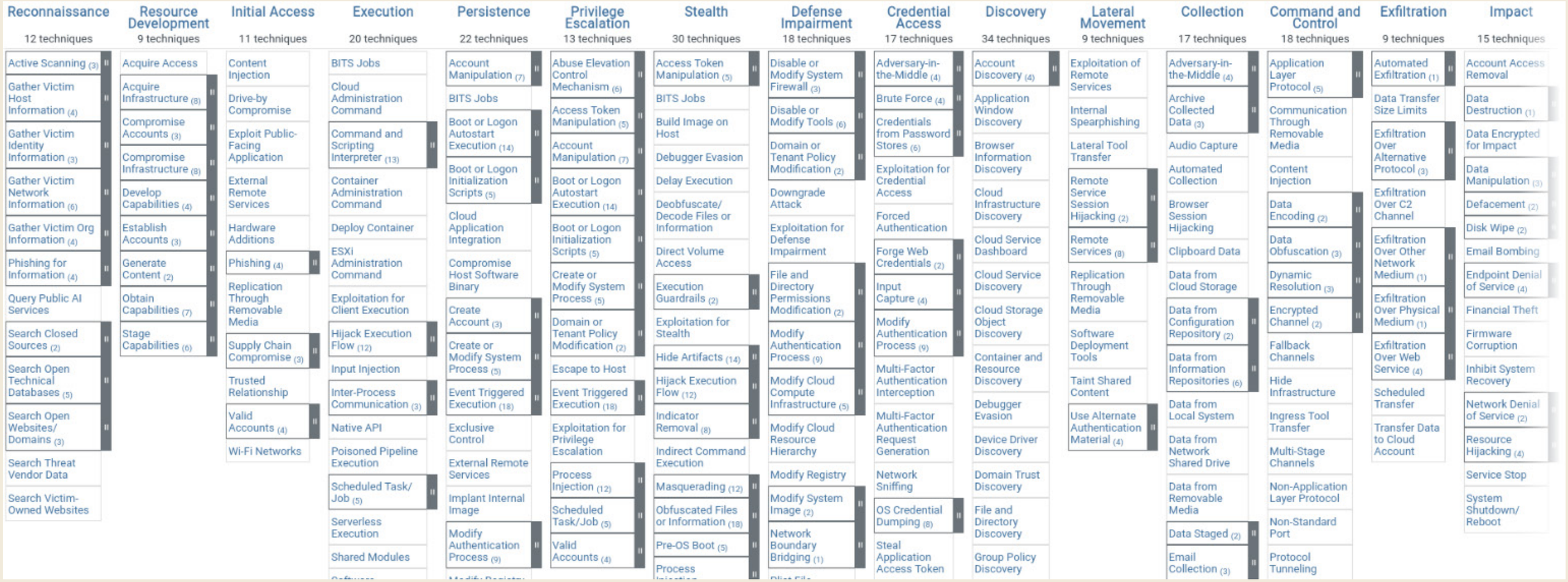
MITRE ATT&CK *a gyakorlatban*

Juhász Réka Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet · Kiberbiztonsági szakértő

MITRE ATT&CK

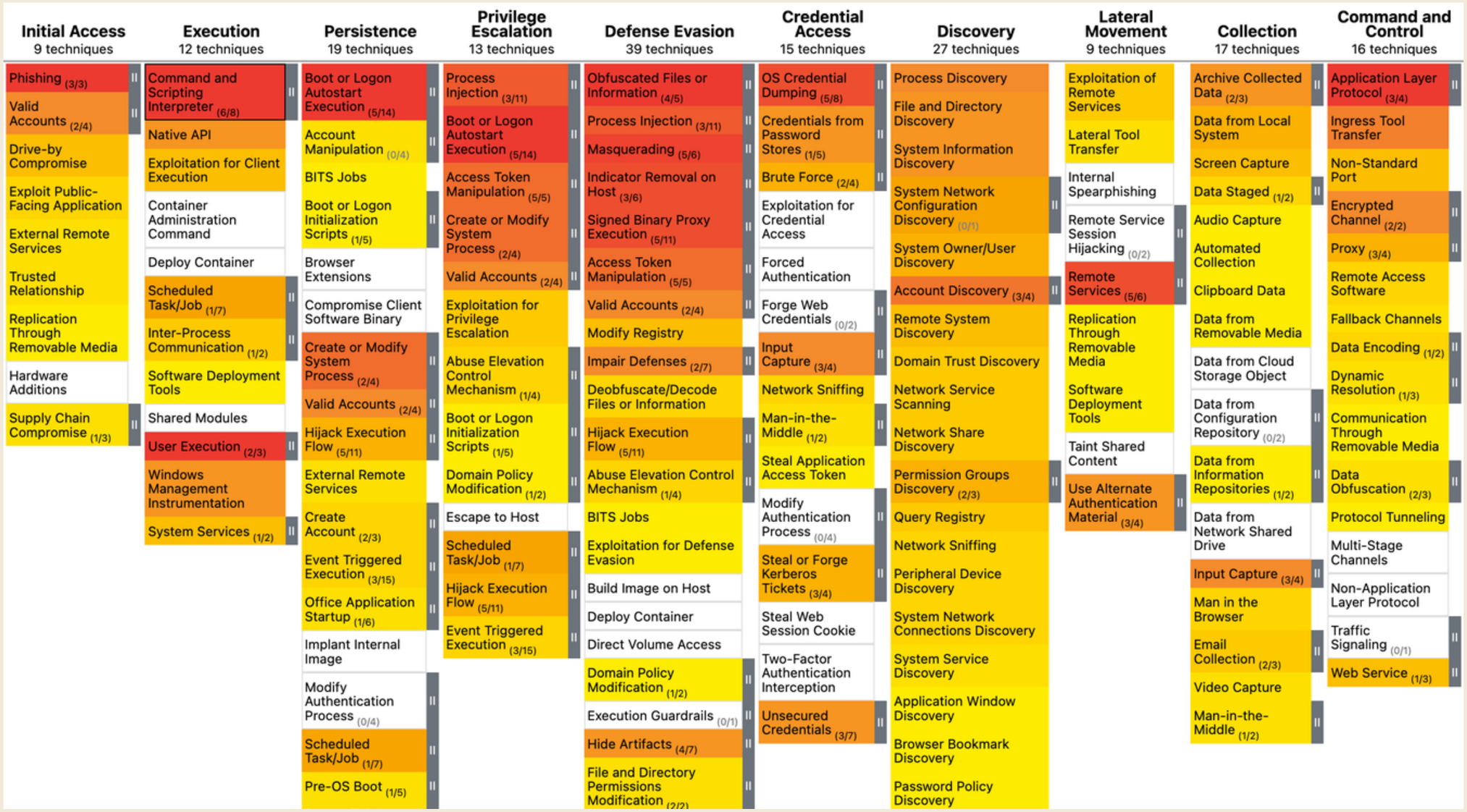
A gyakorlatban



Reconnaissance (12)	Resource Development (9)	Initial Access (11)	Execution (20)	Persistence (22)	Privilege Escalation (13)	Stealth (30)	Defense Impairment (18)	Credential Access (17)	Discovery (34)	Lateral Movement (9)	Collection (17)	Command and Control (18)	Exfiltration (9)	Impact (15)
Active Scanning (3)	Acquire Access	Content Injection	BITS Jobs	Account Manipulation (7)	Abuse Elevation Control Mechanism (6)	Access Token Manipulation (5)	Disable or Modify System Firewall (3)	Adversary-in-the-Middle (4)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (4)	Application Layer Protocol (5)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Cloud Administration Command	BITS Jobs	Access Token Manipulation (5)	BITS Jobs	Disable or Modify Tools (6)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction (1)
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Command and Scripting Interpreter (13)	Boot or Logon Autostart Execution (14)	Account Manipulation (7)	Build Image on Host	Domain or Tenant Policy Modification (2)	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (8)	External Remote Services	Container Administration Command	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Debugger Evasion	Downgrade Attack	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Deploy Container	Cloud Application Integration	Boot or Logon Initialization Scripts (5)	Delay Execution	Exploitation for Defense Impairment	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	ESXi Administration Command	Compromise Host Software Binary	Create or Modify System Process (5)	Deobfuscate/ Decode Files or Information	File and Directory Permissions Modification (2)	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Query Public AI Services	Generate Content (2)	Replication Through Removable Media	Exploitation for Client Execution	Create Account (3)	Domain or Tenant Policy Modification (2)	Direct Volume Access	Modify Authentication Process (9)	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (2)	Exfiltration Over Web Service (4)	Email Bombing
Search Closed Sources (2)	Obtain Capabilities (7)	Supply Chain Compromise (3)	Hijack Execution Flow (12)	Create or Modify System Process (5)	Escape to Host	Execution Guardrails (2)	Modify Cloud Compute Infrastructure (5)	Modify Authentication Process (9)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Fallback Channels	Scheduled Transfer	Endpoint Denial of Service (4)
Search Open Technical Databases (5)	Stage Capabilities (6)	Trusted Relationship	Input Injection	Event Triggered Execution (18)	Event Triggered Execution (18)	Exploitation for Stealth	Modify Cloud Resource Hierarchy	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (6)	Hide Infrastructure	Transfer Data to Cloud Account	Financial Theft
Search Open Websites/ Domains (3)		Valid Accounts (4)	Inter-Process Communication (3)	Exclusive Control	Exploitation for Privilege Escalation	Hide Artifacts (14)	Modify Registry	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System	Ingress Tool Transfer		Firmware Corruption
Search Threat Vendor Data		Wi-Fi Networks	Native API	External Remote Services	Process Injection (12)	Hijack Execution Flow (12)	Modify System Image (2)	Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive	Multi-Stage Channels		Inhibit System Recovery
Search Victim-Owned Websites			Poisoned Pipeline Execution	Implant Internal Image	Scheduled Task/Job (5)	Indicator Removal (8)	Network Boundary Bridging (1)	OS Credential Dumping (8)	File and Directory Discovery		Data from Removable Media	Non-Application Layer Protocol		Network Denial of Service (2)
			Scheduled Task/ Job (5)	Modify Authentication Process (9)	Valid Accounts (4)	Indirect Command Execution		Steal Application Access Token	Group Policy Discovery		Data Staged (2)	Non-Standard Port		Resource Hijacking (4)
			Serverless Execution			Masquerading (12)					Email Collection (3)	Protocol Tunneling		Service Stop
			Shared Modules			Obfuscated Files or Information (18)								System Shutdown/ Reboot
						Pre-OS Boot (5)								
						Process								

MITRE ATT&CK

A gyakorlatban



Initial Access (9 techniques)	Execution (12 techniques)	Persistence (19 techniques)	Privilege Escalation (13 techniques)	Defense Evasion (39 techniques)	Credential Access (15 techniques)	Discovery (27 techniques)	Lateral Movement (9 techniques)	Collection (17 techniques)	Command and Control (16 techniques)
Phishing (3/3)	Command and Scripting Interpreter (6/8)	Boot or Logon Autostart Execution (5/14)	Process Injection (3/11)	Obfuscated Files or Information (4/5)	OS Credential Dumping (5/8)	Process Discovery	Exploitation of Remote Services	Archive Collected Data (2/3)	Application Layer Protocol (3/4)
Valid Accounts (2/4)	Native API	Account Manipulation (0/4)	Boot or Logon Autostart Execution (5/14)	Process Injection (3/11)	Credentials from Password Stores (1/5)	File and Directory Discovery	Lateral Tool Transfer	Data from Local System	Ingress Tool Transfer
Drive-by Compromise	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5/5)	Masquerading (5/6)	Brute Force (2/4)	System Information Discovery	Internal Spearphishing	Screen Capture	Non-Standard Port
Exploit Public-Facing Application	Container Administration Command	Boot or Logon Initialization Scripts (1/5)	Create or Modify System Process (2/4)	Indicator Removal on Host (3/6)	Exploitation for Credential Access	System Network Configuration Discovery (0/1)	Remote Service Session Hijacking (0/2)	Data Staged (1/2)	Encrypted Channel (2/2)
External Remote Services	Deploy Container	Browser Extensions	Valid Accounts (2/4)	Signed Binary Proxy Execution (5/11)	Forced Authentication	System Owner/User Discovery	Remote Services (5/6)	Audio Capture	Proxy (3/4)
Trusted Relationship	Scheduled Task/Job (1/7)	Compromise Client Software Binary	Exploitation for Privilege Escalation	Access Token Manipulation (5/5)	Forge Web Credentials (0/2)	Account Discovery (3/4)	Replication Through Removable Media	Automated Collection	Remote Access Software
Replication Through Removable Media	Inter-Process Communication (1/2)	Create or Modify System Process (2/4)	Abuse Elevation Control Mechanism (1/4)	Valid Accounts (2/4)	Input Capture (3/4)	Remote System Discovery	Software Deployment Tools	Clipboard Data	Fallback Channels
Hardware Additions	Software Deployment Tools	Valid Accounts (2/4)	Boot or Logon Initialization Scripts (1/5)	Modify Registry	Network Sniffing	Domain Trust Discovery	Taint Shared Content	Data from Removable Media	Data Encoding (1/2)
Supply Chain Compromise (1/3)	Shared Modules	Hijack Execution Flow (5/11)	Domain Policy Modification (1/2)	Impair Defenses (2/7)	Man-in-the-Middle (1/2)	Network Service Scanning	Use Alternate Authentication Material (3/4)	Data from Cloud Storage Object	Dynamic Resolution (1/3)
	User Execution (2/3)	External Remote Services	Escape to Host	Deobfuscate/Decode Files or Information	Steal Application Access Token	Network Share Discovery		Data from Configuration Repository (0/2)	Communication Through Removable Media
	Windows Management Instrumentation	Create Account (2/3)	Scheduled Task/Job (1/7)	Hijack Execution Flow (5/11)	Modify Authentication Process (0/4)	Permission Groups Discovery (2/3)		Data from Information Repositories (1/2)	Data Obfuscation (2/3)
	System Services (1/2)	Event Triggered Execution (3/15)	Hijack Execution Flow (5/11)	Abuse Elevation Control Mechanism (1/4)	Steal or Forge Kerberos Tickets (3/4)	Query Registry		Data from Network Shared Drive	Protocol Tunneling
		Office Application Startup (1/6)	Event Triggered Execution (3/15)	BITS Jobs	Steal Web Session Cookie	Network Sniffing		Input Capture (3/4)	Multi-Stage Channels
		Implant Internal Image		Exploitation for Defense Evasion	Two-Factor Authentication Interception	Peripheral Device Discovery		Man in the Browser	Non-Application Layer Protocol
		Modify Authentication Process (0/4)		Build Image on Host	Unsecured Credentials (3/7)	System Network Connections Discovery		Email Collection (2/3)	Traffic Signaling (0/1)
		Scheduled Task/Job (1/7)		Deploy Container		System Service Discovery		Video Capture	Web Service (1/3)
		Pre-OS Boot (1/5)		Direct Volume Access		Application Window Discovery		Man-in-the-Middle (1/2)	
				Domain Policy Modification (1/2)		Browser Bookmark Discovery			
				Execution Guardrails (0/1)		Password Policy Discovery			
				Hide Artifacts (4/7)					
				File and Directory Permissions Modification (2/2)					

Mi a keretrendszer célja?

01 **Támadói viselkedések leírása**

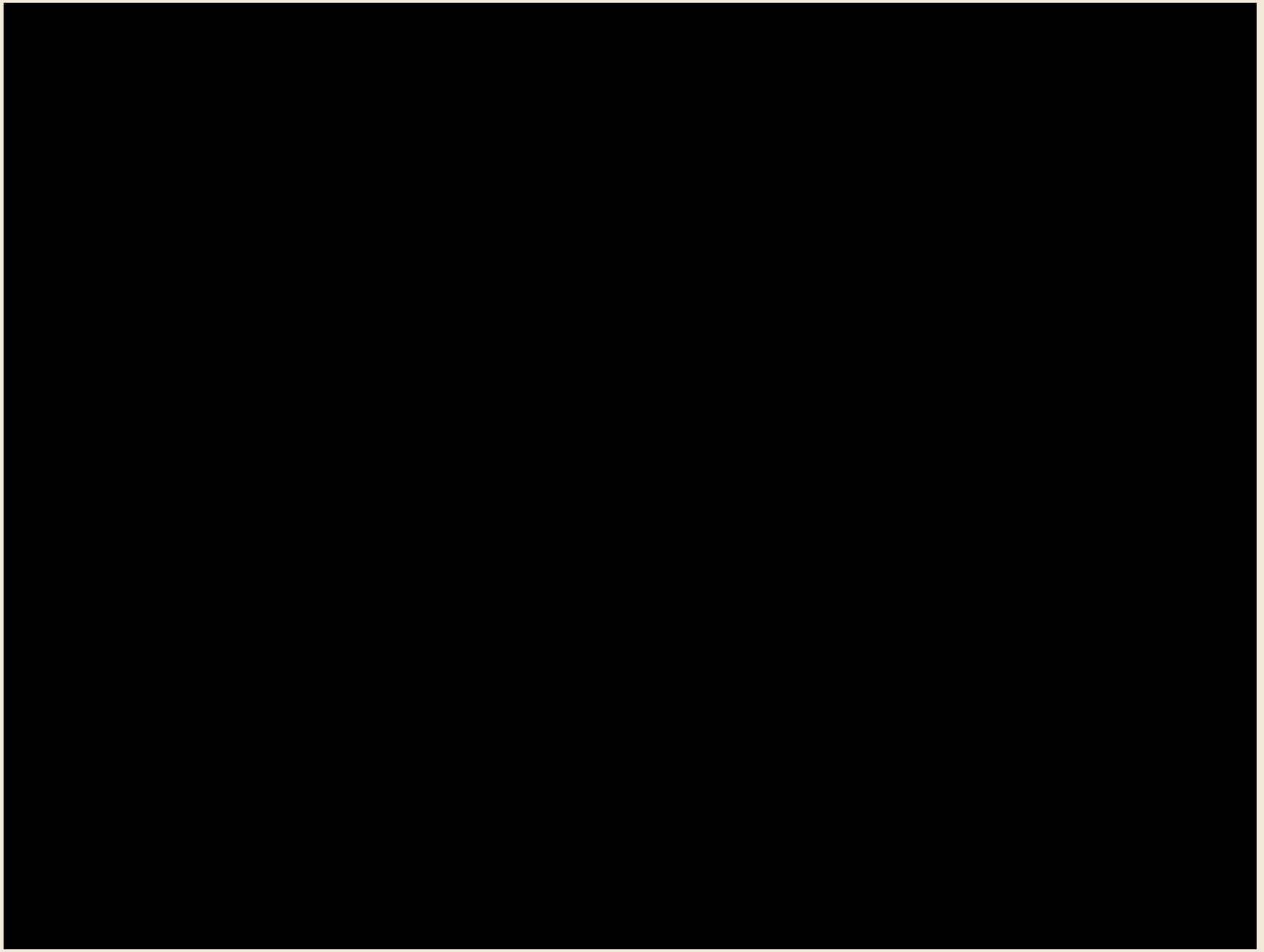
Teljesség igényével, támadás életciklusára bontva

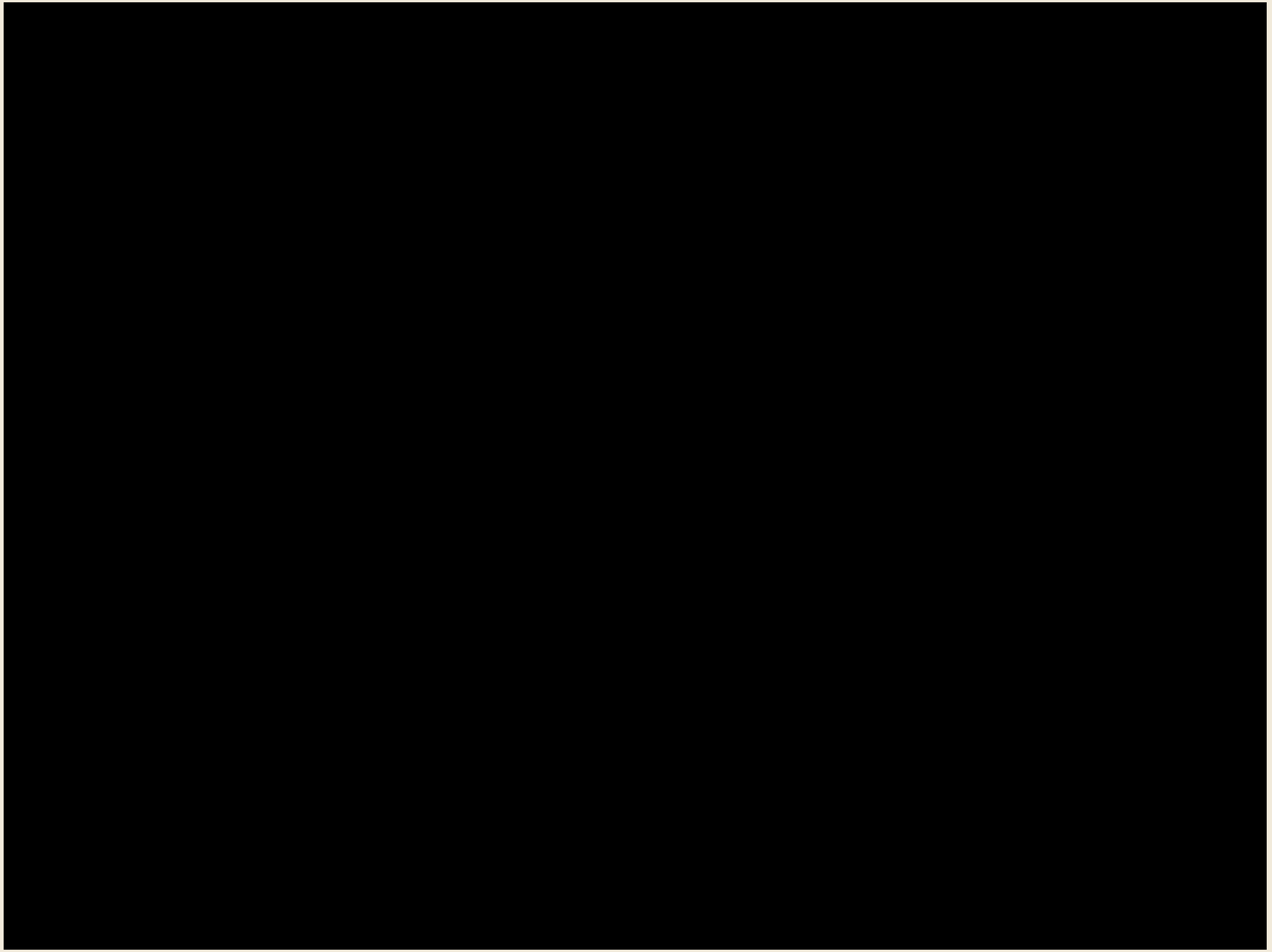
02 **Taktika: oszlop, miért**

A mátrix oszlopai, mint pl. az “Impact”, egy támadás miértjét rejti

03 **TTP: tactics, Techniques, procedures**

Egy specifikus támadási mód “hogyanját” írja le





Blue team

01 **Log-ok TTP-kel**

Snort/YARA szabályok, EDR, SIEM

02 **Korrelációk felfedezése**

Milyen TTP-k kerültek elő gyakran?

03 **Összetett védekezés**

Védekezés kialakítása a saját és CTI adatokból

Red team

01 **Atomic Red team**

Gyors, TTP-re mappelt tesztek

02 **MITRE Caldera**

Adversary emulációs platform

03 **Visszajelzés a blue team-nek**

A TTP-k közös nyelvként szolgálnak

CTI

01 ## Saját adatokból

Idővel a saját adatainkból is trendek rajzolódnak ki

02 ## Hasonló szervezetek adataiból

Hasonló profilú szervezeteknél hasonló kockázati tényezők állnak fenn

03 ## Együttműködés

A keretrendszer közös nyelvként megkönnyíti az együttműködést

Kitekintő

01 **MITRE D3FEND**
Hardening, detection, isolation és egyéb védekezési technikák

02 **MITRE ATLAS**
Generatív AI és AI ágensek elleni támadási technikák

03 **MITRE CAR**
Tudásbázis MITRE alapú detekciók írásához (Sysmon, Splunk, EQL)

CYBERSEC

Köszönöm a figyelmet!

Juhász Réka