SEB

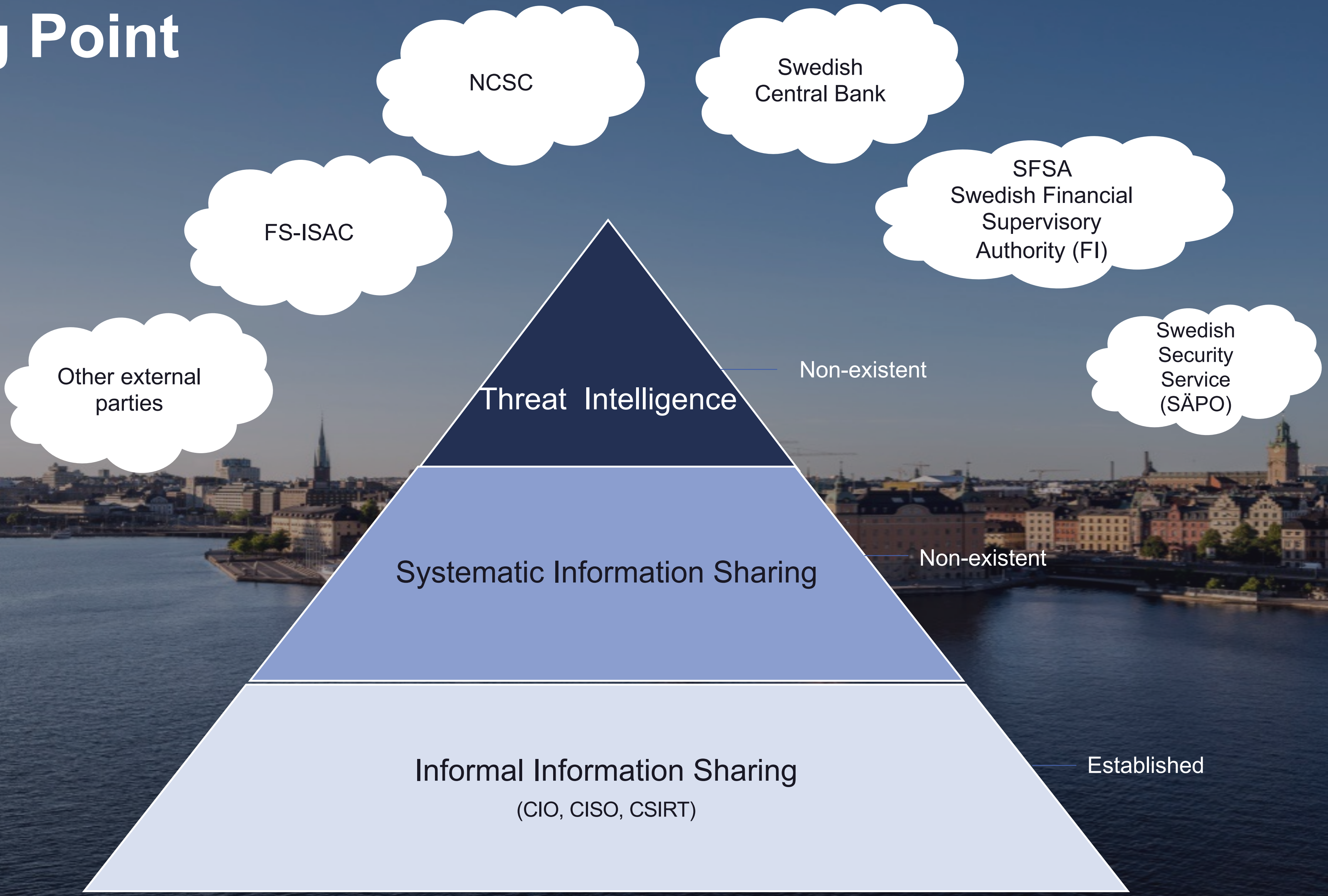
Swedbank

Handelsbanken

Cyber Security Collaboration

Sofia Nacke (SEB), Caroline Gustavsson (Handelsbanken) and Petra Klein (Swedbank)

Starting Point



NCSC

Swedish Central Bank

FS-ISAC

SFSA
Swedish Financial Supervisory Authority (FI)

Other external parties

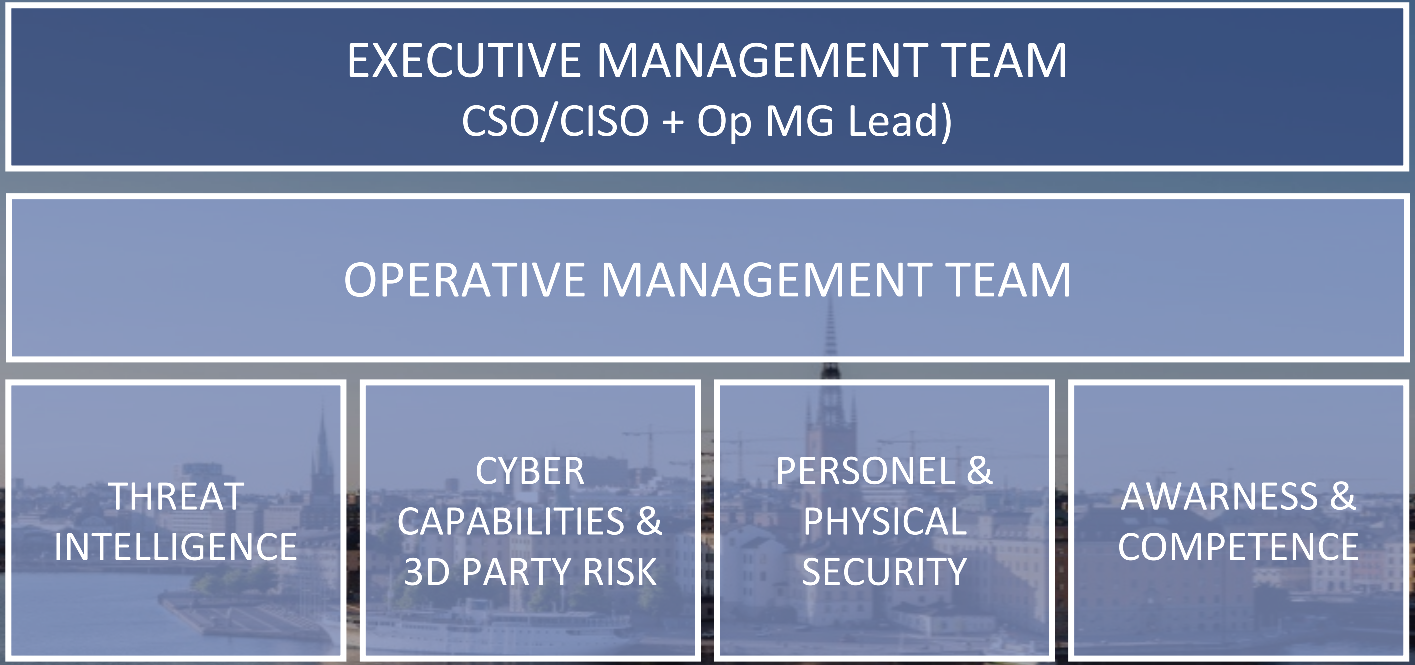
Swedish Security Service (SÄPO)

Threat Intelligence — Non-existent

Systematic Information Sharing — Non-existent

Informal Information Sharing
(CIO, CISO, CSIRT) — Established

Governance



EXECUTIVE MANAGEMENT TEAM
CSO/CISO + Op MG Lead)

OPERATIVE MANAGEMENT TEAM

THREAT INTELLIGENCE

CYBER CAPABILITIES & 3D PARTY RISK

PERSONEL & PHYSICAL SECURITY

AWARNESS & COMPETENCE

- Bi-weekly meetings (physical)
- Lead of each area distributed between SEB, Swedbank & Handelsbanken
- The leaders for each area are members of the operative management team

Collaboration public – private sector

National Cyber Security Centre
(SE-NCSC)

2021, SE-NCSC established by FRA, Försvarsmakten, MSB and Säkerhetspolisen, in close collaboration with PTS, FMV and Polismyndigheten

2022, finance pilot

SE-NCSC and the financial sector

1/7 New head, FRA; improves governance

Working Groups within the Cyber Security Collaboration

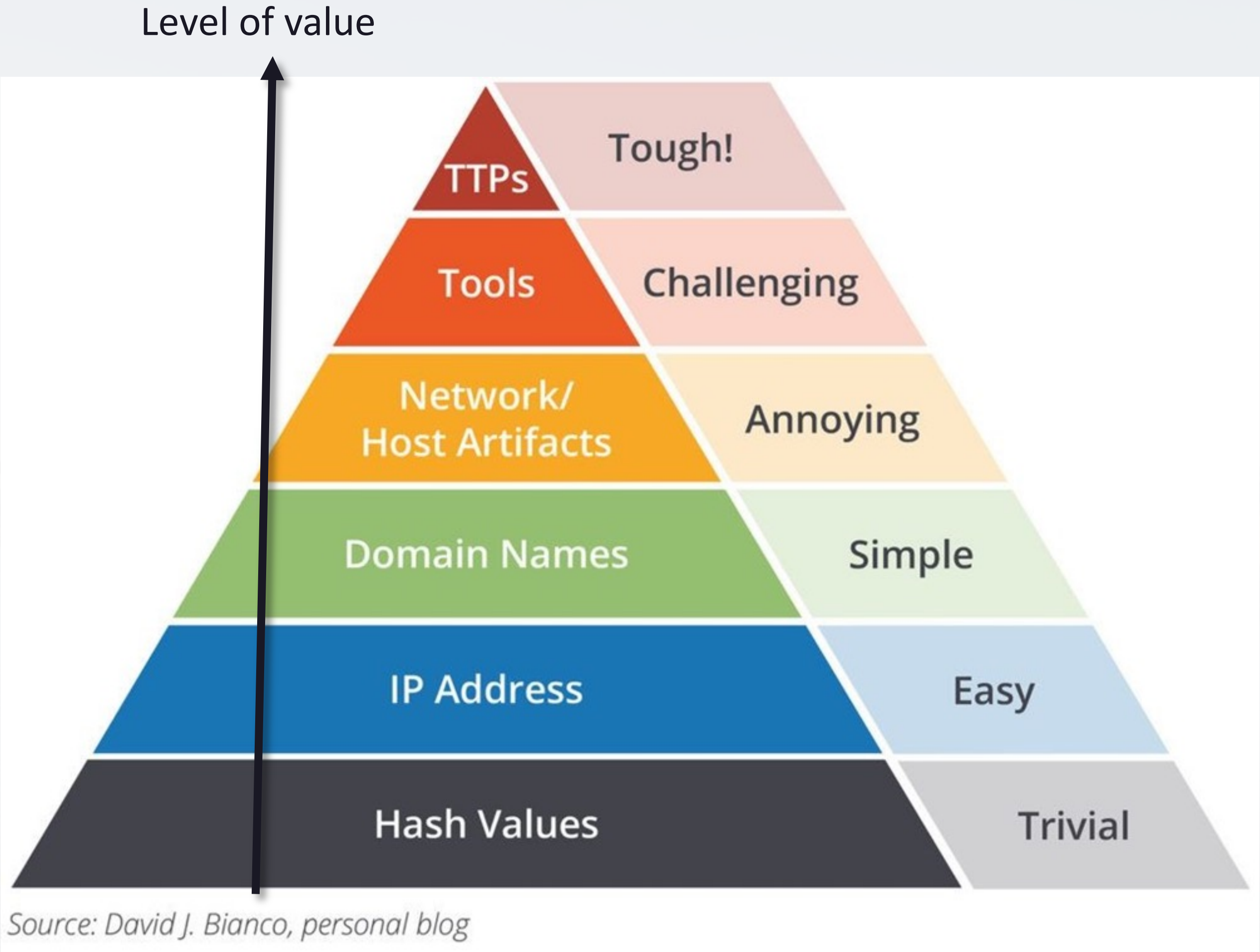
OPERATIVE MANAGEMENT TEAM	• Transfer from project to line organization • Update of collaboration agreement • NCSC
THREAT INTELLIGENCE	• Formalize Threat Intel meetings within the sector • POC Information Sharing Platform (MISP) • Heatmap based on MITRE
CYBER CAPABILITIES & 3D PARTY RISK	• Future Management System for the financial sector (ISMS) • 3d party security requirements • Secure Coding • DDoS and Ransomware Whitepaper
PERSONEL & PHYSICAL SECURITY	• Insider Threat
AWARNESS & COMPETENCE	• Define Communication Plan • Joint security awareness activities with external inspirational speakers, employees in all 3 banks are invited

Collaboration with **MITRE ATT&CK** – A method for threat- and data-driven prioritization of Cyber defence in the Swedish finance sector.

The challenge – Information sharing on threats between public and private sectors

The solution – Pivoting from talking about threats actors to instead focusing on their tactics and techniques

Why not just share IOC:s?



Source: David J. Bianco, personal blog

”The Pyramid of Pain”

The tool – A common and known framework

ATT&CK®

https://attack.mitre.org/

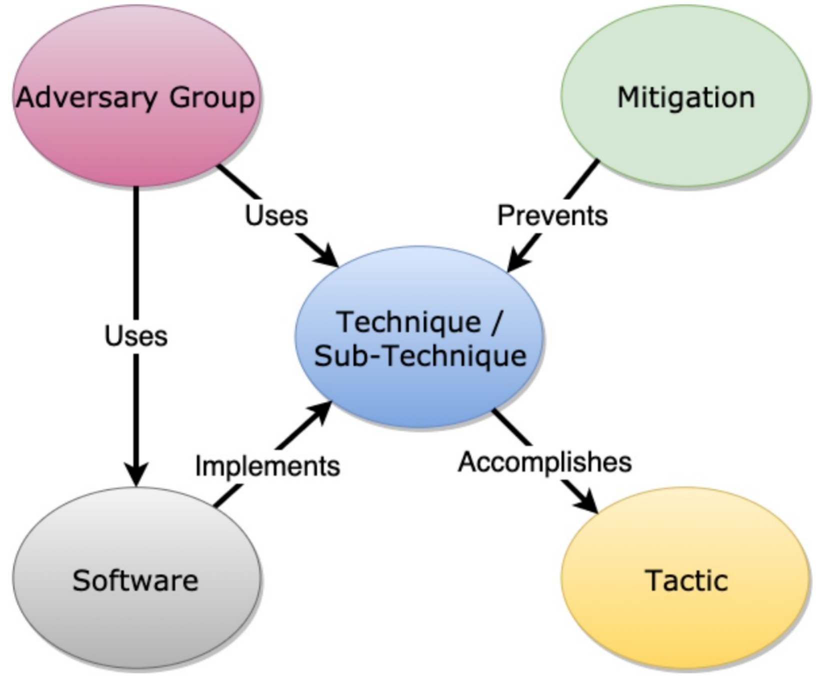
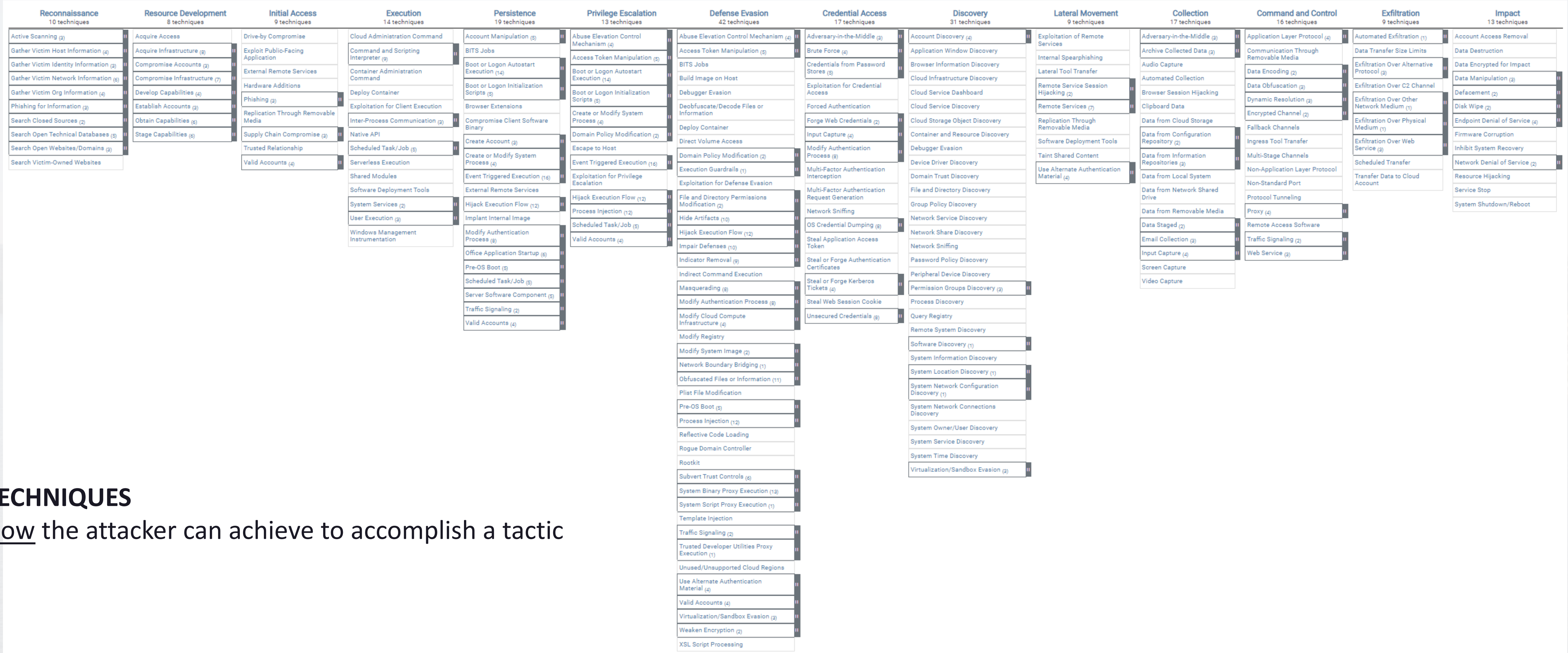


Figure 3. ATT&CK Model Relationships

The tool – A common and known framework

(MITRE killchain) **TACTICS,** What the attacker needs to achieve its objective



Reconnaissance
10 techniques

- Active Scanning (3)
- Gather Victim Host Information (4)
- Gather Victim Identity Information (3)
- Gather Victim Network Information (6)
- Gather Victim Org Information (4)
- Phishing for Information (3)
- Search Closed Sources (2)
- Search Open Technical Databases (5)
- Search Open Websites/Domains (3)
- Search Victim-Owned Websites

Resource Development
8 techniques

- Acquire Access
- Acquire Infrastructure (8)
- Compromise Accounts (3)
- Compromise Infrastructure (7)
- Develop Capabilities (4)
- Establish Accounts (3)
- Obtain Capabilities (6)
- Stage Capabilities (6)

Initial Access
9 techniques

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

Execution
14 techniques

- Cloud Administration Command
- Command and Scripting Interpreter (9)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (3)
- Native API
- Scheduled Task/Job (5)
- Serverless Execution
- Shared Modules
- Software Deployment Tools
- System Services (2)
- User Execution (3)
- Windows Management Instrumentation

Persistence
19 techniques

- Account Manipulation (5)
- BITS Jobs
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (3)
- Create or Modify System Process (4)
- Event Triggered Execution (16)
- External Remote Services
- Hijack Execution Flow (12)
- Implant Internal Image
- Modify Authentication Process (8)
- Office Application Startup (6)
- Pre-OS Boot (5)
- Scheduled Task/Job (5)
- Server Software Component (5)
- Traffic Signaling (2)
- Valid Accounts (4)

Privilege Escalation
13 techniques

- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Create or Modify System Process (4)
- Domain Policy Modification (2)
- Escape to Host
- Event Triggered Execution (16)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (12)
- Process Injection (12)
- Scheduled Task/Job (5)
- Valid Accounts (4)

Defense Evasion
42 techniques

- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (2)
- Execution Guardrails (1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (2)
- Hide Artifacts (10)
- Hijack Execution Flow (12)
- Impair Defenses (10)
- Indicator Removal (9)
- Indirect Command Execution
- Masquerading (8)
- Modify Authentication Process (8)
- Modify Cloud Compute Infrastructure (4)
- Modify Registry
- Modify System Image (2)
- Network Boundary Bridging (1)
- Obfuscated Files or Information (11)
- Plist File Modification
- Pre-OS Boot (5)
- Process Injection (12)
- Reflective Code Loading
- Rogue Domain Controller
- Rootkit
- Subvert Trust Controls (6)
- System Binary Proxy Execution (13)
- System Script Proxy Execution (1)
- Template Injection
- Traffic Signaling (2)
- Trusted Developer Utilities Proxy Execution (1)
- Unused/Unsupported Cloud Regions
- Use Alternate Authentication Material (4)
- Valid Accounts (4)
- Virtualization/Sandbox Evasion (3)
- Weaken Encryption (2)
- XSL Script Processing

Credential Access
17 techniques

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

Discovery
31 techniques

- Account Discovery (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
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (1)
- System Information Discovery
- System Location Discovery (1)
- System Network Configuration Discovery (1)
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion (3)

Lateral Movement
9 techniques

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

Collection
17 techniques

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

Command and Control
16 techniques

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

Exfiltration
9 techniques

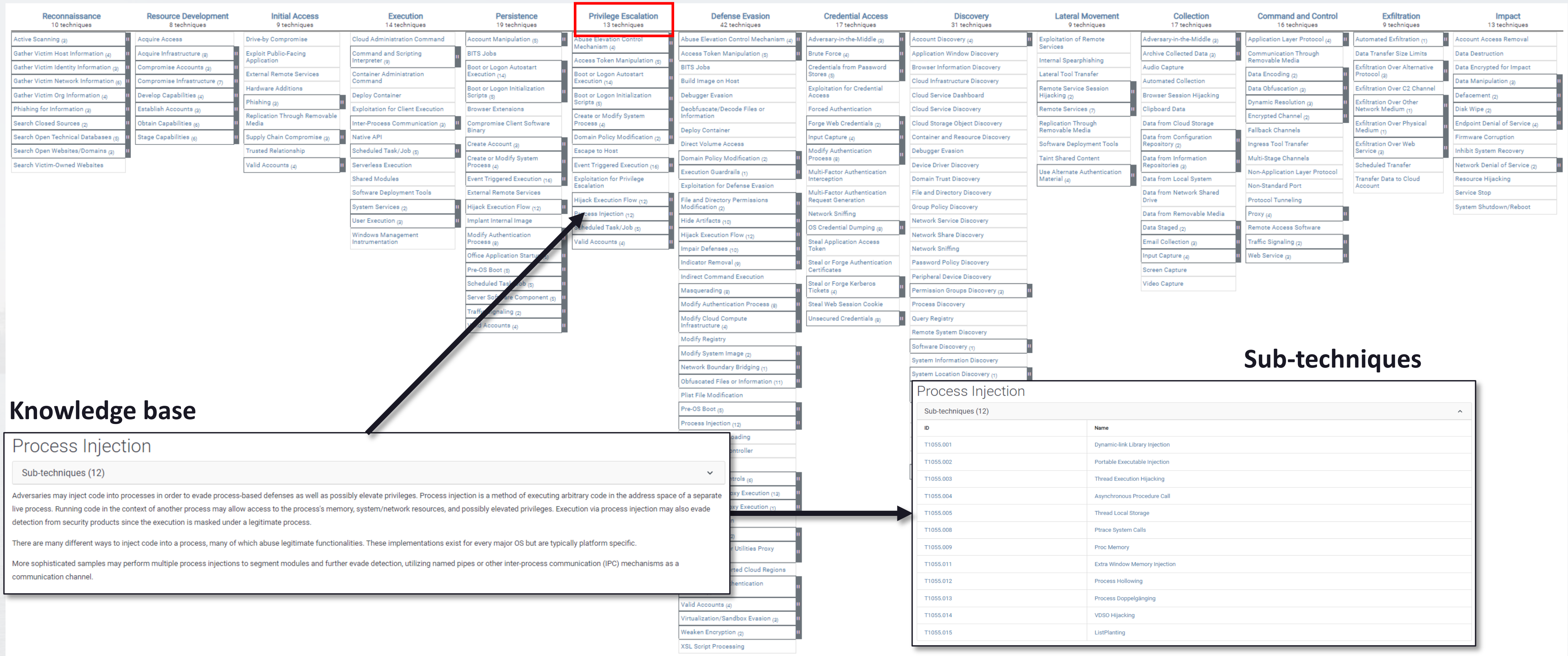
- Automated Exfiltration (1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (1)
- Exfiltration Over Physical Medium (1)
- Exfiltration Over Web Service (3)
- Scheduled Transfer
- Transfer Data to Cloud Account

Impact
13 techniques

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

TECHNIQUES

How the attacker can achieve to accomplish a tactic



Reconnaissance
10 techniques

- Active Scanning (3)
- Gather Victim Host Information (4)
- Gather Victim Identity Information (3)
- Gather Victim Network Information (6)
- Gather Victim Org Information (4)
- Phishing for Information (3)
- Search Closed Sources (2)
- Search Open Technical Databases (5)
- Search Open Websites/Domains (3)
- Search Victim-Owned Websites

Resource Development
8 techniques

- Acquire Access
- Acquire Infrastructure (8)
- Compromise Accounts (3)
- Compromise Infrastructure (7)
- Develop Capabilities (4)
- Establish Accounts (3)
- Obtain Capabilities (6)
- Stage Capabilities (6)

Initial Access
9 techniques

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

Execution
14 techniques

- Cloud Administration Command
- Command and Scripting Interpreter (9)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (3)
- Native API
- Scheduled Task/Job (5)
- Serverless Execution
- Shared Modules
- Software Deployment Tools
- System Services (2)
- User Execution (3)
- Windows Management Instrumentation

Persistence
19 techniques

- Account Manipulation (5)
- BITS Jobs
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (3)
- Create or Modify System Process (4)
- Event Triggered Execution (16)
- External Remote Services
- Hijack Execution Flow (12)
- Implant Internal Image
- Modify Authentication Process (8)
- Office Application Startup (6)
- Pre-OS Boot (5)
- Scheduled Task/Job (5)
- Server Software Component (5)
- Traffic Signaling (2)
- Valid Accounts (4)

Privilege Escalation
13 techniques

- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Create or Modify System Process (4)
- Domain Policy Modification (2)
- Escape to Host
- Event Triggered Execution (16)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (12)
- Process Injection (12)
- Scheduled Task/Job (5)
- Valid Accounts (4)

Defense Evasion
42 techniques

- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (2)
- Execution Guardrails (1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (2)
- Hide Artifacts (10)
- Hijack Execution Flow (12)
- Impair Defenses (10)
- Indicator Removal (9)
- Indirect Command Execution
- Masquerading (8)
- Modify Authentication Process (8)
- Modify Cloud Compute Infrastructure (4)
- Modify Registry
- Modify System Image (2)
- Network Boundary Bridging (1)
- Obfuscated Files or Information (11)
- Plist File Modification
- Pre-OS Boot (5)
- Process Injection (12)
- oading
- ontroller
- ntrols (6)
- oxy Execution (13)
- xy Execution (1)
- n
- 2)
- r Utilities Proxy
- rted Cloud Regions
- hentication
- Valid Accounts (4)
- Virtualization/Sandbox Evasion (3)
- Weaken Encryption (2)
- XSL Script Processing

Credential Access
17 techniques

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

Discovery
31 techniques

- Account Discovery (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
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (1)
- System Information Discovery
- System Location Discovery (1)

Lateral Movement
9 techniques

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

Collection
17 techniques

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

Command and Control
16 techniques

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

Exfiltration
9 techniques

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

Impact
13 techniques

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

Sub-techniques

Process Injection

Sub-techniques (12)

ID	Name
T1055.001	Dynamic-link Library Injection
T1055.002	Portable Executable Injection
T1055.003	Thread Execution Hijacking
T1055.004	Asynchronous Procedure Call
T1055.005	Thread Local Storage
T1055.008	Ptrace System Calls
T1055.009	Proc Memory
T1055.011	Extra Window Memory Injection
T1055.012	Process Hollowing
T1055.013	Process Doppelgänging
T1055.014	VDSO Hijacking
T1055.015	ListPlanting

Knowledge base

Process Injection

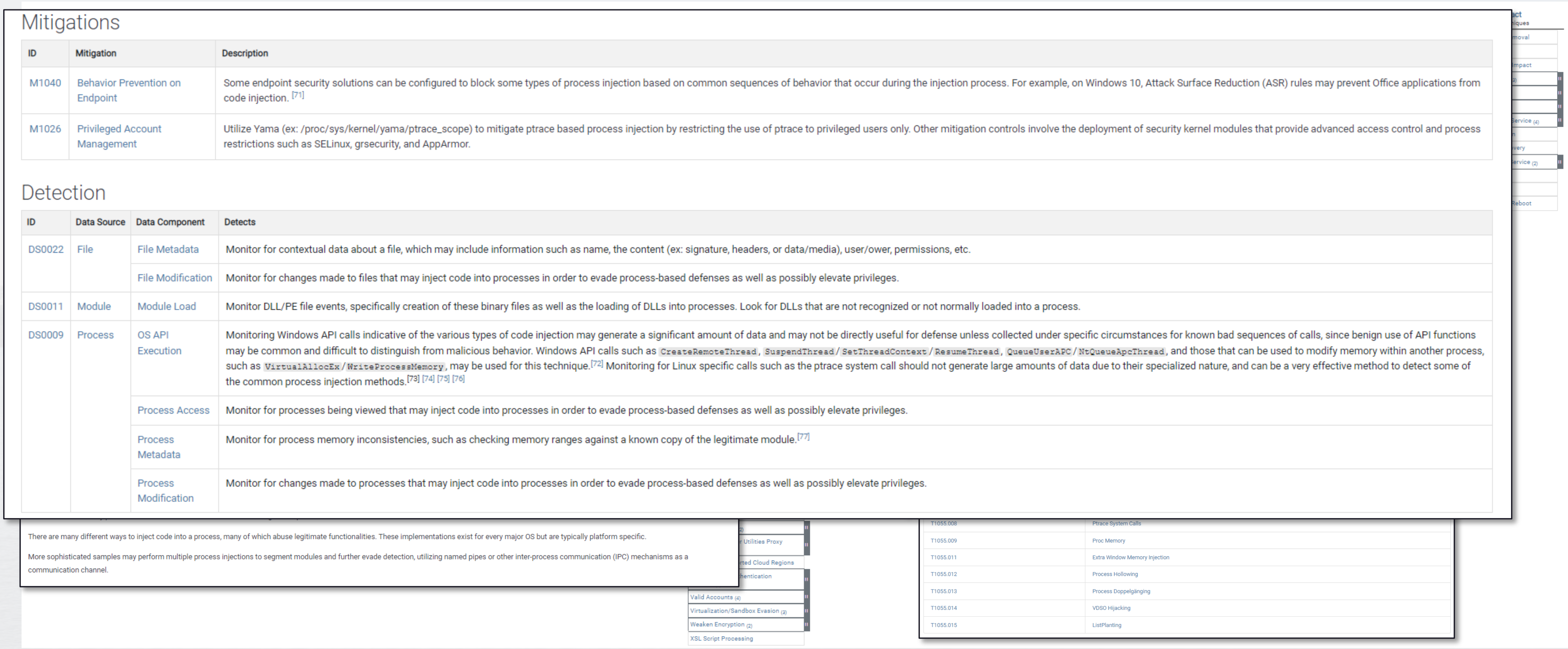
Sub-techniques (12)

Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process.

There are many different ways to inject code into a process, many of which abuse legitimate functionalities. These implementations exist for every major OS but are typically platform specific.

More sophisticated samples may perform multiple process injections to segment modules and further evade detection, utilizing named pipes or other inter-process communication (IPC) mechanisms as a communication channel.

Mitigations and Detections



Mitigations

ID	Mitigation	Description
M1040	Behavior Prevention on Endpoint	Some endpoint security solutions can be configured to block some types of process injection based on common sequences of behavior that occur during the injection process. For example, on Windows 10, Attack Surface Reduction (ASR) rules may prevent Office applications from code injection. [71]
M1026	Privileged Account Management	Utilize Yama (ex: /proc/sys/kernel/yama/ptrace_scope) to mitigate ptrace based process injection by restricting the use of ptrace to privileged users only. Other mitigation controls involve the deployment of security kernel modules that provide advanced access control and process restrictions such as SELinux, grsecurity, and AppArmor.

Detection

ID	Data Source	Data Component	Detects
DS0022	File	File Metadata	Monitor for contextual data about a file, which may include information such as name, the content (ex: signature, headers, or data/media), user/ower, permissions, etc.
		File Modification	Monitor for changes made to files that may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges.
DS0011	Module	Module Load	Monitor DLL/PE file events, specifically creation of these binary files as well as the loading of DLLs into processes. Look for DLLs that are not recognized or not normally loaded into a process.
DS0009	Process	OS API Execution	Monitoring Windows API calls indicative of the various types of code injection may generate a significant amount of data and may not be directly useful for defense unless collected under specific circumstances for known bad sequences of calls, since benign use of API functions may be common and difficult to distinguish from malicious behavior. Windows API calls such as `CreateRemoteThread`, `SuspendThread` / `SetThreadContext` / `ResumeThread`, `QueueUserAPC` / `NtQueueApcThread`, and those that can be used to modify memory within another process, such as `VirtualAllocEx` / `WriteProcessMemory`, may be used for this technique.[72] Monitoring for Linux specific calls such as the ptrace system call should not generate large amounts of data due to their specialized nature, and can be a very effective method to detect some of the common process injection methods.[73] [74] [75] [76]
		Process Access	Monitor for processes being viewed that may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges.
		Process Metadata	Monitor for process memory inconsistencies, such as checking memory ranges against a known copy of the legitimate module.[77]
		Process Modification	Monitor for changes made to processes that may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges.

There are many different ways to inject code into a process, many of which abuse legitimate functionalities. These implementations exist for every major OS but are typically platform specific.

More sophisticated samples may perform multiple process injections to segment modules and further evade detection, utilizing named pipes or other inter-process communication (IPC) mechanisms as a communication channel.

Valid Accounts (4)
Virtualization/Sandbox Evasion (3)
Weaken Encryption (2)
XSL Script Processing

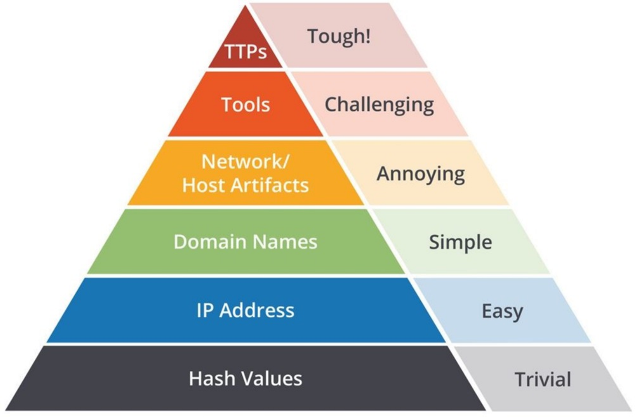
T1055.008	Ptrace System Calls
T1055.009	Proc Memory
T1055.011	Extra Window Memory Injection
T1055.012	Process Hollowing
T1055.013	Process Doppelgänging
T1055.014	VDSO Hijacking
T1055.015	ListPlanting

The process

Step 1 – Establish a joint threat model

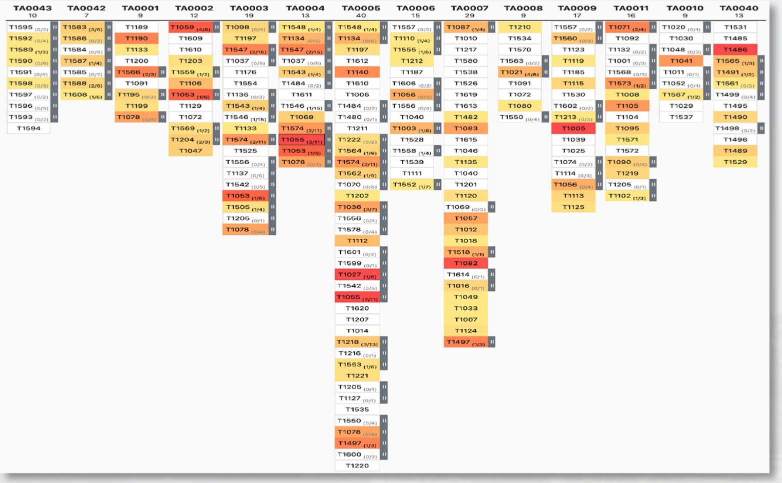
Intermediate product– list of threat actors

Step 2 – Fusion of Threat actor (TA) with TTPs in their activities



Source: David J. Bianco, personal blog

Step 3 – Create a heatmap of frequency of TA use of TTPs



TA0043	TA0042	TA0001	TA0002	TA0003	TA0004	TA0005	TA0006	TA0007	TA0008	TA0009	TA0011	TA0010	TA0040
10	7	9	12	19	13	40	15	29	9	17	16	9	13
T1595 (0/2)	T1583 (3/6)	T1189	T1059 (4/8)	T1098 (0/4)	T1548 (1/4)	T1548 (1/4)	T1557 (0/2)	T1087 (1/4)	T1210	T1557 (0/2)	T1071 (2/4)	T1020 (0/1)	T1531
T1592 (0/4)	T1586 (0/2)	T1190	T1609	T1197	T1134 (0/5)	T1134 (0/5)	T1110 (1/4)	T1010	T1534	T1560 (0/3)	T1092	T1030	T1485
T1589 (1/3)	T1584 (0/6)	T1133	T1610	T1547 (2/15)	T1547 (2/15)	T1197	T1555 (1/5)	T1217	T1570	T1123	T1132 (0/2)	T1048 (0/3)	T1486
T1590 (0/6)	T1587 (1/4)	T1200	T1203	T1037 (0/5)	T1037 (0/5)	T1612	T1212	T1580	T1563 (0/2)	T1119	T1001 (0/3)	T1041	T1565 (1/3)
T1591 (0/4)	T1585 (0/2)	T1566 (2/3)	T1559 (1/2)	T1176	T1543 (1/4)	T1140	T1187	T1538	T1021 (4/6)	T1185	T1568 (0/3)	T1011 (0/1)	T1491 (1/2)
T1598 (0/3)	T1588 (2/6)	T1091	T1106	T1554	T1484 (0/2)	T1610	T1606 (0/2)	T1526	T1091	T1115	T1573 (1/2)	T1052 (0/1)	T1561 (0/2)
T1597 (0/2)	T1608 (1/5)	T1195 (0/3)	T1053 (1/6)	T1136 (0/3)	T1611	T1006	T1056 (0/4)	T1619	T1072	T1530	T1008	T1567 (1/2)	T1499 (0/4)
T1596 (0/5)		T1199	T1129	T1543 (1/4)	T1546 (1/15)	T1484 (0/2)	T1556 (0/4)	T1613	T1080	T1602 (0/2)	T1105	T1029	T1495
T1593 (0/2)		T1078 (0/4)	T1072	T1546 (1/15)	T1068	T1480 (0/1)	T1040	T1482	T1550 (0/4)	T1213 (0/3)	T1104	T1537	T1490
T1594			T1569 (1/2)	T1133	T1574 (2/11)	T1211	T1003 (1/8)	T1083		T1005	T1095		T1498 (0/2)
			T1204 (2/3)	T1574 (2/11)	T1055 (2/11)	T1222 (0/2)	T1528	T1615		T1039	T1571		T1496
			T1047	T1525	T1053 (1/6)	T1564 (1/9)	T1558 (1/4)	T1046		T1025	T1572		T1489
				T1556 (0/4)	T1078 (0/4)	T1574 (2/11)	T1539	T1135		T1074 (0/2)	T1090 (0/4)		T1529
				T1137 (0/6)		T1562 (1/9)	T1111	T1040		T1114 (0/3)	T1219		
				T1542 (0/5)		T1070 (0/6)	T1552 (1/7)	T1201		T1056 (0/4)	T1205 (0/1)		
				T1053 (1/6)		T1202		T1120		T1113	T1102 (1/3)		
				T1505 (1/4)		T1036 (3/7)		T1069 (0/3)		T1125			
				T1205 (0/1)		T1556 (0/4)		T1057					
				T1078 (0/4)		T1578 (0/4)		T1012					
						T1112		T1018					
						T1601 (0/2)		T1518 (1/1)					
						T1599 (0/1)		T1082					
						T1027 (1/6)		T1614 (0/1)					
						T1542 (0/5)		T1016 (0/1)					
						T1055 (2/11)		T1049					
						T1620		T1033					
						T1207		T1007					
						T1014		T1124					
						T1218 (3/13)		T1497 (1/3)					
						T1216 (0/1)							
						T1553 (1/6)							
						T1221							
						T1205 (0/1)							
						T1127 (0/1)							
						T1535							
						T1550 (0/4)							
						T1078 (0/4)							
						T1497 (1/3)							
						T1600 (0/2)							
						T1220							

INPUT

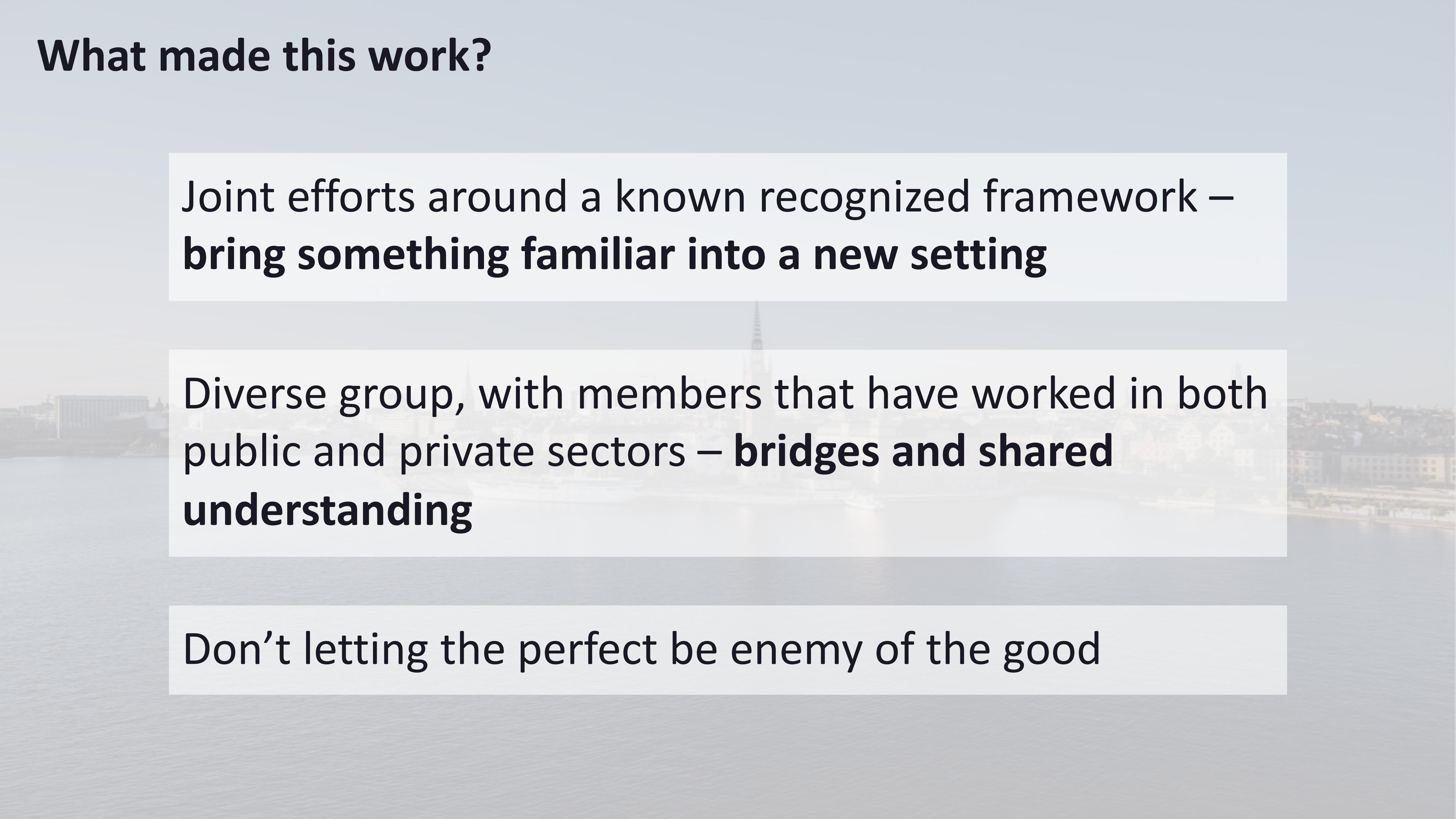
ANALYTICAL PROCESS

OUTPUT

The Result – 15 top reported Techniques from TA list

ATT&CK	Technique	Tactic
T1190	Exploit Public-Facing Application	Initial Access
T1566.001	Phishing: Spearphishing Attachment	Initial Access
T1078	Valid Accounts	Defense Evasion, Persistence, Privilege Escalation, Initial Access
T1059	Command and Scripting Interpreter	Execution
T1204	User Execution	Execution
T1574	Hijack Execution Flow	Persistence, Privilege Escalation, Defense Evasion
T1027	Obfuscated Files or Information	Defense Evasion
T1082	System Information Discovery	Discovery
T1497	Virtualization/Sandbox Evasion	Defense Evasion, Discovery
T1036	Masquerading	Defense Evasion
T1070	Indicator Removal	Defense Evasion
T1005	Data from Local System	Collection
T1071	Application Layer Protocol	Command and Control
T1105	Ingress Tool Transfer	Command and Control
T1489	Service Stop	Impact
T1486	Data Encrypted for impact	Impact

What made this work?



Joint efforts around a known recognized framework – **bring something familiar into a new setting**

Diverse group, with members that have worked in both public and private sectors – **bridges and shared understanding**

Don’t letting the perfect be enemy of the good