0007: Discovery	TA0008: Lateral Movement
T1548: Abuse Elevation Control Mechanism	T1548: Abuse Elevation Control Mechanism	T1557: Adversary-in-the-Middle	T1087: Account Discovery	T1210: Exploitation of Remote Services
T1134: Access Token Manipulation	T1134: Access Token Manipulation	T1110: Brute Force	T1010: Application Window Discovery	T1534: Internal Spearphishing
T1098: Account Manipulation	T1197: BITS Jobs	T1555: Credentials from Password Stores	T1217: Browser Information Discovery	T1570: Lateral Tool Transfer
T1547: Boot or Logon Autostart Execution	T1612: Build Image on Host	T1212: Exploitation for Credential Access	T1580: Cloud Infrastructure Discovery	T1563: Remote Service Session Hijacking
T1037: Boot or Logon Initialization Scripts	T1622: Debugger Evasion	T1187: Forced Authentication	T1538: Cloud Service Dashboard	T1021: Remote Services
T1543: Create or Modify System Process	T1678: Delay Execution	T1606: Forge Web Credentials	T1526: Cloud Service Discovery	T1091: Replication Through Removable Media
T1484: Domain or Tenant Policy Modification	T1140: Deobfuscate/Decode Files or Information	T1056: Input Capture	T1619: Cloud Storage Object Discovery	T1072: Software Deployment Tools
T1611: Escape to Host	T1610: Deploy Container	T1556: Modify Authentication Process	T1613: Container and Resource Discovery	T1080: Taint Shared Content
T1546: Event Triggered Execution	T1006: Direct Volume Access	T1111: Multi-Factor Authentication Interception	T1622: Debugger Evasion	T1550: Use Alternate Authentication Material
T1068: Exploitation for Privilege Escalation	T1484: Domain or Tenant Policy Modification	T1621: Multi-Factor Authentication Request Generation	T1652: Device Driver Discovery	
T1574: Hijack Execution Flow	T1672: Email Spoofing	T1040: Network Sniffing	T1482: Domain Trust Discovery	
T1055: Process Injection	T1480: Execution Guardrails	T1003: OS Credential Dumping	T1083: File and Directory Discovery	
T1053: Scheduled Task/Job	T1211: Exploitation for Defense Evasion	T1528: Steal Application Access Token	T1615: Group Policy Discovery	
T1078: Valid Accounts	T1222: File and Directory Permissions Modification	T1649: Steal or Forge Authentication Certificates	T1680: Local Storage Discovery	
	T1564: Hide Artifacts	T1558: Steal or Forge Kerberos Tickets	T1654: Log Enumeration	
	T1574: Hijack Execution Flow	T1539: Steal Web Session Cookie	T1046: Network Service Discovery	
	T1562: Impair Defenses	T1552: Unsecured Credentials	T1135: Network Share Discovery	
	T1656: Impersonation		T1040: Network Sniffing	
	T1070: Indicator Removal		T1201: Password Policy Discovery	
	T1202: Indirect Command Execution		T1120: Peripheral Device Discovery	
	T1036: Masquerading		T1069: Permission Groups Discovery	
	T1556: Modify Authentication Process		T1057: Process Discovery	
	T1578: Modify Cloud Compute Infrastructure		T1012: Query Registry	
	T1666: Modify Cloud Resource Hierarchy		T1018: Remote System Discovery	
	T1112: Modify Registry		T1518: Software Discovery	
	T1601: Modify System Image		T1082: System Information Discovery	
	T1599: Network Boundary Bridging		T1614: System Location Discovery	
	T1027: Obfuscated Files or Information		T1016: System Network Configuration Discovery	
	T1647: Plist File Modification		T1049: System Network Connections Discovery	
	T1542: Pre-OS Boot		T1033: System Owner/User Discovery	
	T1055: Process Injection		T1007: System Service Discovery	
	T1620: Reflective Code Loading		T1124: System Time Discovery	
	T1207: Rogue Domain Controller		T1673: Virtual Machine Discovery	
	T1014: Rootkit		T1497: Virtualization/Sandbox Evasion	
	T1679: Selective Exclusion			
	T1553: Subvert Trust Controls			
	T1218: System Binary Proxy Execution			

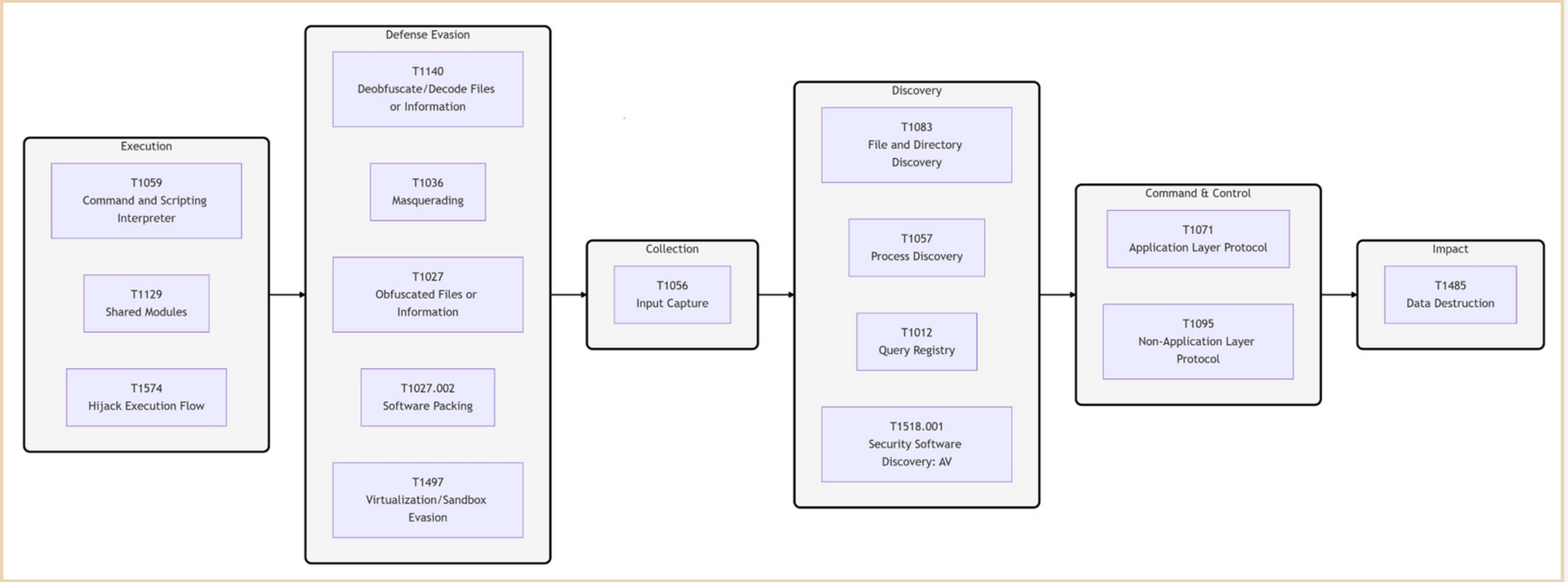
Top TTPs

most commonly used

Tactic	(Sub-)Technique	ID	Score (Occurrences)
Initial Access	Exploit Public-Facing Application	T1190	5
Defense Evasion	Impair Defenses: Disable or Modify Tools	T1562.001	4
Lateral Movement	Remote Services	T1021	4
Collection	Archive Collected Data	T1560	4
Initial Access, Persistence, Privilege Escalation, Defense Evasion	Valid Accounts	T1078	3
Execution	Windows Management Instrumentation	T1047	3
Execution	Command and Scripting Interpreter: PowerShell	T1059.001	3
Privilege Escalation, Defense Evasion	Abuse Elevation Control Mechanism: Bypass User Account Control	T1548.002	3
Defense Evasion	Impair Defenses	T1562	3
Defense Evasion	Masquerading	T1036	3

Top TTPs

used against Higher Education



Model to Action

Bridging the Gap

Operational

- Translates business risks to technical controls
- Surfaces exploitable vulnerabilities
- Shifts security config to a more targeted posture
- Maps Threat Intelligence directly to external exposures

Tactical

ATT&CK Navigator

current security posture mapping

TA0002: Execution	TA0003: Persistence	TA0004: Privilege Escalation	TA0005: Defense Evasion
T1651: Cloud Administration Command	T1098: Account Manipulation	T1548: Abuse Elevation Control Mechanism	T1548: Abuse Elevation Control Mechanism
T1059: Command and Scripting Interpreter	T1197: BITS Jobs	T1134: Access Token Manipulation	T1134: Access Token Manipulation
T1609: Container Administration Command	T1547: Boot or Logon Autostart Execution	T1547: Boot or Logon Autostart Execution	T1197: BITS Jobs
T1610: Deploy Container	T1037: Boot or Logon Initialization Scripts	T1037: Boot or Logon Initialization Scripts	T1612: Build Image on Host
T1203: Exploitation for Client Execution	T1176: Browser Extensions	T1543: Create or Modify System Process	T1622: Debugger Evasion
T1559: Inter-Process Communication	T1554: Compromise Client Software Binary	T1484: Domain Policy Modification	T1140: Deobfuscate/Decode Files or Information
T1106: Native API	T1136: Create Account	T1611: Escape to Host	T1610: Deploy Container
T1053: Scheduled Task/Job	T1543: Create or Modify System Process	T1546: Event Triggered Execution	T1006: Direct Volume Access
T1648: Serverless Execution	T1546: Event Triggered Execution	T1068: Exploitation for Privilege Escalation	T1484: Domain Policy Modification
T1129: Shared Modules	T1133: External Remote Services	T1574: Hijack Execution Flow	T1480: Execution Guardrails
T1072: Software Deployment Tools	T1574: Hijack Execution Flow	T1055: Process Injection	T1211: Exploitation for Defense Evasion
T1569: System Services	T1525: Implant Internal Image	T1053: Scheduled Task/Job	T1222: File and Directory Permissions Modification
T1204: User Execution	T1556: Modify Authentication Process	T1078: Valid Accounts	T1564: Hide Artifacts

Key Recommendations

based on Top TTPs

1. M1026 – Privileged Account Management
2. M1018 – User Account Management
3. M1047 – Audit
4. M1038 – Execution Prevention
5. M1027 – Password Policies
6. M1028 – Operating System Configuration
7. M1035 – Limit Access to Resource Over Network
8. M1040 – Behavior Prevention on Endpoint
9. M1042 – Disable or Remove Feature or Program
10. M1017 – User Training
11. M1032 – Multi-factor Authentication
12. M1051 – Update Software

Privileged Account Management – M1026

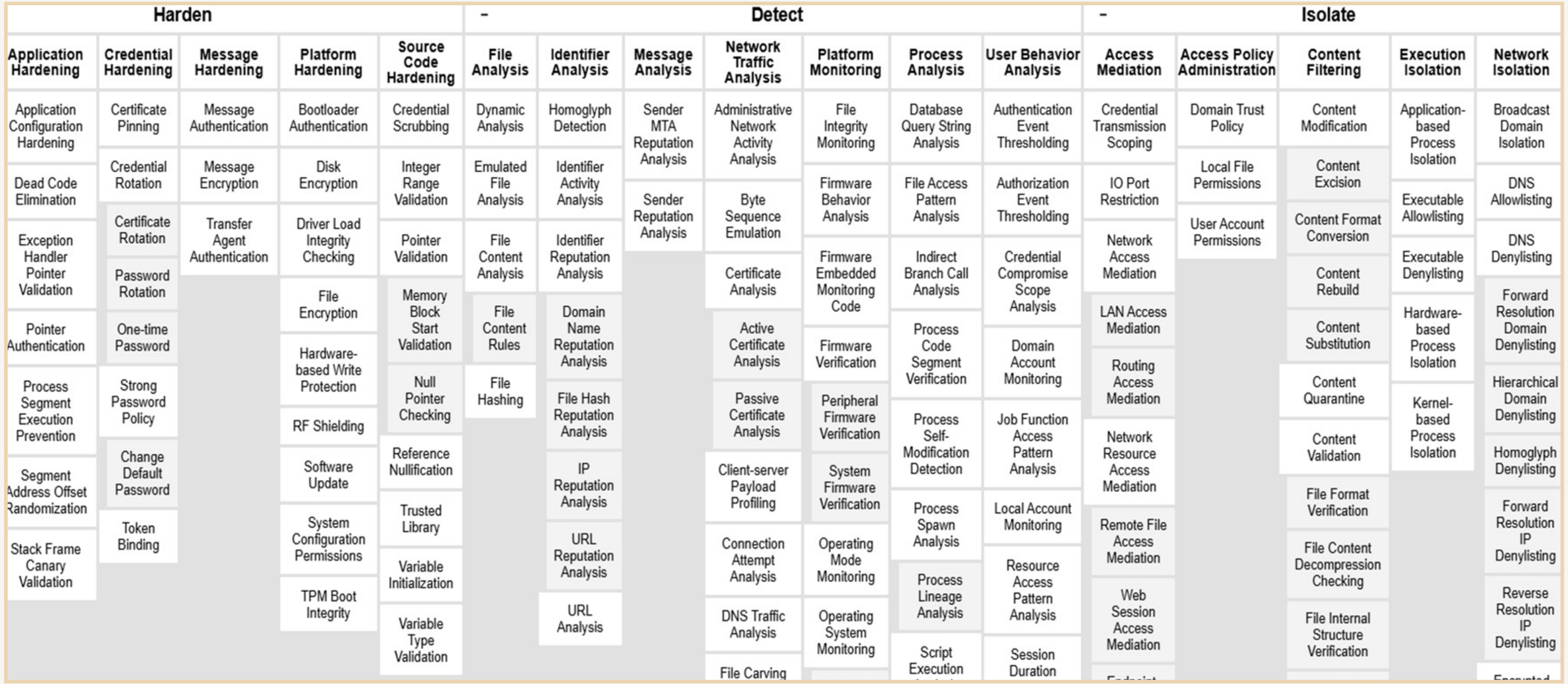
Mitigates (sub-)techniques: T1078, T1021.001, T1021.002, T1555, T1047, T1548.002, T1190, T1059.001, T1003

Privileged Account Management focuses on implementing policies, controls, and tools to securely manage privileged accounts (e.g., SYSTEM, root, or administrative accounts). This includes restricting access, limiting the scope of permissions, monitoring privileged account usage, and ensuring accountability through logging and auditing. This mitigation can be implemented through the following selected measures:[54]

- Routinely audit domain and local accounts as well as their permission levels to look for situations that could allow an adversary to gain wide access by obtaining credentials of a privileged account.[55] [56] These audits should also check for unauthorized new local account creation and whether default accounts have been enabled.
- Follow enterprise-network design and administration best practices to limit privileged account use across administrative tiers.[57]

MITRE D3FEND

knowledge graph of security countermeasures



MITRE D3FEND

Linking Attack Techniques to Countermeasures

ATT&CK ID	ATT&CK Name	Related D3FEND Techniques					
T1057	Process Discovery	may-invoke	Create Process	Detect	Process Spawn Analysis	analyzes	Create Process
		may-invoke	Create Process	Detect	System Call Analysis	analyzes	System Call
		may-invoke	Create Process	Isolate	Hardware-based Process Isolation	restricts	Create Process
		may-invoke	Create Process	Isolate	Executable Denylisting	filters	Create Process
		may-invoke	Create Process	Isolate	Executable Allowlisting	filters	Create Process
		may-invoke	Create Process	Isolate	System Call Filtering	filters	System Call
T1012	Query Registry	accesses	System Configuration Database	Model	Data Inventory	inventories	Database
		accesses	System Configuration Database	Restore	Restore Database	restores	Database
		may-invoke	Get System Config Value	Detect	System Call Analysis	analyzes	System Call
		accesses	System Configuration Database	Harden	System Configuration Permissions	restricts	System Configuration Database
		may-invoke	Get System Config Value	Isolate	System Call Filtering	filters	System Call

MITRE D3FEND

Linking Attack Techniques to Countermeasures

ATT&CK Mapping

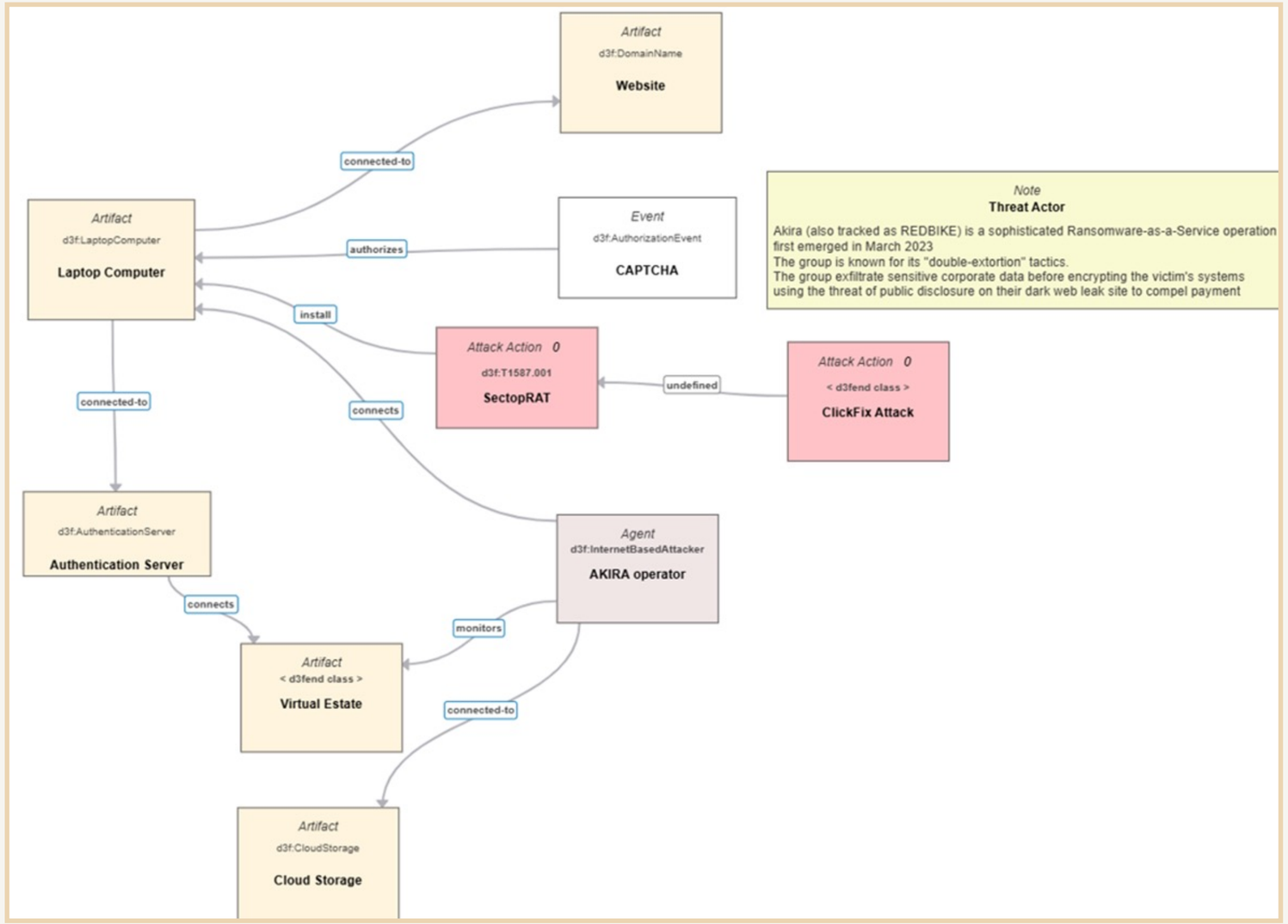
ATT&CK ID	ATT&CK Name
T1057	Process Discovery

Related D3FEND Techniques

Technique ID	Technique Name	Objective	Analysis Type	Description	Link
may-invoke	Create Process	Detect	Process Spawn Analysis	analyzes	Create Process

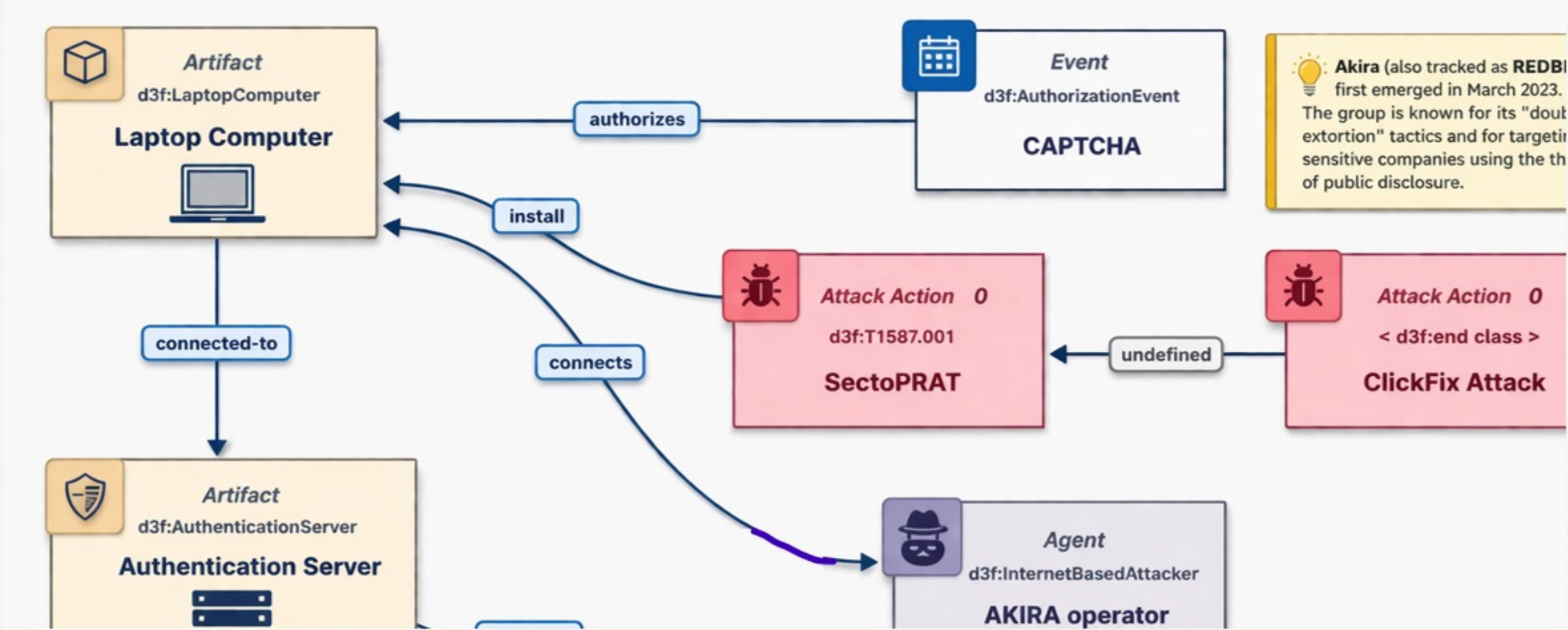
MITRE D3FEND

realisation of the D3FEND ontology



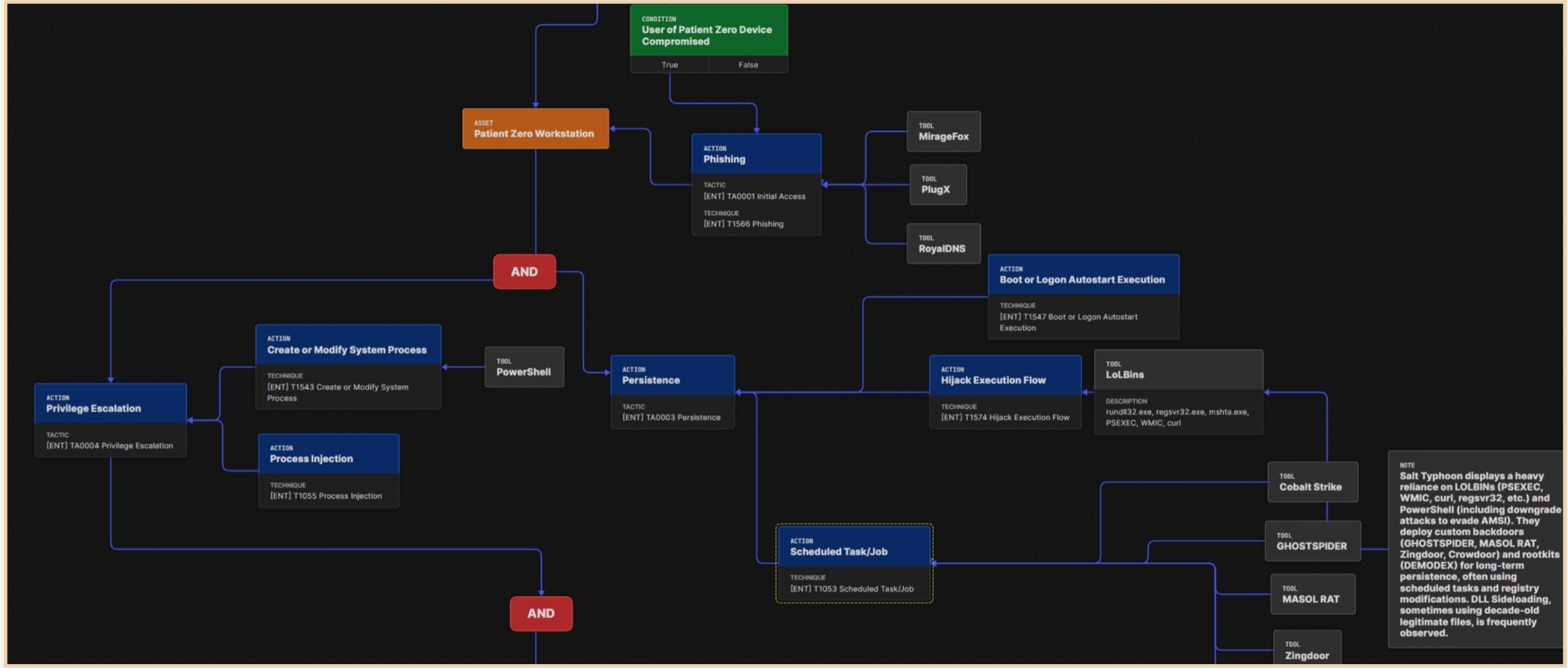
MITRE D3FEND

realisation of the D3FEND ontology



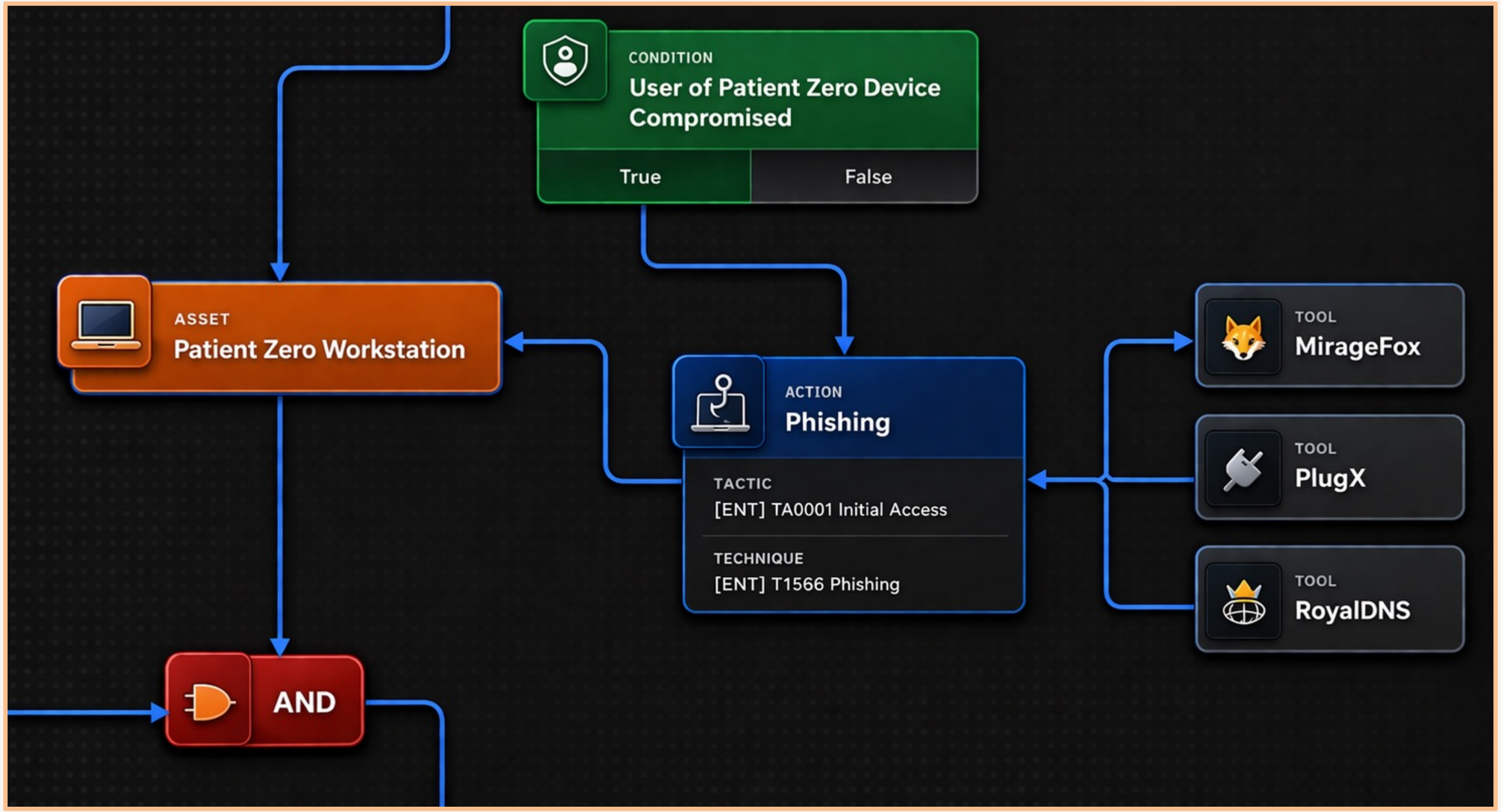
MITRE Attack Flow

targeting strategic assets and environments



MITRE Attack Flow

targeting strategic assets and environments



Key Takeaways

Use ATT&CK to structure CTI reporting

Use D3FEND to link threats to defences

Use Attack Flow to reason about adversary behaviour