

Using MITRE ATT&CK to improve SOC operations

Federico Charosky

Federico.Charosky@quorumcyber.com

@FedeCharosky

#WeFightBullies

About Me

ATT&CK®



Federico Charosky

Federico.Charosky@quorumcyber.com
@FedeCharosky

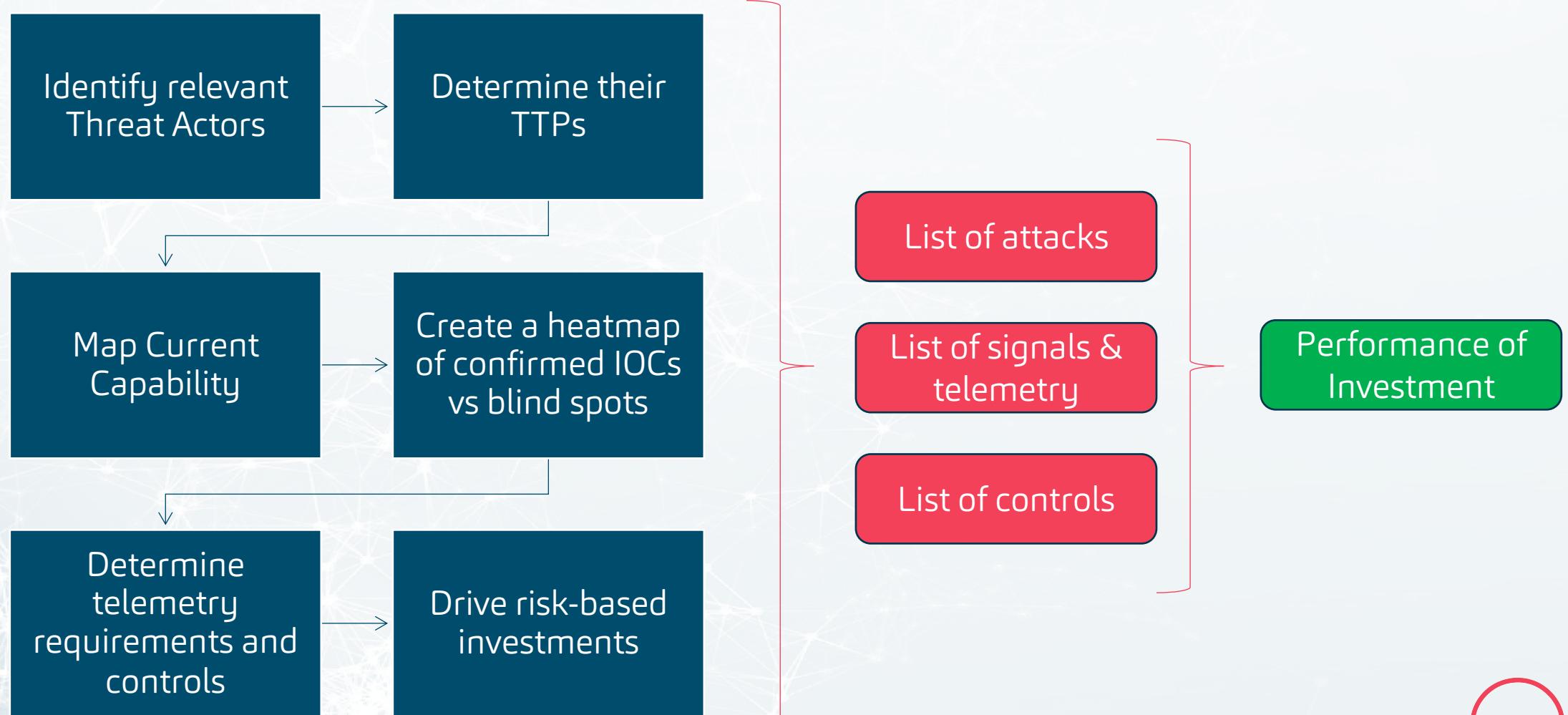
#WeFightBullies

- Managing Director of Quorum Cyber
- Microsoft Azure Sentinel SOC & MDR
- Microsoft Azure security engineering
- Using MITRE ATT&CK threat modelling to drive SOC and risk management since 2016

- We defend teams and organisations that feel overwhelmed by the increasing risk of cyber security breaches and attacks

Methodology

ATT&CK®



#WeFightBullies

1) Identify

ATT&CK®

MITRE | ATT&CK® Matrices Tactics ▾ Techniques ▾ Mitigations ▾ Groups Software Resources ▾ Blog ☰ Contribute Search 

The sub-techniques beta is now live! Read the [release blog post](#) for more info.

Home > Groups

Groups

Groups are sets of related intrusion activity that are tracked by a common name in the security community. Analysts track clusters of activities using various analytic methodologies and terms such as threat groups, activity groups, threat actors, intrusion sets, and campaigns. Some groups have multiple names associated with similar activities due to various organizations tracking similar activities by different names. Organizations' group definitions may partially overlap with groups designated by other organizations and may disagree on specific activity.

For the purposes of the Group pages, the MITRE ATT&CK team uses the term Group to refer to any of the above designations for a cluster of adversary activity. The team makes a best effort to track overlaps between names based on publicly reported associations, which are designated as "Associated Groups" on each page (formerly labeled "Aliases"), because we believe these overlaps are useful for analyst awareness. We do not represent these names as exact overlaps and encourage analysts to do additional research.

Groups are mapped to publicly reported technique use and original references are included. The information provided does not represent all possible technique use by Groups, but rather a subset that is available solely through open source reporting. Groups are also mapped to reported Software used, and technique use for that Software is tracked separately on each Software page.

Groups: 94

Name	Associated Groups	Description
admin@338		admin@338 is a China-based cyber threat group. It has previously used newsworthy events as lures to deliver malware and has primarily targeted organizations involved in financial, economic, and trade policy, typically using publicly available RATs such as PoisonIvy , as well as some non-public backdoors.
APT1	Comment Crew, Comment	APT1 is a Chinese threat group that has been attributed to the 2nd Bureau of the People's

#WeFightBullies



Focus on Industry



Focus on Region

2) TTPs

ATT&CK®

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	External Movement	Collection	Command And Control	Efiltration	Impact
Drive-by Compromise	AppleScript	bash_profile and bashrc	Access Token Manipulation	Access Token Manipulation	Access Token Manipulation	Access Tokens	AppleScript	Audio Capture	Compressed Data	Automated Collection	Data Destruction
Exploit Public-Facing Application	CMSSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software Automated Collection	Communication Through Remote Data Compressed	Communication Through Remote Data Compressed	Custom Command and Control Protocol	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Kernel Modification	Kernel Modification	AppCert DLLs	BITS Jobs	Browser Bookmark Discovery	Distributed Component Object Model Clipboard Data	Customized Collection	Customized Collection	Custom Cryptographic Protocol	Data Encryption
Hardware Additions	Compiled HTML File	AppCert DLLs	AppCert DLLs	Bypass User Account Control	Clear Command History	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repository	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable & Control Panel Items	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSSTP	Credential In Registry	Exploitation for Credential Access	Network Service Scanning	File from Network Shared Drive	File from Network Shared Drive	File from Network Shared Drive	File from Network Shared Drive
Spearphishing Attachment	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Forced Authentication	Network Sniffing	Pass the Hash	Data Encoding	File from Network Shared Drive	File from Network Shared Drive	File from Network Shared Drive
Spearphishing Link	Execution through Module Load	BITs Jobs	Dylib Hijacking	Compile After Delivery	Hooking	Network Sniffing	Pass the Ticket	Data from Removable Media	File from Network Shared Drive	File from Network Shared Drive	File from Network Shared Drive
Spearphishing via Service	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Exploitation for Privilege Escalation	>Password Policy Discovery	Remote Desktop Protocol	Data Encryption	File from Network Shared Drive	File from Network Shared Drive	File from Network Shared Drive
Supply Chain Compromise	Exploitation for Client Execution	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Desktop Protocol	Domain Fronting	Domain Generation Algorithms	Scheduled Transfer	Domain Generation Algorithms
Trusted Relationship	Exploit for Interface	Change Default File Association	File System Permissions Weakness	Component Object Model Hijack Input Prompt	Peripherals Discovery	Remote Services	Input Capture	Fallback Channels	Network Denial of Service	Network Denial of Service	Network Denial of Service
Valid Accounts	InstallUtil	Component Object Model Hijack Input Prompt	Control Panel Items	Control Panel Items	Peripherals Discovery	Replication Through Removable & Man in the Browser	Input Capture	Multi-hop Proxy	Resource Hijacking	Run-time Data Manipulation	Run-time Data Manipulation
	Launchctl	Component Object Model Hijack Image File Execution Options Injec	Kernel Driver	Kerberasting	Peripherals Discovery	Pass the Hash	Logon Scripts	Multi-Hop Channels	Service Stop	Service Stop	Service Stop
	Local Job Scheduling	Component Object Model Hijack Image File Execution Options Injec	Launch Daemon	Keychain	Peripherals Discovery	Pass the Hash	Logon Scripts	Multi-Band Communication	Stored Data Manipulation	Stored Data Manipulation	Stored Data Manipulation
	LSASS Driver	Component Object Model Hijack Image File Execution Options Injec	DLL Search Order Hijacking	Query Registry	Peripherals Discovery	Pass the Hash	Logon Scripts	Multilayer Encryption	Transmitted Data Manipulation	Transmitted Data Manipulation	Transmitted Data Manipulation
	Mhba	Component Object Model Hijack Image File Execution Options Injec	Hooking	SSH Hijacking	Peripherals Discovery	Pass the Hash	Logon Scripts	Port Knocking	Transmitted Data Manipulation	Transmitted Data Manipulation	Transmitted Data Manipulation
	PowerShell	Dylib Hijacking	Path Interception	Shared Webroot	Peripherals Discovery	Pass the Hash	Logon Scripts	Remote Access Tools	Transmitted Data Manipulation	Transmitted Data Manipulation	Transmitted Data Manipulation
	Regsvcs/Regasm	External Remote Services	Plist Modification	Screen Capture	Peripherals Discovery	Pass the Hash	Logon Scripts	Remote File Copy	Transmitted Data Manipulation	Transmitted Data Manipulation	Transmitted Data Manipulation
	Regsvr32	File System Permissions Weakness	Plist Modification	Video Capture	Peripherals Discovery	Pass the Hash	Logon Scripts	Standard Application Layer Protocol	Transmitted Data Manipulation	Transmitted Data Manipulation	Transmitted Data Manipulation
	Rundll32	Hidden Files and Directories	Process Injection	Security Software Discovery	Peripherals Discovery	Pass the Hash	Logon Scripts	Standard Cryptographic Protocol	Transmitted Data Manipulation	Transmitted Data Manipulation	Transmitted Data Manipulation
	Scheduled Task	Hooking	Exploitation for Defense Evasion	Third-party Software	Peripherals Discovery	Pass the Hash	Logon Scripts	Standard Non Application Layer Protocol	Transmitted Data Manipulation	Transmitted Data Manipulation	Transmitted Data Manipulation
	Scripting	Scheduled Task	Two-Factor Authentication Inter	Taint Shared Content	Peripherals Discovery	Pass the Hash	Logon Scripts	Uncommonly Used Port	Transmitted Data Manipulation	Transmitted Data Manipulation	Transmitted Data Manipulation
	Service Execution	Image File Execution Options Injec Setuid and Setgid	Service Registry Permissions Weak	Windows Admin Shares	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
	Signed Binary Proxy Execution	Kernel Modules and Extensions	File Permissions Modification	System Information Discovery	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
	Signed Script Proxy Execution	SID-History Injection	File System Logical Offsets	System Network Configuration Dis	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
	Source	Launch Agent	Startup Items	Group Policy Modification	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
	Space after Filename	Launch Daemon	Sudo	Hidden Files and Directories	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
	Third-party Software	Launchctl	Sudo Caching	Securityd Memory	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
	Trap	LC_LOAD_DYLIB Addition	Valid Accounts	Shared Webroot	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
	Trusted Developer Utilities	Local Job Scheduling	Web Shell	Service Registry Permissions Weak	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
	User Execution	Login Item		File Permissions Modification	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
	Windows Management Instrumentation	Logon Scripts		HISTCONTROL	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
	Windows Remote Management	LSASS Driver		Image File Execution Options Injec	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
	XSL Script Processing	New Service		Indicator Blocking	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
		Office Application Startup		Indicator Removal from Tools	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
		Path Interception		Indicator Removal on Host	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
		Plist Modification		Indirect Command Execution	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
		Port Knocking		Install Root Certificate	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
		Port Monitors		Launchctl	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
		Rc.common		LC_MAIN Hijacking	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
		Re-opened Applications		Masquerading	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
		Redundant Access		Modify Registry	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
		Registry Run Keys / Startup Folder		Msha	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
		Scheduled Task		Network Share Connection Removal	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
		Screensaver		NFTS File Attributes	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
		Security Support Provider		Obfuscated Files or Information	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
		Service Registry Permissions Weakness		Plist Modification	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
		Setuid and Setgid		Port Knocking	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
		Shortcut Modification		Process Doppelgänging	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
		SIP and Trust Provider Hijacking		Process Hollowing	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
		Startup Items		Process Injection	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
		System Firmware		Redundant Access	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
		Systemd Service		Regsvcs/Regasm	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
		Time Providers		Regsvr32	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
		Trap		Rootkit	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
		Valid Accounts		Rundll32	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
		Web Shell		Scripting	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
		Windows Management Instrumentation Event Subscription		Signed Binary Proxy Execution	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
		Winlogon Helper DLL		Signed Script Proxy Execution	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
				SIP and Trust Provider Hijacking	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
				Software Packing	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
				Space after filename	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
				Template Injection	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
				Timestamp	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
				Trusted Developer Utilities	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
				Valid Accounts	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
				Virtualization/Sandbox Evasion	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
				Web Service	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service
				XSL Script Processing	Peripherals Discovery	Pass the Hash	Logon Scripts	Web Service	Web Service	Web Service	Web Service

- Construction and Engineering



#WeFightBullies

Quorum Cyber

2) TTPs

ATT&CK®

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

- Targeting Middle East



#WeFightBullies

Quorum Cyber

3) Map Current Capabilities

ATT&CK®

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

#WeFightBullies

Q
Quorum Cyber

4) Heatmap

ATT&CK®

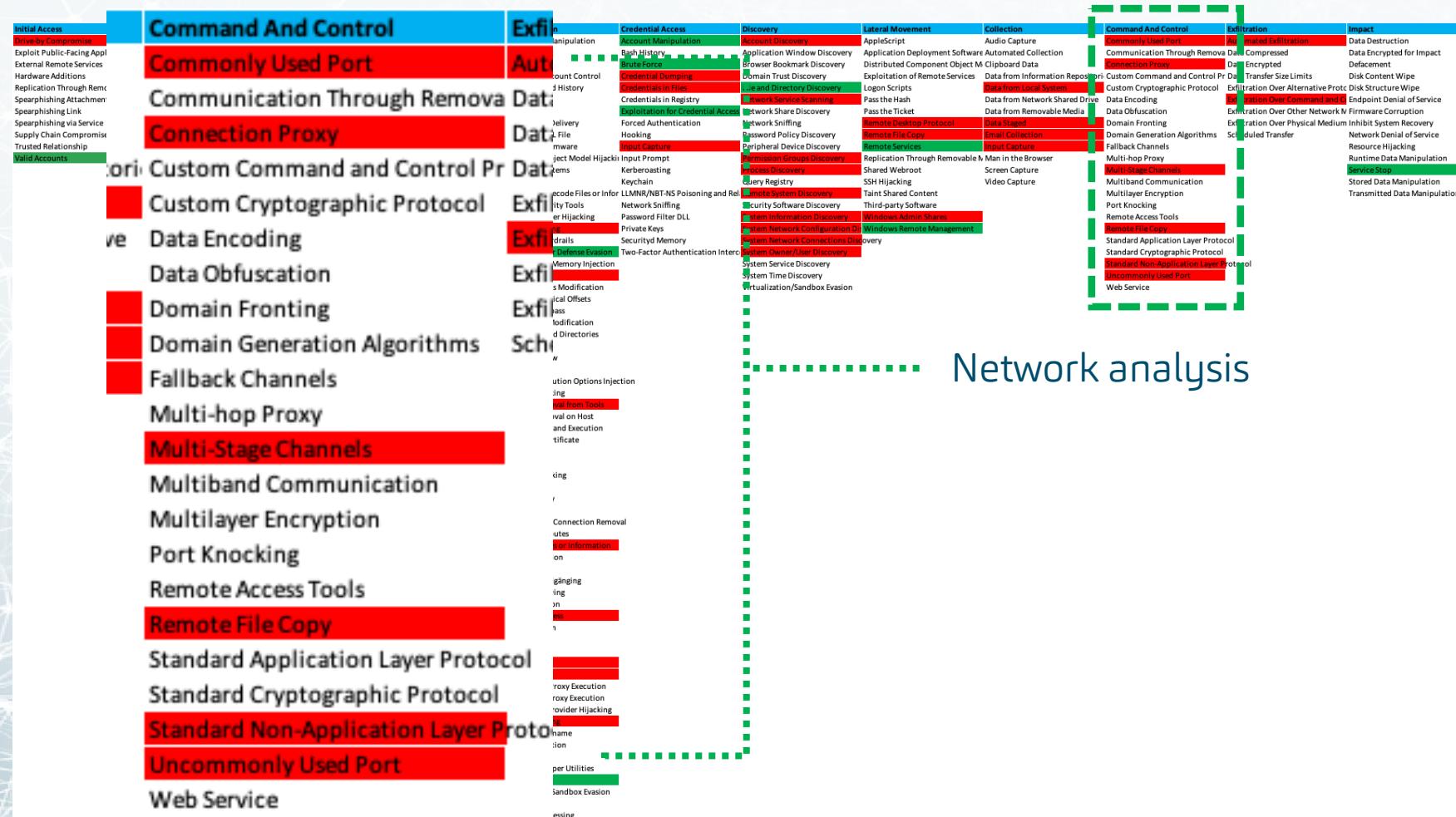
#WeFightBullies



Quorum Cyber

5) Telemetry and Controls

ATT&CK®



Network analysis

#WeFightBullies



Quorum Cyber

So now we have...

ATT&CK®

1. A list of relevant actors
2. A list of relevant TTPs
3. Positive coverage (list of things we know we can find)
4. Known blind spots (list of things we know we can't find)
5. A list of controls to mitigate those blind spots (investment needs)
6. How do we drive investment?

#WeFightBullies



SOC Framework

ATT&CK®



7 Threat actors



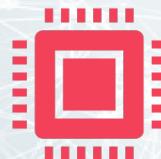
50 TTPs, 150 IOCs



45 IOCs - confirmed



105 IOCs - blind



7 Controls (750K CAPEX)
4 Controls (350K OPEX)

#WeFightBullies



Risk Coverage
30%



Residual risk
70%



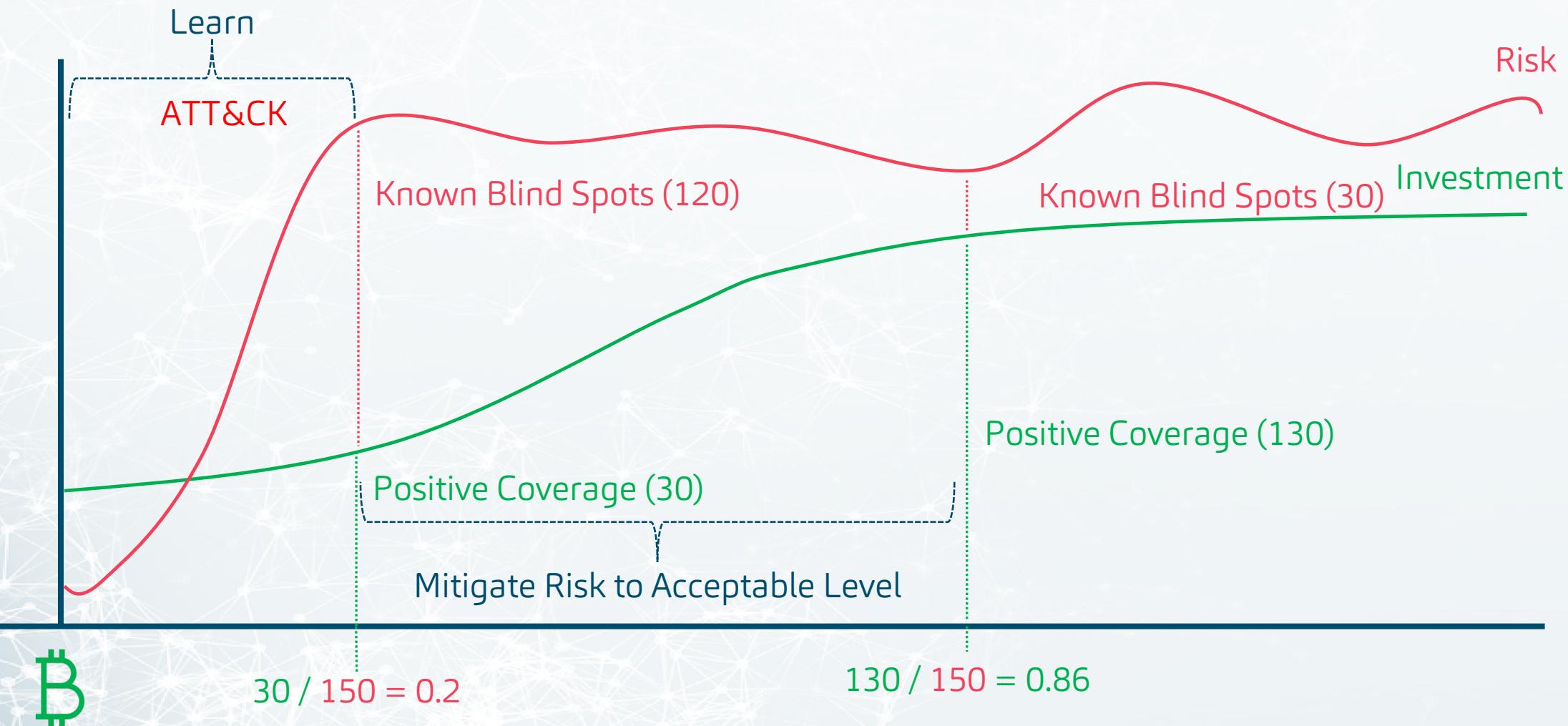
Performance of
Investment
(Confirmed / Known)



Quorum Cyber

Performance of Investment

ATT&CK®



ATT&CK®



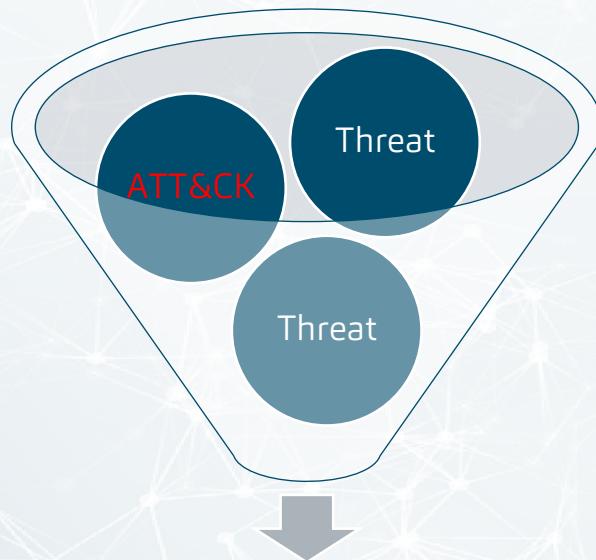
#WeFightBullies

Q
Quorum Cyber

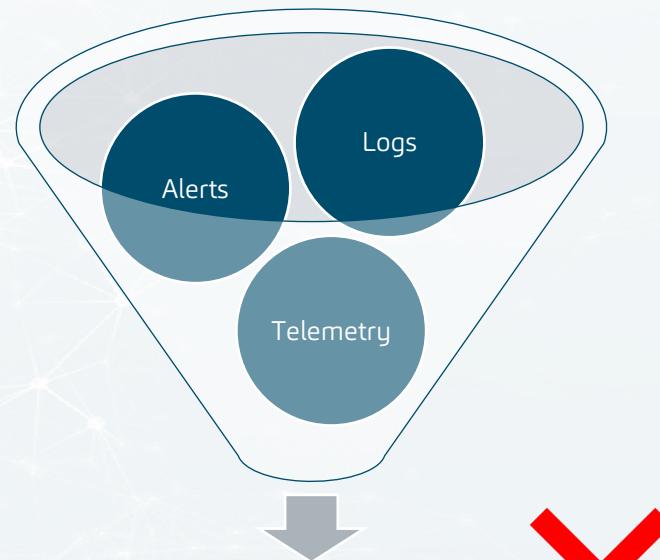
1) Threat-focused SOC (not volume)

ATT&CK®

- Your threats should determine the signals and telemetry you need (not the other way around!)



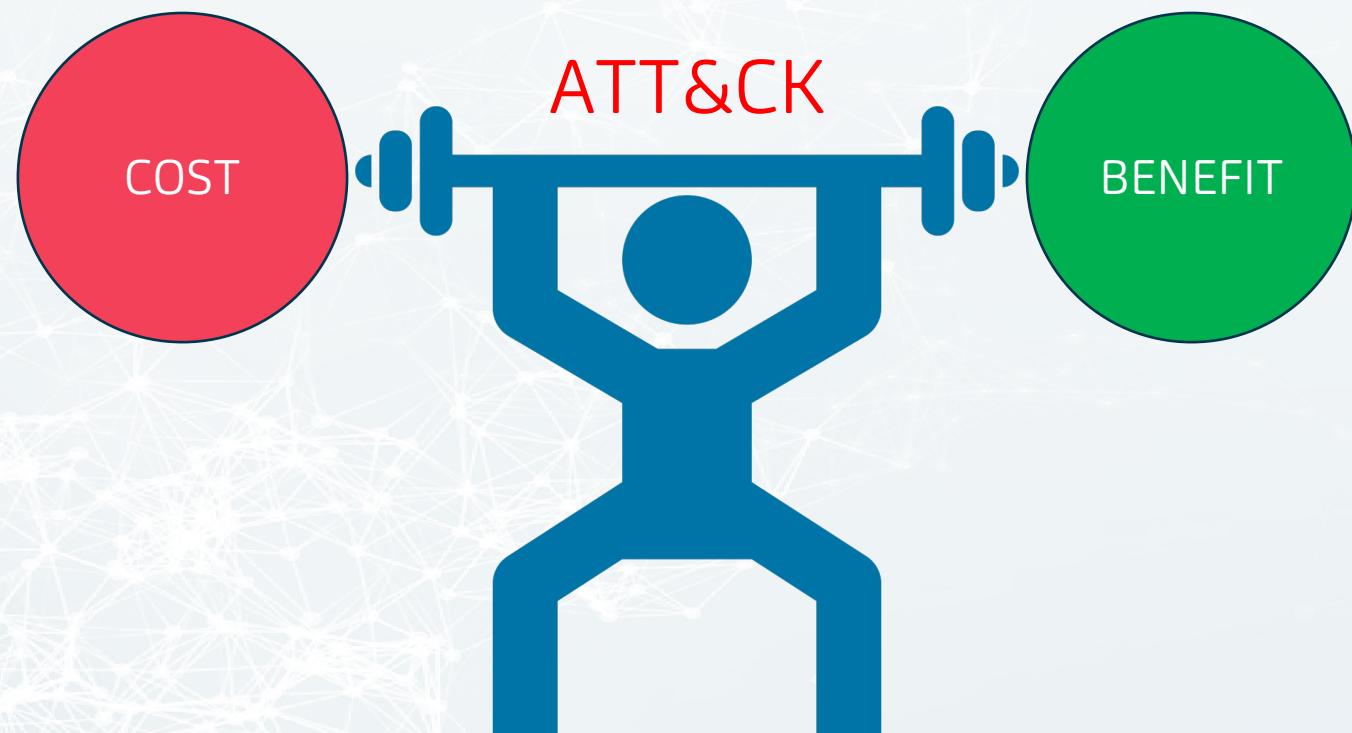
#WeFightBullies



2) Investment Performance

ATT&CK®

- Measuring risk coverage and investment performance is essential to communicating the **Business Value** of the SOC



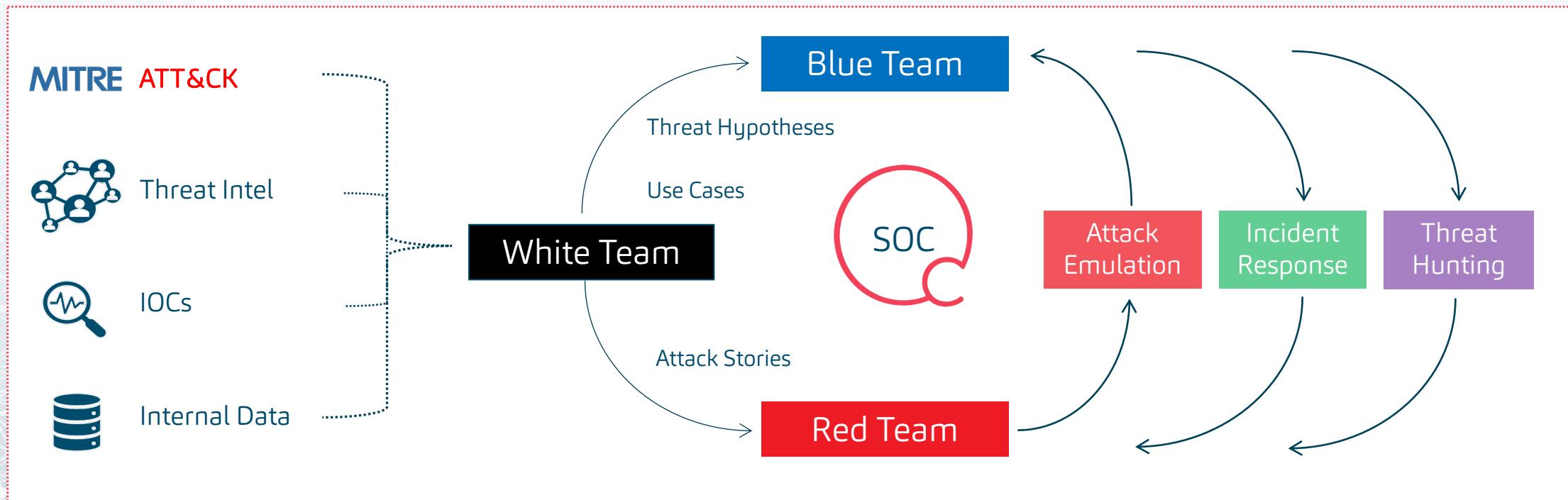
#WeFightBullies

Q
Quorum Cyber

3) Continuous Improvement

ATT&CK®

- A SOC is a living, breathing organism: ATT&CK Threat Modelling is the key for continuous improvement!



#WeFightBullies



Thank You!

Federico Charosky

Federico.Charosky@quorumcyber.com

@FedeCharosky

#WeFightBullies