

INCREASE YOUR SECURITY VISIBILITY WITH THE MITRE ATT&CK FRAMEWORK

BY ERAN ALSHEH CTO, CYBERPROOF

JULY, 2019

TABLE OF CONTENTS

KEY TAKEAWAYS
WHAT IS THE MITRE ATT&CK?
WHY IS THE MITRE ATT&CK IMPORTANT TO CYBER SECURITY?6
USING MITRE ATT&CK TO PRIORITIZE DETECTION7
1. MAPPING ATTACK METHODOLOGIES8
2. IDENTIFYING GAPS NOT COVERED BY THE CUSTOMER'S EXISTING RULES
3. UNCOVERING NEW THREATS
4. PROACTIVELY PROVIDING NEW DETECTION RULES
USING THE MITRE ATT&CK TO TRACK CHANGES IN RISK11



KEY TAKEAWAYS

The MITRE ATT&CK is a powerful foundation for developing threat models and incident response methodologies for security operations teams.

For each customer, CyberProof maps out and baselines the detection rules of the organization's SIEM and network data and highlights gaps in the security posture in the form of a custom heatmap.

CyberProof continuously researches and identifies new tactics and techniques and contributes new detection rules to improve the customer's security coverage.

By utilizing the matrix together with our advanced threat intelligence capabilities, CyberProof provides customers with the ability to quantify risk and maintain full risk posture on a continuous basis. CyberProof leverages the MITRE ATT&CK to map out where organizations are protected and where they are vulnerable to attack.

CyberProof continuously provides new detection rules and playbooks, based on the identified gaps. This leads to greater security visibility and reduced risk level.

CyberProof creates a customized version of the MITRE ATT&CK that is contextual and specific to the unique threats and vulnerabilities of the organization. This is comprised of the standard matrix, and those threats uncovered by the Threat Intelligence Team which are customer and environment specific.

WHAT IS THE MITRE ATT&CK?

MITRE ATT&CK is a knowledge base of adversary tactics and techniques based on real-world observations. It defines and groups TTPs (tactics, techniques, and procedures) used by hackers and is a powerful and insightful foundation for developing threat models and methodologies.

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	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	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	Binary Padding	Baste Force	Browser Bookmark	Distributed Component	Cliphoard Data	Connection Proxy	Data Encrypted	Defacement
						Discovery	Object Model Exploitation of Remote		Custom Command and		
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Services	Data Staged	Control Protocol	Data Transfer Size Limits	Disk Content Wipe
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	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account	Clear Command History	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System		Exfiltration Over Command and	Endpoint Denial of
			Control		Exploitation for Credential			Data from Network		Control Channel Exfiltration Over Other Network	Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Access	Network Share Discovery	Pass the Ticket	Shared Drive	Data Obfuscation	Medium	Firmware Corruption
Spearphishing via Service	Execution through Module	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data from Removable Media	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client	Bootkit	Exploitation for Privilege	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of
	Execution		Escalation Extra Window Memory							Scheduled Hanster	Service
Trusted Relationship	Graphical User Interface	Browser Extensions	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-Stage Channels		Runtime Data Manipulation
	LSASS Driver	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	SSH Hijacking	Screen Capture	Multi-hop Proxy		Service Stop
	Launchetl	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	Shared Webroot	Video Capture	Multiband Communication		Stored Data Manipulation
	Local Job Scheduling	Create Account	Launch Daemon	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning	Remote System Discovery	Taint Shared Content		Multilayer Encryption		Transmitted Data
	Local Job Scheduling Mshta		Launch Daemon	DLL Search Order Hijacking	and Relay	Remote System Discovery Security Software Discovery					Manipulation
		DLL Search Order Hijacking		DLL Side-Loading Deobfuscate/Decode Files or	Network Sniffing	Security Software Discovery System Information	Third-party Software		Port Knocking		
	PowerShell	Dylib Hijacking	Path Interception	Information	Password Filter DLL	Discovery	Windows Admin Shares		Remote Access Tools		
	Regsvcs/Regasm	External Remote Services	Plist Modification	Disabling Security Tools	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			Standard Application Layer		
					Two-Factor Authentication	Connections Discovery System Owner/User			Protocol Standard Cryptographic		
	Rundli32	Hidden Files and Directories	Process Injection	Evasion	Interception	Discovery			Protocol		
	Scheduled Task	Hooking	SID-History Injection	Extra Window Memory Injection		System Service Discovery			Standard Non-Application Layer Protocol		
	Scripting	Hypervisor	Scheduled Task	File Deletion		System Time Discovery			Uncommonly Used Port		
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	File Permissions Modification		Virtualization/Sandbox Evasion			Web Service		
	Signed Binary Proxy	Kernel Modules and Extensions	Setuid and Setgid	File System Logical Offsets		Lingion					
	Execution Signed Script Proxy	Kerner moudles and Extensions	Setulu anu Setgiu								
	Execution	LC_LOAD_DYLIB Addition	Startup Items	Gatekeeper Bypass							
	Source	LSASS Driver	Sudo Caching	Group Policy Modification HISTCONTROL							
	Space after Filename Third-party Software	Launch Agent Launch Daemon	Sudo Valid Accounts	HISTCONTROL Hidden Files and Directories							
	Trap	Launchetl	Web Shell	Hidden Users							
	Trusted Developer Utilities	Local Job Scheduling		Hidden Window							
	User Execution	Login Item		Image File Execution Options Injection							
	Windows Management Instrumentation	Logon Scripts		Indicator Blocking							
	Windows Remote	Modify Existing Service		Indicator Removal from							
	Management XSL Script Processing	Netsh Helper DLL		Tools Indicator Removal on Host							
	XSL Script Processing	New Service		Indirect Command Execution							
		Office Application Startup		Install Root Certificate							
		Path Interception Plist Modification		InstallUtil LC_MAIN Hijacking							
		Port Knocking		Launchetl							
		Port Monitors		Masquerading							
		Rc.common Re-opened Applications		Modify Registry Mshta							
		Redundant Access		NTFS File Attributes							
		Registry Run Keys / Startup Folder		Network Share Connection Removal							
		SIP and Trust Provider Hijacking		Obfuscated Files or							
		SIP and Trust Provider Hijacking		Information Plist Modification							
		Scheduled Task Screensaver		Plist Modification Port Knocking							
		Security Support Provider		Process Doppelgänging							
		Service Registry Permissions Weakness Setuid and Setuid		Process Hollowing Process Injection							
		Shortcut Modification		Redundant Access							
		Startup Items		Regsvcs/Regasm							
		System Firmware Systemd Service		Regsvr32 Rootkit							
		Time Providers		Rundll32							
		Trap		SIP and Trust Provider Hijacking							
		Valid Accounts		Scripting							
		Web Shell		Signed Binary Proxy							
		Windows Management Instrumentation		Execution Signed Script Proxy							
		Event Subscription		Execution							
		Winlogon Helper DLL		Software Packing Space after Filename							
				Template Injection							

MITRE Enterprise ATT&CK Framework

copyright: 2018 The MITRE Corporation.



Initial Access			Privilege Escalation	Defense Evasion	Credential Access		Lateral Movement	Collection	
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection 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	Custom Command and Control Protocol
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	Custom Cryptographic Protocol
pearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Data Encoding
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 Network Shared Drive	Data Obfuscation
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data from Removable Media	Domain Fronting
upply 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 Algorithm

Tactics in the MITRE Enterprise ATT&CK Framework

For each tactic, there is a list of known techniques:

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control
Drive-by Compromise		.bash_profile and .bashrc	Access Token Manipulation		Account Manipulation	Account Discovery	and the second se	Audio Capture	Commonly Used Port
Drive-by Compromise	AppleScript	.basn_profile and .basnrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection 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	Custom Command and Control Protocol
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	Custom Cryptographic Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Data Encoding
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 Network Shared Drive	Data Obfuscation
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data from Removable Media	Domain Fronting
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 Algorith

MITRE ATT&CK Techniques



WHY IS THE MITRE ATT&CK IMPORTANT TO CYBER SECURITY?

The MITRE ATT&CK framework is used to identify and map out which threats an organization is currently protected against, and then uncovers where it's vulnerable to attack. CyberProof builds upon the matrix, using various threat intelligence means, to identify new threats and provide a unique means of prioritizing response based on risk.

The CyberProof Threat Intelligence (CTI) Team works to discover additional types of attacks. By thinking like a hacker and conducting in-depth research, the CTI team is able to learn about new tactics and techniques for attack and CyberProof's remediation team can develop detection & response controls and actions to remediate against these kinds of attack.

Using the MITRE ATT&CK as the basis, we add each new threat found to the enterprise matrix – and create a new, customer-specific version of the matrix that maps out the threats we've discovered that are most relevant to each organization.



USING MITRE ATT&CK TO PRIORITIZE DETECTION

The enterprise matrix is valuable as a methodology – a means of allowing us to stay focused on how hackers work, of uncovering their TTPs, and of mapping out what methods they are likely to use in an attack on a particular customer. We continuously adapt our existing digital playbooks and add new ones, and our AI engine learns new ways to automate more steps of the playbook – to continuously reduce dwell time and reduce false positive results.



Pyramid of Pain

The hierarchy of the pyramid of pain reflects how much time, effort, and resources are required for a hacker to develop a replacement for a given method of attack. Because TTPs are at the top of the cyber pyramid, they require the greatest amount of time, effort, and resources to develop and, therefore, they are hardest for hackers to change.

By figuring out how to block TTPs, we provide our customers with robust cyber protection and offer them the ability to reduce risk. By mapping out TTPs and adding new detection rules that identify them, we are able to quantify and track improvements in risk level.





Let's have a look at exactly how CyberProof uses the MITRE ATT&CK to reduce the risk of attack:

MAPPING ATTACK METHODOLOGIES

As part of the onboarding process for a new customer, CyberProof conducts a detailed cyber assessment that includes manually conducted interviews, questionnaires, and a tools survey. The CyberProof Defense Center (CDC) platform provides automated log analysis to help drill down and identify existing data sources and detection rules.

This important process helps the CyberProof team identify which detection rules (if any) already are defined in the customer's SIEM. CyberProof then conducts a gap analysis. The team does the following:

- 1. Takes all of the detection rules that the customer has available.
- 2. Uses automatic tools to map out how the SIEM's off-the-shelf rules relate to the techniques in the MITRE ATT&CK.
- 3. Maps the customer's custom SIEM detection rules to the MITRE ATT&CK.
- 4. Maps the capabilities of other customer tools to the matrix, including EDR, BAS, etc.
- 5. While most of the above is automated, the CyberProof on-boarding team then does a manual review, looking further at each detection rule and identifying additional mapping possibilities not discovered through the automatic process.



This process provides a clear, visual heatmap indicating where the organization is protected and where it is most vulnerable. Areas of the heatmap marked in red indicate a lack of detection; areas marked in green indicate the presence of full detection capabilities; and areas marked in orange reflect partial detection capabilities. Because the heatmap relates to a specific time period, there must be a continuous cycle of update and review.

N1 end S1 ends	Initial Access	Execution	Persistence	Privilege	Defense	Credential	Discovery	Lateral	Collection	Exfiltration	Command and
Anisons<	0 items	33 items	58 items	Escalation	Evation	Access	20 items	Movement	13 items	9 items	Control
concordingfor a lationManipulationManipulationManipulationDiscoveryFund on the left and											
Baking with any and any and any and any and any any and any		Applescript				Manipulation	Discovery	Applescript	Audio Capture		
Mathematical Backersonal<	Public-Facing	CMSTP	Accessibility Features		Binary Padding	Bash History	Window	Deployment	Automated Collection	Data Compressed	Removable
Barchard Formation Formation Backney Barchard Reparation			Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Bookmark	Component			Connection Proxy
Name Istantinuity Spinomical Control File Section Section Control Including Section Control Control Description Section Control Control Description Section Control Control Description Section Control Control Description Section Control Control Description Section Control Control Description Section Control Description Section Control Section Section Control Section Control Section Control Section Control Section Control Section Control Section Control Section Control Section Control Section Control S	Through Removable	Compiled HTML File	AppCert DLLs	AppInit DLLs	Account		Directory	of Remote	Information		Custom Command and Control Protoco
Link Finkmanna Schwannina Schwannin Schwannin			AppInit DLLs	Application Shimming	Command		Service	Logon Scripts		Over Alternative	Cryptographic
via serviceUnwaphPackageOptimizeting light magnetingConcordential proceedential serviceStaffingPackageDeter the packageDeter the package </td <td>Spearphising Link</td> <td>Dynamic Data Exchange</td> <td>Application Shimming</td> <td>Account</td> <td>CMSTP</td> <td>Credentials in Registry</td> <td>Network Share Discovery</td> <td>Pass the Hash</td> <td>Network</td> <td>Over Command and Control</td> <td>Data Encoing</td>	Spearphising Link	Dynamic Data Exchange	Application Shimming	Account	CMSTP	Credentials in Registry	Network Share Discovery	Pass the Hash	Network	Over Command and Control	Data Encoing
Camponine Monodify Higksking Hill Fill Authentication Ballow Packog Decktog Decktog <thdecktog< th=""> <thdecktog< th=""> Deckt</thdecktog<></thdecktog<>				Order	Code Signing	for Credential		Pass the Ticket	Removable	Over Other Netwrok	
Relationship For Cillection For Copy Copy Collection Transfer Channels Valid Accounts Graphical Uries Browser Edita Windows Option Input Capiture Input	Supply Chain Compromise	through	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Policy	Desktop	Data Staged	Over Physical	Domain Fronting
Interface Extensions Memory Melection Object Model Forume Figure		for Client	Bootkit	for Privilege		Hooking	Device				
File Association Permissions Items File Association Proviser Browser Browser Channels Launchett Component Hooking DCShadow Kerbenasting Query Registry Shared Screen Amedia Component Multiband Local 20 Opponent Image File Deoblecation Repetitor Shared Stared Creen Capture Component Multiband Local 20 Opponent Image File Deoblecation Repetitor Shared Stared Creen Component Multiband Local 20 Opponent Image File Deoblecation Repetitor Stared	Valid Accounts			Memory	Object Model	Input Capture	Groups		Input Capture		Multi-hop Proxy
Indication Finitware Finitware Finitware Finitware Finitware Finitware Communication Local Job Component Hijscking Component Hijscking Deebdarsette/ Deibning Security Security Toos Set Hijscking Video Capure Multilayer Intercent LSASS Driver Create Account Dawnoh Security Toos Security Toos Security Toos Taint Shared Intercent Port Knocking Mahta DLL Search Order Hijscking New Service DLL Search Hijscking Network System Discovery Taint Shared Intercent Remote Capure Mahta DLL Search Order Hijscking New Service DLL Search Hijscking Network System Discovery Taint Shared Inter- Femote File Remote Season Due Service Network System Hijsching System System Versione System Network Taint Shared Inter- Femote File Remote Season Poito Hijsching Poito Hige Dasword File System Network Windows Admins fairs System Network Mindows Inter- System Poitocol Mindows Inter- System Poitocol Network System		InstallUtil	Change Default File Association	Permissions		Input Prompt		Through Removable			Multi-Stage Channels
Scheduling Object Model Hjack Mg Execution Decode Files Decode Files Dissoling System Software Tail Share Interception Encryption LSASS Driver Create Account Juan Jisabiling Sisbiling Software Contect Contect Port Moncking Mshta DLL Search Order Hijacking New Service DLL Search Order Hijacking Network High Anno System Discount Tail Shared Tail Shared Tail Shared Tail Shared Port Moncking PowerShell DLJ Search Order Hijacking Network Interception System Discount Tail Shared Tail Shared <t< td=""><td></td><td>Launchctl</td><td></td><td>Hooking</td><td>DCShadow</td><td>Kerberoasting</td><td>Query Registry</td><td></td><td>Screen Capture</td><td></td><td>Multiband Communication</td></t<>		Launchctl		Hooking	DCShadow	Kerberoasting	Query Registry		Screen Capture		Multiband Communication
Image: Security Tools Poisoning Software Contect <			Object Model	Execution Options	Decode Files	Keychain	System	SSH Hijacking	Video Capure		
IndexOrder HijackingOrder HijackingSniffingInformation InformationSoftwareSoftwareToolsPowerShellDylib HijackingPath InterceptionDLL Side- LoadingPassword Filter DLLSystem Network ConectionsWindows Admin SharesRemote File CopyRegasmExternal RegasmPilet ServicesPilet System Port MolificationPrivate KeysSystem Network ConectionsWindows Memote Memote MemoteWindows Memote MemoteWindows Memote MemoteSystem Memote MemoteWindows Memote MemoteWindows Memote MemoteWindows MemoteSystem Memote MemoteWindows Memote MemoteWindows MemoteSystem Memote MemoteWindows MemoteSystem Memote MemoteWindows MemoteSystem MemoteWindows MemoteSystem MemoteWindows MemoteSystem MemoteWindows MemoteSystem MemoteWindows MemoteSystem MemoteWindows MemoteSystem MemoteWindows MemoteSystem MemoteWindows MemoteSystem MemoteWindows MemoteSystem MemoteWindows MemoteSystem MemoteWindows MemoteSystem MemoteWindows MemoteSystem MemoteWindows MemoteSystem MemoteWindows MemoteSystem MemoteWindows MemoteSystem MemoteWindows MemoteSystem MemoteWindows MemoteSystem MemoteWindows MemoteSystem MemoteSystem M		LSASS Driver	Create Account			LLMNR/NBT-NS Poisoning	Software				Port Knocking
InterceptionLoadingDLLNetwork ObscoveryAdmin SharesCompCopyRegswr.5/External ServicesPiotSyloitation Exploitation EvasionPrivate KeysSystem ManagementMindowsServicesStapplard Applard ConnectionsManagementServicesStapplard Applard ConnectionsRegswr.32File System 		Mshta	DLL Search Order Hijacking	New Service	Order	Network Sniffing	Information				Remote Access Tools
Regasm Remote Services Remote Weakness Remote Weakness Remote Management Remote Management Remote Management Remote Management Application Appletion Regsvr32 File System Veakness Port Monitors Extra Window Memory Securityd Memory Securityd Memory <td></td> <td>PowerShell</td> <td>Dylib Hijacking</td> <td></td> <td></td> <td></td> <td>Network Configuration</td> <td></td> <td></td> <td></td> <td></td>		PowerShell	Dylib Hijacking				Network Configuration				
Permissions Memory Memory Memory Memory Memory Memory Cryptographic Rundll32 Hidden Files and Directories Process Injection File Deletion Two-Factor Authentication Interception Two-Factor Image: Cryptographic Scheduled Task Scheduled Task Scheduled Task Scheduled Task File Permissions Memory Image: Cryptographic Scripting Scheduled Task Scheduled Task Scheduled Task File System Logical offsets Image: Cryptographic Scripting Image: Cryptographic File System Logical offsets Image: Cryptographic Service Execution Image: Cryptographic File System Logical offsets Image: Cryptographic Bignady Bignady Proxy Execution Image: Cryptographic File System Logical offsets Image: Cryptographic Image: Cryptographic File System Logical offsets File System Logical offsets Image: Cryptographic Image: Cryptographic Gatekeeper Bypass File System Logical offsets Image: Cryptographic Image: Cryptographic Hidden Files Hidden Files Image: Cryptographic Image: Cryptographic		Regsvcs/ Regasm	Remote	Plist Modification	for Defense	Private Keys	Network	Remote			Standard Application Layer Protocol
Injection Injection Authentication Interception Scheduled Task Hooking Task Scheduled Task File Permissions Modification File Permissions Modification Scripting File Stefe File Scripting File Stefe Service File Stefe Service File Stefe Signed Binary Proxy Execution File		Regsvr32	Permissions	Port Monitors	Extra Window Memory Injection	Securityd Memory					Standard Cryptographic Protocol
Task Task Permissions Modification Scripting Scripting File System Logical Offsets Service Execution Service Execution Signed Binary Proxy Execution Signed Binary Proxy Execution Image: Signed Binary Proxy Execution			and Directories	Injection		Authentication					
Service		Task	Hooking		Permissions Modification						
Signed Binary Proxy Execution		Service			Logical Offsets Gatekeeper						
		Signed Binary Proxy			Hidden Files						

Visual Heatmap

2 IDENTIFYING GAPS NOT COVERED BY THE CUSTOMER'S EXISTING RULES

Once the mapping process is complete, CyberProof identifies all of the TTPs listed in the MITRE ATT&CK that might be relevant to the customer.

CyberProof integrates its own detection rules into the customer's SIEM, and customizes the digital playbooks in the CyberProof Defense Center platform. This reduces the customer's level of risk by increasing the detection capabilities and improves response times - mean time to detect (MTTD) and mean time to respond (MTTR).

UNCOVERING NEW THREATS

In addition to working on threats that already appear in the MITRE ATT&CK, CyberProof conducts in-depth threat analysis, identifying what new kinds of tactics and techniques hackers may be planning. The evaluation takes into consideration the customer's industry, location, and many other variables.

CyberProof develops an understanding of which potential threats are most relevant, prioritizes all known threats on a per-customer basis, maps them to the enterprise matrix, and creates a tailor-made heat map that illustrates which of the cyber threats potentially are the most dangerous.

PROACTIVELY PROVIDING NEW DETECTION RULES

Once CyberProof has mapped out which threats are not addressed, the team provides new detection rules. Here's the procedure CyberProof follows for providing detection rules for each new TTP that our analysts discover:

- 1. CyberProof's threat intelligence analysts expose previously-unknown threats identifying new hacking TTPs and documenting them.
- 2. The new TTPs are added to the customer's own instance of the MITRE ATT&CK.
- 3. At the CyberProof research lab, the red team runs simulations of the threat attack.
- 4. The new tactic or technique is simulated in CyberProof's lab, and the team documents the behavior of the threat, extracting IoCs and evaluating its potential impact.
- 5. New detection rules are developed by the blue team and deployed in the lab that identify the threat.
- 6. Playbooks are prepared that define the process to follow if the attack takes place.
- 7. The attack is simulated again by the red team to validate that the new detection rules successfully identify it.
- 8. The team informs the customer of each threat it discovers, and recommends new detection rules to be added to the customer's SIEM proactively protecting the organization, and reducing the level of risk.



USING THE MITRE ATT&CK TO TRACK CHANGES IN RISK

CyberProof's goal is to improve the risk status of each customer. Using the enterprise matrix, CyberProof provides a quantifiable understanding of the organization's degree of risk – increasing threat landscape visibility by allowing clear insight into which threats the organization is protected against, and which threats continue to present a danger.

By utilizing the MITRE ATT&CK and leveraging its advanced threat intelligence capabilities, CyberProof offers continuous visibility of risk posture.



This helps customers set goals and monitor improvement in coverage. With each additional detection rule and playbook provided by CyberProof, a customer is able to visualize the shift, and view the reduction in the number of TTPs for which the organization is vulnerable. Thus, leveraging the MITRE ATT&CK opens the door for decision-making based on a quantified understanding of the threat landscape, and allows an organization to track how its detection & response capabilities improve over time.



ABOUT CYBERPROOF

CyberProof's advanced cloud-based orchestration and automation platform drives operational efficiency, allowing our nation-state cyber experts to remain focused on each individual threat. In the face of a hostile and evolving threat environment, CyberProof integrates all the key elements you need to detect & prioritize threats early while both rapidly and decisively responding.

CyberProof is part of the UST Global family. Some of the world's largest enterprises trust us to create and maintain secure digital ecosystems using our comprehensive cyber security platform and mitigation services.

For more information, visit our website at <u>www.cyberproof.com</u> or reach out to us at: <u>info@cyberproof.com</u>

LOCATIONS

Aliso Viejo | London | Tel Aviv | Trivandrum | Singapore

