Mit dem MITRE ATT&CK Framework Cyberangriffe frühzeitig erkennen & abwehren

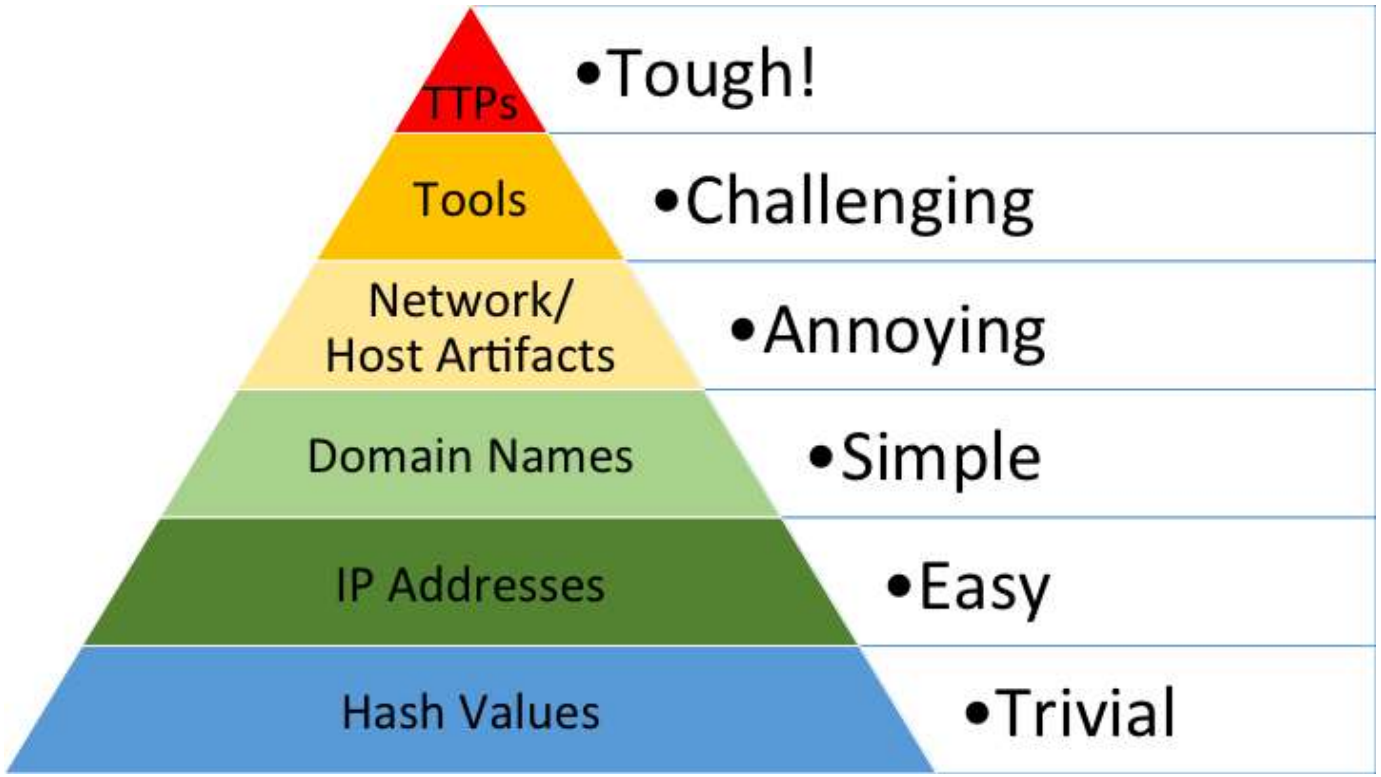
Angelo Brancato CISSP, CISM, CCSK | **Security Specialist, EMEA**

splunk> turn data into doing™

MITRE | ATT&CK™

Adversarial Tactics, Techniques and Common Knowledge

The Pyramid of Pain



http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

MITRE ATT&CK – What is it?

- **Free, Open, Community** Driven **Knowlegebase**
- Describes Cyber **Adversary Behavior**
- Provides a **Common Language** (Taxonomy) for both **Offense** and **Defense**

https://attack.mitre.org/resources/enterprise-introduction/

- 3 Flavours: **PRE-**ATT&CK™, **Enterprise** ATT&CK™, **Mobile** ATT&CK™

Tactics & Techniques

Actor: Angelo Brancato
Goal: Vortrag auf der ITsa halten

Tactics

Techniques

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Resource Hijacking
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy		Runtime Data Manipulation
	Launchctl	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels		Service Stop
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	SSH Hijacking	Video Capture	Multiband Communication		Stored Data Manipulation
	LSASS Driver	Create Account	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content		Multilayer Encryption		Transmitted Data Manipulation
	Mshta	DLL Search Order Hijacking	New Service	Disabling Security Tools	Network Sniffing	Security Software Discovery	Third-party Software		Port Knocking		
	PowerShell	Dylib Hijacking	Path Interception	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote Access Tools		
	Regsvcs/Regasm	External Remote Services	Plist Modification	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Remote File Copy		
	Regsvr32	File System Permissions Weakness	Port Monitors	Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard Application Layer Protocol		
	Rundll32	Hidden Files and Directories	Process Injection	Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Owner/User Discovery			Standard Cryptographic Protocol		
	Scheduled Task	Hooking	Scheduled Task	Extra Window Memory Injection		System Service Discovery			Standard Non-Application Layer Protocol		
	Scripting	Hypervisor	Service Registry Permissions Weakness	File Deletion		System Time Discovery			Uncommonly Used Port		
	Service Execution	Image File Execution Options Injection	Setuid and Setgid	File Permissions Modification		Virtualization/Sandbox Evasion			Web Service		
	Signed Binary Proxy Execution	Kernel Modules and Extensions	SID-History Injection	File System Logical Offsets							
	Signed Script Proxy Execution	Launch Agent	Startup Items	Gatekeeper Bypass							
	SIP and Trust Provider Hijacking	Launch Daemon	Sudo	Group Policy Modification							
	Startup Items	Launchctl	Sudo Caching	Hidden Files and Directories							
	System Firmware	LC_LOAD_DYLIB Addition	Valid Accounts	Hidden Users							
	Systemd Service	Local Job Scheduling	Web Shell	Hidden Window							
	Time Providers	Login Item		HISTCONTROL							
	Trap	Logon Scripts		Image File Execution Options Injection							
	Valid Accounts	LSASS Driver		Indicator Blocking							
	Web Shell	Modify Existing Service		Indicator Removal from Tools							
	Windows Management Instrumentation Event Subscription	Netsh Helper DLL		Indicator Removal on Host							
	Winlogon Helper DLL	New Service		Indirect Command Execution							
		Office Application Startup		Install Root Certificate							
		Path Interception		InstallUtil							
		Plist Modification		Launchctl							
		Port Knocking		LC_MAIN Hijacking							
		Port Monitors		Masquerading							
		Process Injection		Modify Registry							
		Redundant Access		Mshta							
		Registry Run Keys / Startup Folder		Network Share Connection Removal							
		Scheduled Task		NTFS File Attributes							
		Screensaver		Obfuscated Files or Information							
		Security Support Provider		Plist Modification							
		Service Registry Permissions Weakness		Port Knocking							
		Setuid and Setgid		Process Doppelgänging							
		Shortcut Modification		Process Hollowing							
		SIP and Trust Provider Hijacking		Process Injection							
		Startup Items		Redundant Access							
		System Firmware		Regsvcs/Regasm							
		Systemd Service		Regsvr32							
		Time Providers		Rootkit							
		Trap		Rundll32							
		Valid Accounts		Scripting							
		Web Shell		Signed Binary Proxy Execution							
		Windows Management Instrumentation Event Subscription		Signed Script Proxy Execution							
		Winlogon Helper DLL		SIP and Trust Provider Hijacking							
				Software Packing							
				Space after Filename							
				Template Injection							
				Timestomp							
				Trusted Developer Utilities							
				Valid Accounts							
				Virtualization/Sandbox Evasion							
				Web Service							
				XSL Script Processing							

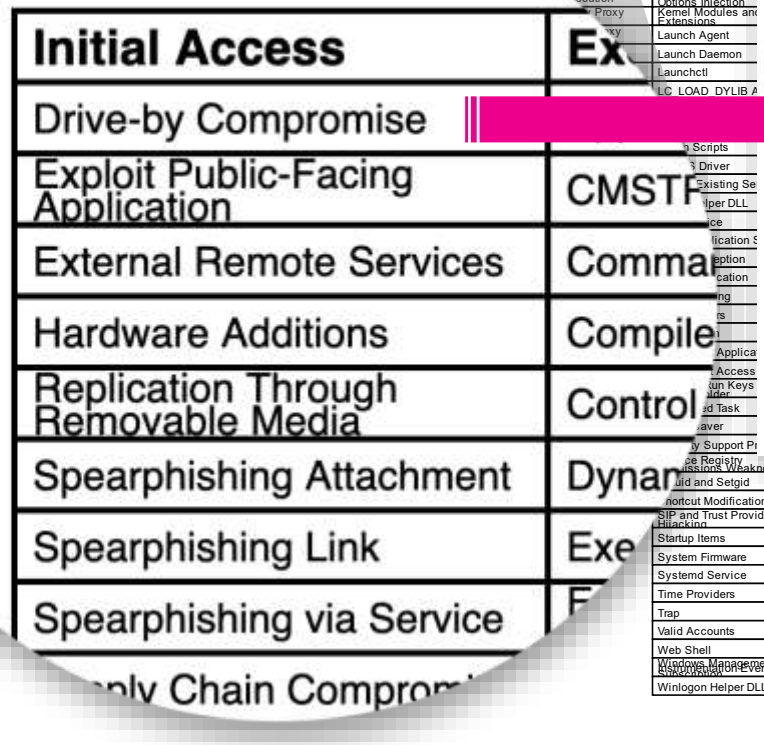
Initial Access	Ex
Drive-by Compromise	Apple
Exploit Public-Facing Application	CMSTP
External Remote Services	Comma
Hardware Additions	Compile
Replication Through Removable Media	Control
Spearphishing Attachment	Dynam
Spearphishing Link	Exe
Spearphishing via Service	
ply Chain Compro	

https://mitre-attack.github.io/attack-navigator/enterprise/#

Tactics

Techniques

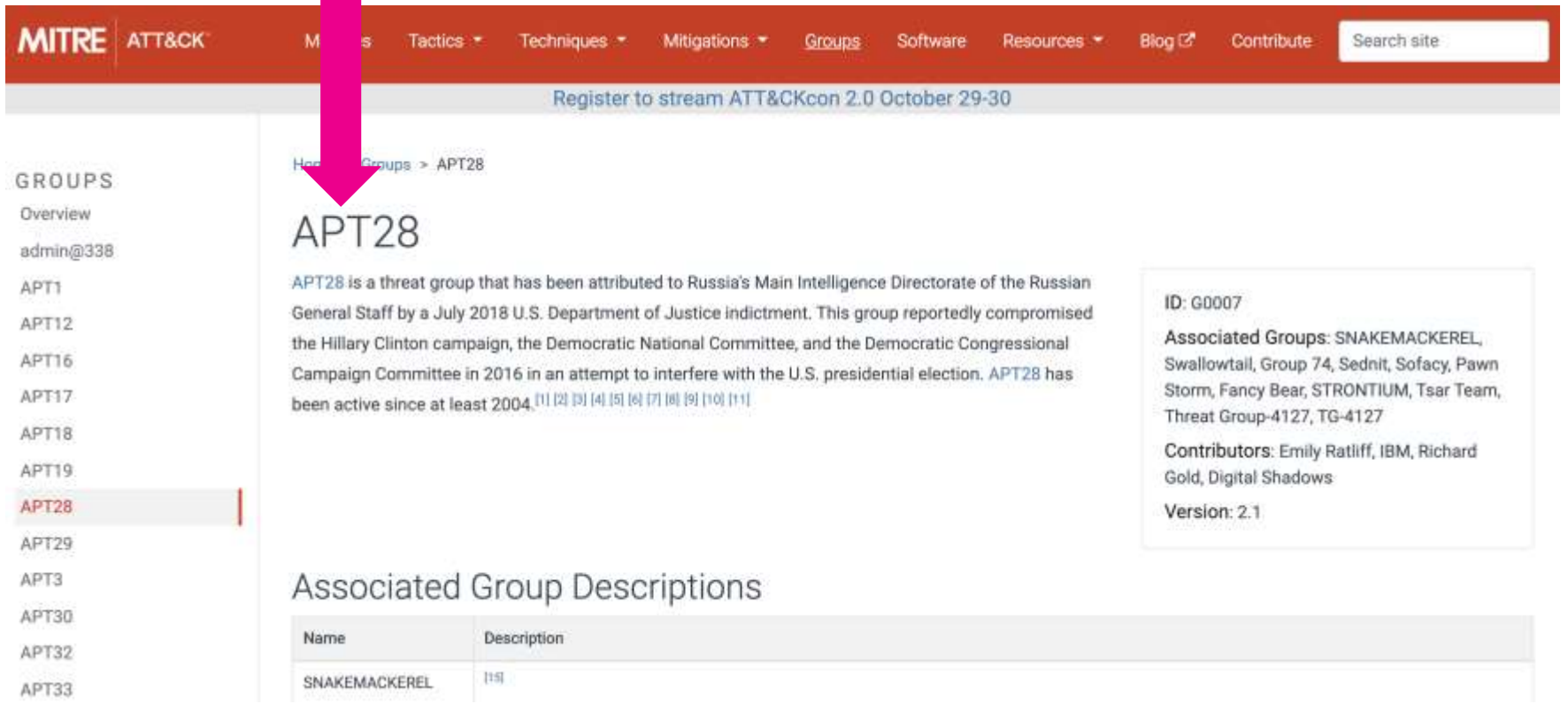
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Resource Hijacking
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy		Runtime Data Manipulation
	Launchctl	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels		Service Stop
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	SSH Hijacking	Video Capture	Multiband Communication		Stored Data Manipulation
	LSASS Driver	Create Account	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content		Multilayer Encryption		Transmitted Data Manipulation
	Mshta	DLL Search Order Hijacking	New Service	Disabling Security Tools	Network Sniffing	Security Software Discovery	Third-party Software		Port Knocking		
	PowerShell	Dylib Hijacking									
	Regsvcs/Regasm	External Remote Services									
	Regsvr32	File System Permissions Weakness									
	Rundll32	Hidden Files and Directories									
	Scheduled Task	Hooking									
		Hypervisor									
		Image File Execution Options Injection									
		Kernel Modules and Extensions									
		Launch Agent									
		Launch Daemon									
		Launchctl									
		LC_LOAD_DYLIB Addition									
		Login Item									
		Logon Scripts									
		LSASS Driver									
		Modify Existing Service									
		Netsh Helper DLL									
		New Service									
		Office Application Startup									
		Path Interception									
		Plist Modification									
		Port Knocking									
		Port Monitors									
		Process Injection									
		Redundant Access									
		Registry Run Keys / Startup Folder									
		Rootkit									
		Scheduled Task									
		Screensaver									
		Security Support Provider									
		Service Registry Permissions Weakness									
		Setuid and Setgid									
		Shortcut Modification									
		SIP and Trust Provider Hijacking									
		Startup Items									
		System Firmware									
		Systemd Service									
		Time Providers									
		Trap									
		Valid Accounts									
		Web Shell									
		Windows Management Instrumentation Event Subscription									
		Winlogon Helper DLL									
				Process Doppelgänging							
				Process Hollowing							
				Process Injection							
				Redundant Access							
				Regsvcs/Regasm							
				Regsvr32							
				Rootkit							
				Rundll32							
				Scripting							
				Signed Binary Proxy Execution							
				Signed Script Proxy Execution							
				SIP and Trust Provider Hijacking							
				Software Packing							
				Space after Filename							
				Template Injection							
				Timestomp							
				Trusted Developer Utilities							
				Valid Accounts							
				Virtualization/Sandbox Evasion							
				Web Service							
				XSL Script Processing							



https://mitre-attack.github.io/attack-navigator/enterprise/#

APT28

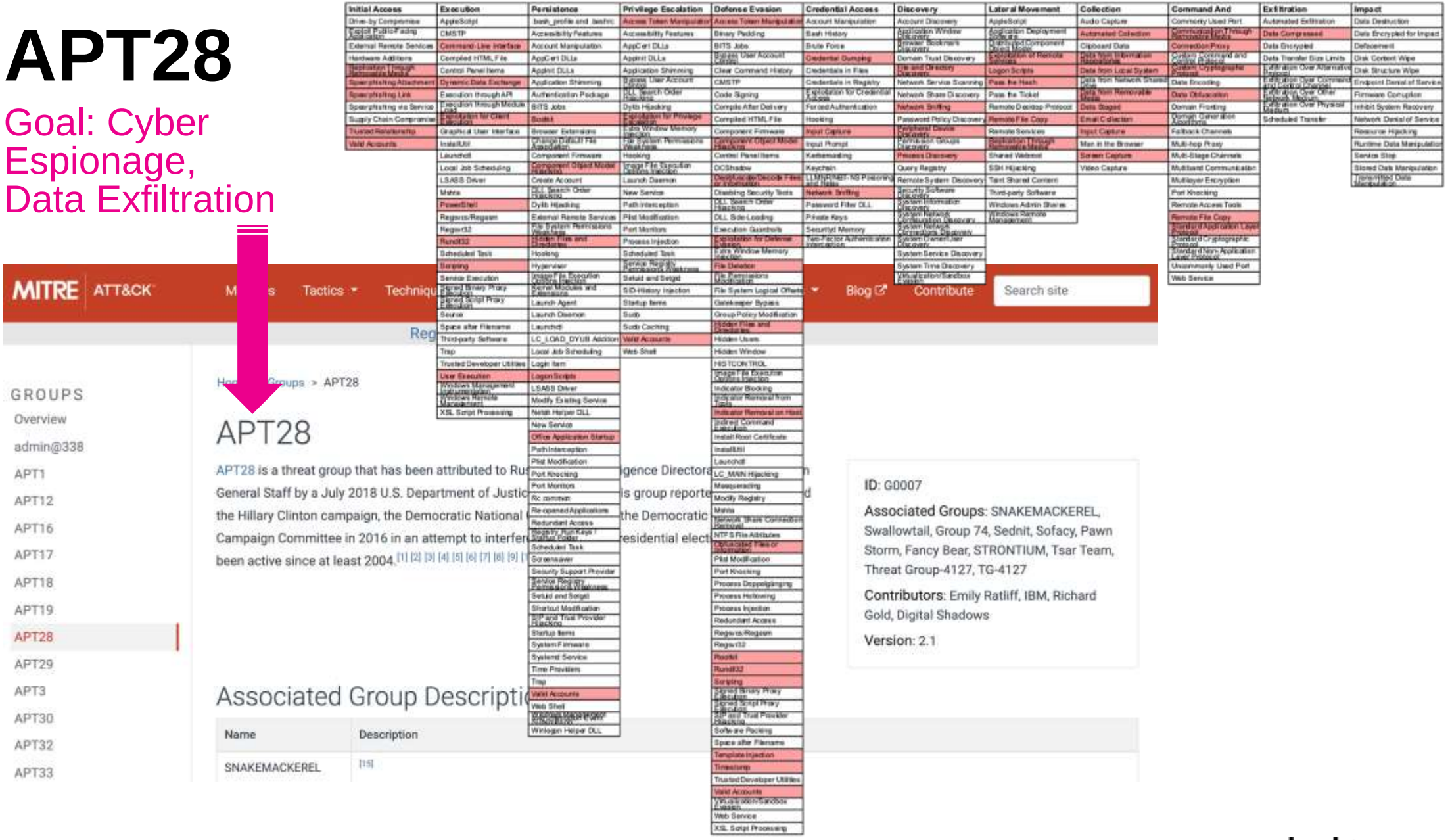
Goal: Cyber Espionage, Data Exfiltration



https://mitre-attack.github.io/attack-navigator/enterprise/#

APT28

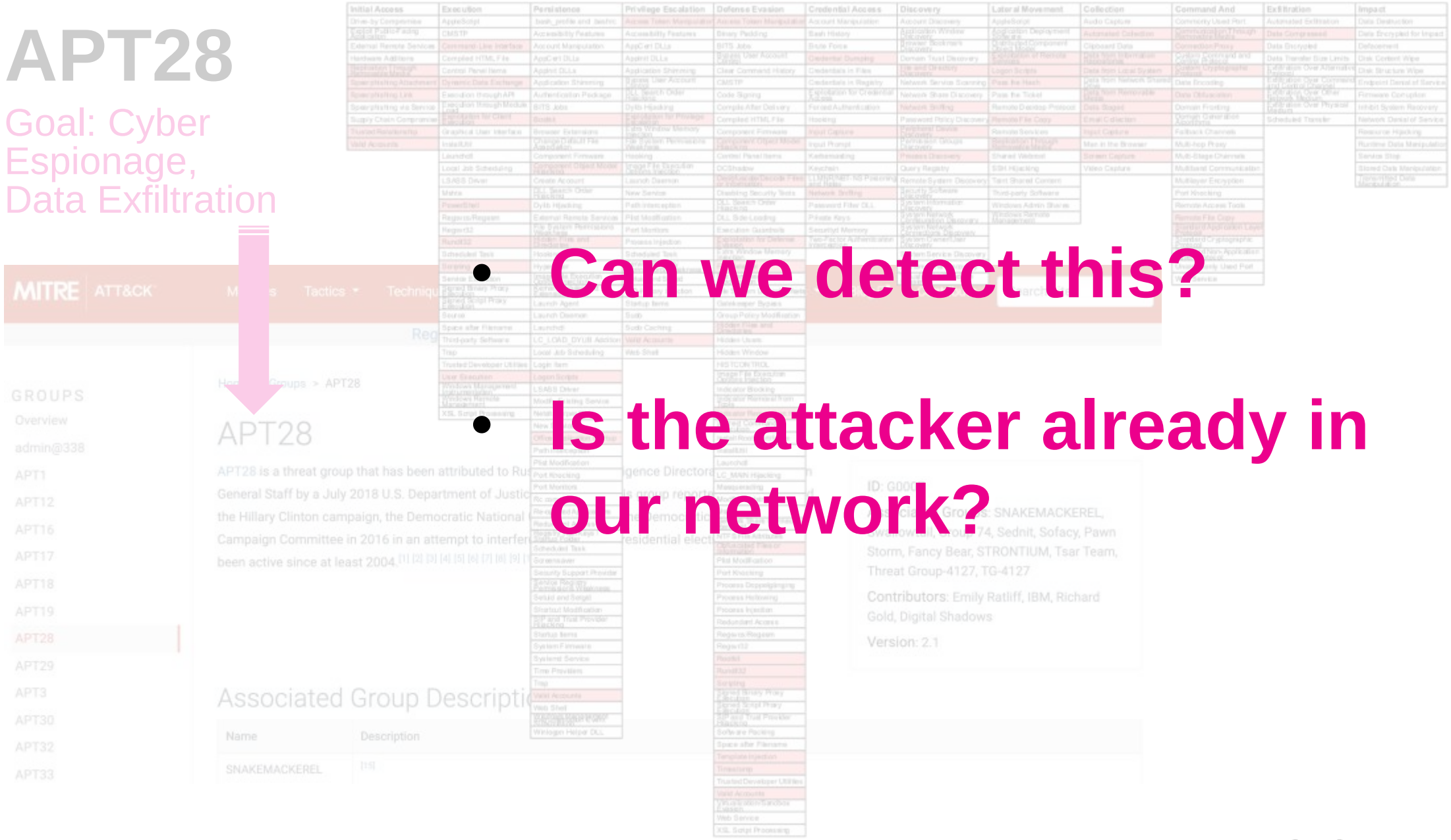
Goal: Cyber Espionage, Data Exfiltration



https://mitre-attack.github.io/attack-navigator/enterprise/#

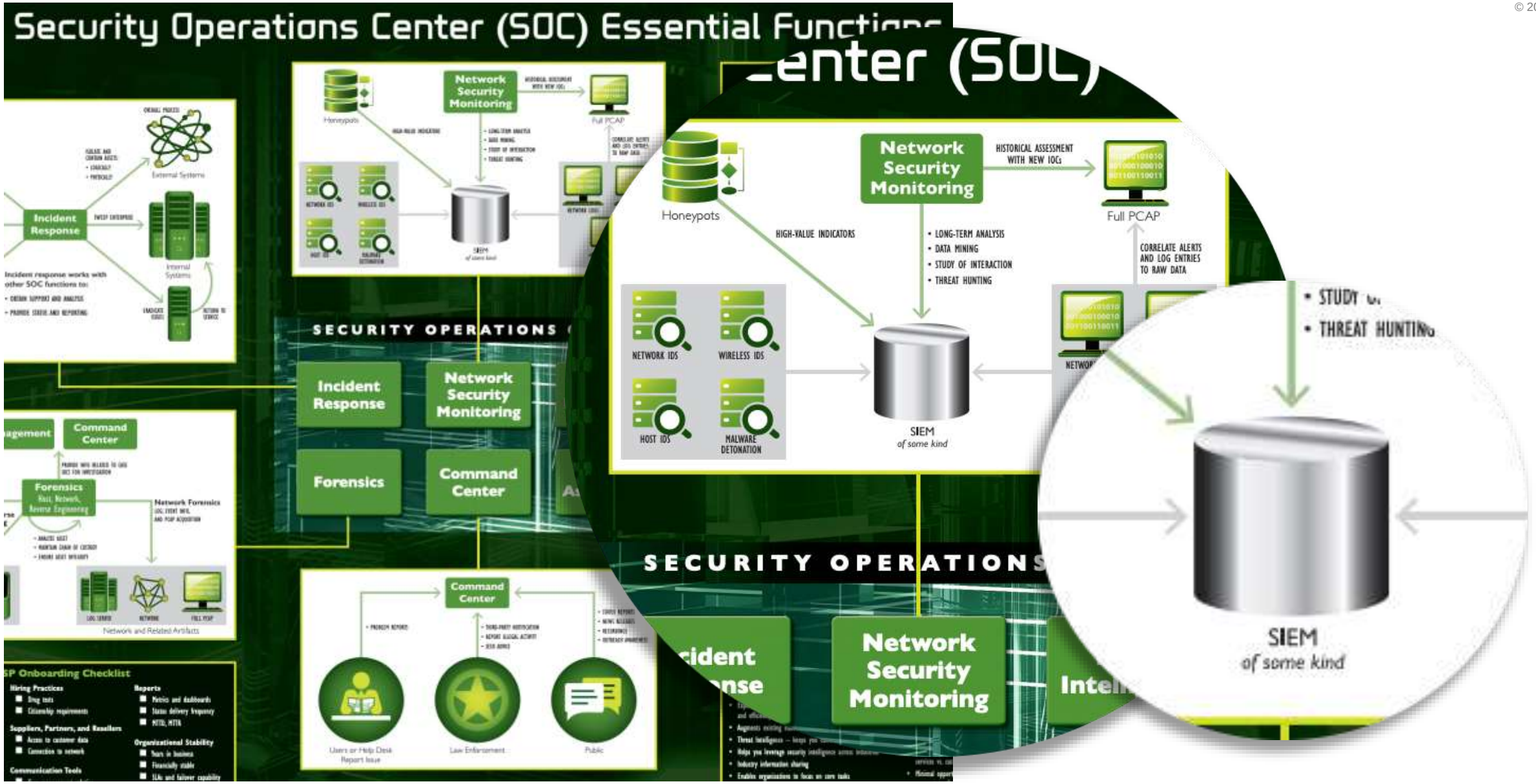
APT28

Goal: Cyber Espionage, Data Exfiltration



- **Can we detect this?**
- **Is the attacker already in our network?**

https://mitre-attack.github.io/attack-navigator/enterprise/#



https://www.sans.org/security-resources/posters/security-leadership-poster/135/download

Security Operations Center (SOC) Essential Functions

⊘	Emotet Malware (DHS Report TA18-201A)	Malware	Detect rarely used executables, specific registry paths that may confer malware survivability and persistence, instances where cmd.exe is used to launch script interpreters, and other indicators that the Emotet financial malware has compromised your environment.	ES Content Updates	11 Sep 2018

Detection Searches

- ⊘ ESCU - Detect Rare Executables - Rule - edit
- ⊘ ESCU - Registry Keys Used For Persistence - Rule - edit
- ⊘ ESCU - Detect Use of cmd.exe to Launch Script Interpreters - Rule - edit
- ⊘ ESCU - Prohibited Software On Endpoint - Rule - edit
- ⊘ ESCU - SMB Traffic Spike - Rule - edit
- ⊘ ESCU - SMB Traffic Spike - MLTK - Rule - edit
- ⊘ ESCU - Suspicious Email Attachment Extensions - Rule - edit
- ⊘ ESCU - Email Attachments With Lots Of Spaces - Rule - edit
- ⊘ ESCU - Detection of tools built by NirSoft - Rule - edit

Recommended Data Sources

Carbon Black Response

CrowdStrike Falcon

Sysmon

Tanium

Ziften

See all 9 Data Sources

Sourcetypes

No items found.

Data Models

- Endpoint
- Network_Traffic
- Email

Lookups

- interesting_processes_lookup
- isSuspiciousFileExtension_looku

Framework Mapping

CIS 20: CIS 2 | CIS 8 | CIS 3 | CIS 7 | CIS 12

KILL CHAIN PHASES: Installation | Command and Control | Actions on Objectives | Exploitation | Delivery

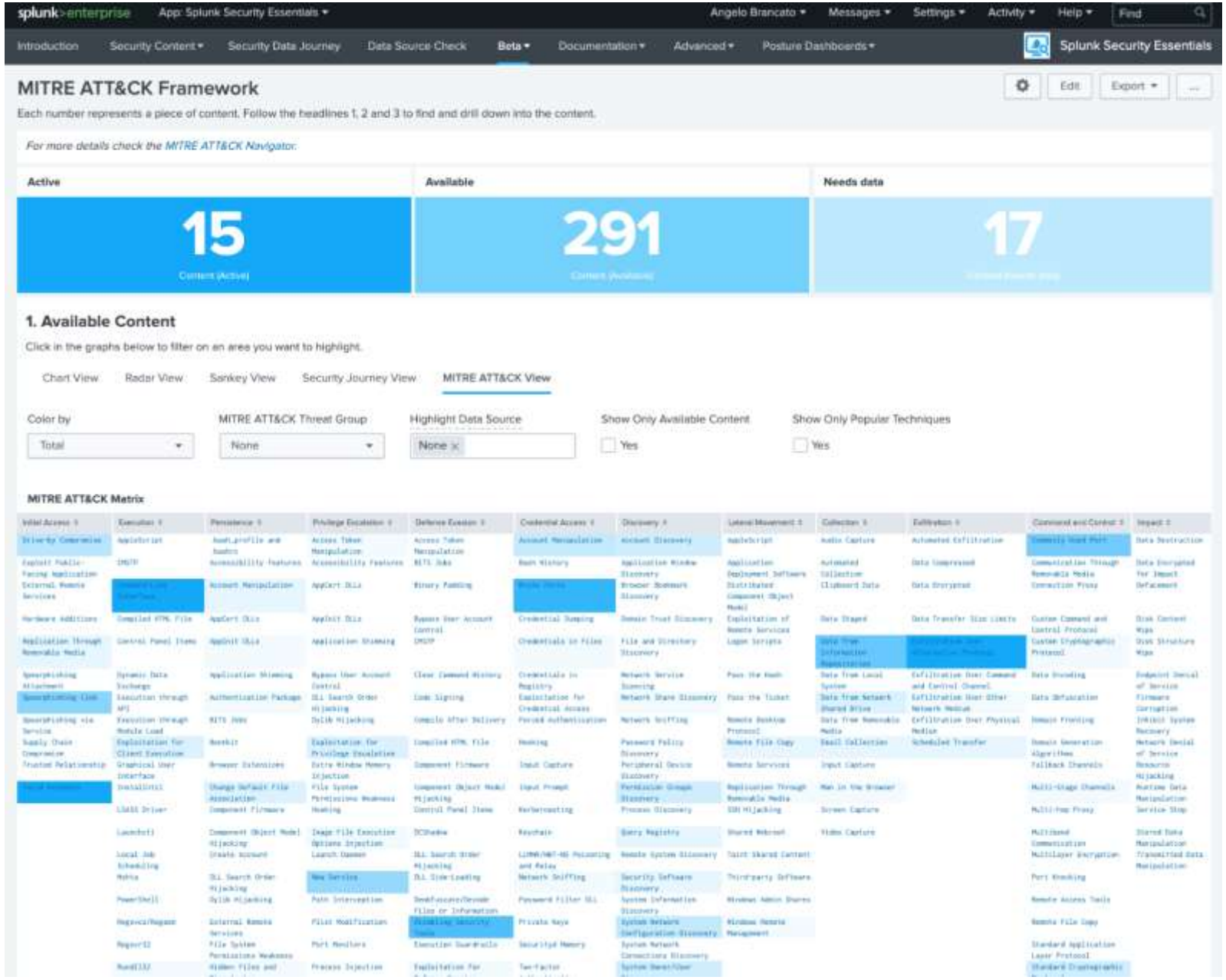
ATT&CK: Execution | Persistence | Registry Run Keys / Start Folder | Appinit DLLs | Authentication Package | Command-Line Interface | Lateral Movement | Command and Control | Commonly Used Port | Defense Evasion | Discovery | Third-party Software | Account Discovery

NIST: ID.AM | PR.PT | PR.DS | DE.CM | DE.AE | PR.IP

https://www.sans.org/security-resources/posters/security-leadership-poster/128/download

APT28

Overlay with **YOUR** current Security Use Cases



Color by

Total

MITRE ATT&CK Threat Group

APT28

Highlight Data Source

None

Show Only Available Content

Yes

Show Only Popular Techniques

Yes

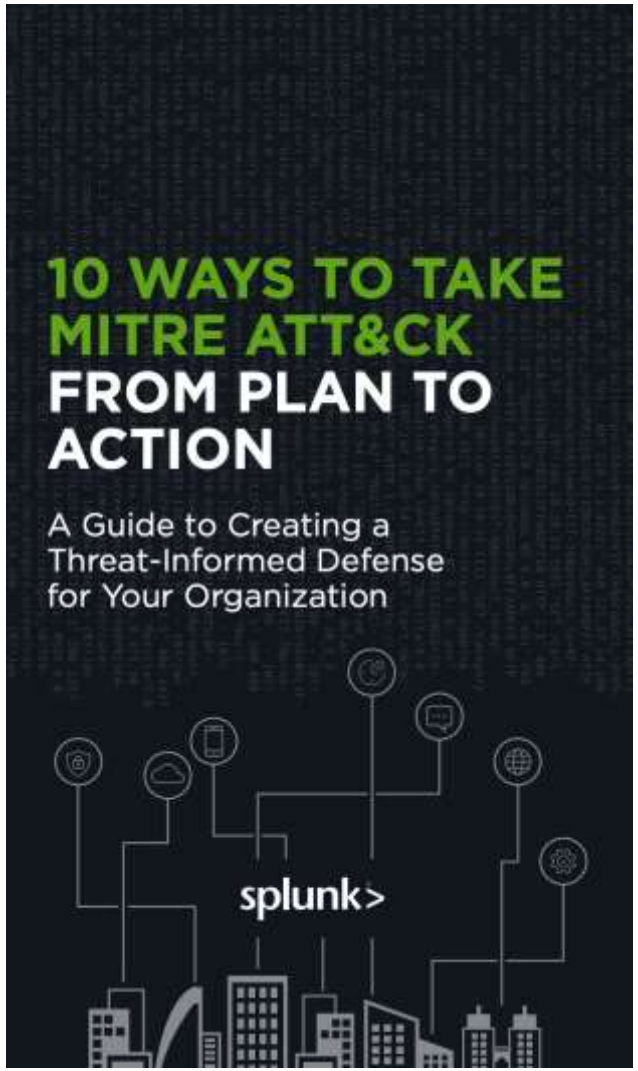
We have no use case.

We‘re good.

We have the use case but no log-data.

MITRE ATT&CK Matrix

Initial Access			Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lat… Mo…		Comm… Contr…
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	App…		Common Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	App… Dep… Sof…		Commu… Throu… Remova… Media
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Conne… Proxy
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custo… and C… Proto…
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custo… Crypt… Proto…
Spearphishing	Dynamic Data	Application	Bypass User	Clear Command	Credentials in	Network Service	Pass the Has…	Data from	Exfiltration	Data …



https://www.splunk.com/de_de/form/10-ways-to-take-the-mitre-att-and-ck-framework-from-plan-to-action.html

1. Establish a Detect, Response, Prevent Strategy	Head of Security Ops
2. Respond with a short analytics turnaround	Sec. Content Developer (Blue Team)
3. Validate Coverage	SIEM Architect
4. Justify need for Data Sources	SOC Engineer
5. Document decisions based on risk evaluation	Head of Security Ops
6. Justify Investment and define roadmap	CISO
7. Risk Based Alerting Model	SOC Analysts
8. Measure Quality of Data Sources and Coverage	SIEM Admin
9. Document and Communicate Improvement Efforts	Penetration Tester (Red Team)
10. Third Party Suppliers	IT Leaders and Purchase Dep.

Dankeschön!

Besuchen Sie uns gerne am Splunk Stand.
Halle 10.0 / 10.0-116

Angelo Brancato, Splunk

splunk> turn data into doing™