CyberProof™

INCREASE YOUR SECURITY VISIBILITY WITH THE MITRE ATT&CK FRAMEWORK

BY ERAN ALSHEH
CTO, CYBERPROOF

JULY, 2019

TABLE OF CONTENTS

KEY TAKEAWAYS

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

2. 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.

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

4. 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.

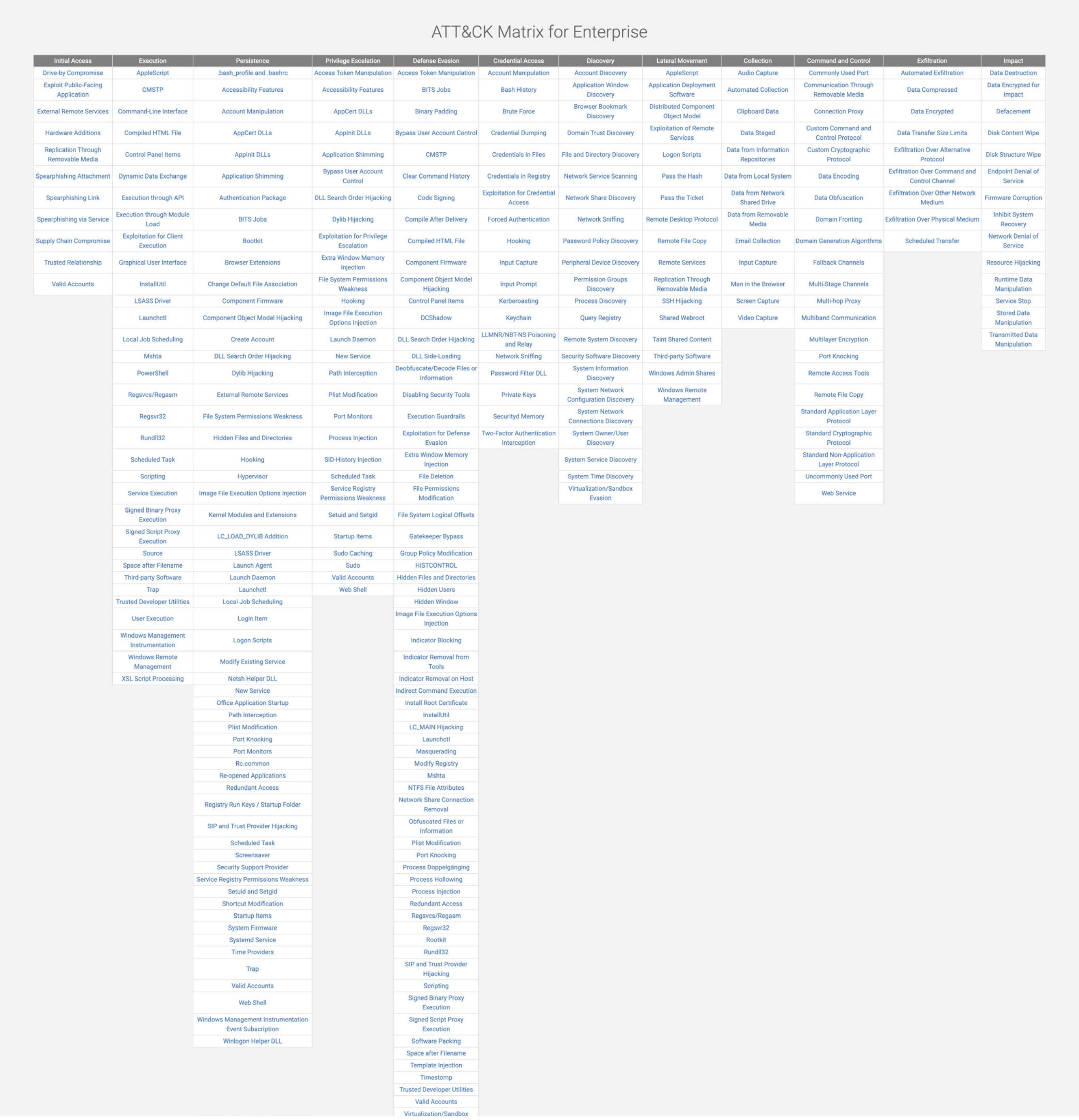
5. CyberProof leverages the MITRE ATT&CK to map out where organizations are protected and where they are vulnerable to attack.

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

7. 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.

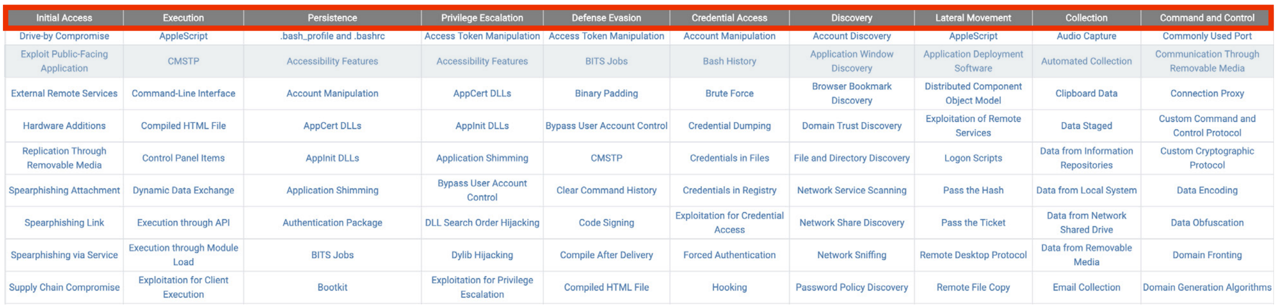


ATT&CK Matrix for Enterprise

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	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 Staged	Custom Command and 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 Control	Clear Command History	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	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 Network Shared Drive	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 from Removable Media	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-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
	Launchctl	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 and Relay	Remote System Discovery	Taint Shared Content		Multilayer Encryption		Transmitted Data Manipulation
	Mshta	DLL Search Order Hijacking	New Service	DLL Side-Loading	Network Sniffing	Security Software Discovery	Third-party Software		Port Knocking		
	PowerShell	Dylib Hijacking	Path Interception	Deobfuscate/Decode Files or Information	Password Filter DLL	System Information 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 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	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 Execution	Kernel Modules and Extensions	Setuid and Setgid	File System Logical Offsets							
	Signed Script Proxy Execution	LC_LOAD_DYLIB Addition	Startup Items	Gatekeeper Bypass							
	Source	LSASS Driver	Sudo Caching	Group Policy Modification							
	Space after Filename	Launch Agent	Sudo	HISTCONTROL							
	Third-party Software	Launch Daemon	Valid Accounts	Hidden Files and Directories							
	Trap	Launchctl	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 Management	Modify Existing Service		Indicator Removal from Tools							
	XSL Script Processing	Netsh Helper DLL		Indicator Removal on Host							
		New Service		Indirect Command Execution							
		Office Application Startup		Install Root Certificate							
		Path Interception		InstallUtil							
		Plist Modification		LC_MAIN Hijacking							
		Port Knocking		Launchctl							
		Port Monitors		Masquerading							
		Rc.common		Modify Registry							
		Re-opened Applications		Mshta							
		Redundant Access		NTFS File Attributes							
		Registry Run Keys / Startup Folder		Network Share Connection Removal							
		SIP and Trust Provider Hijacking		Obfuscated Files or Information							
		Scheduled Task		Plist Modification							
		Screensaver		Port Knocking							
		Security Support Provider		Process Doppelgänging							
		Service Registry Permissions Weakness		Process Hollowing							
		Setuid and Setgid		Process Injection							
		Shortcut Modification		Redundant Access							
		Startup Items		Regsvcs/Regasm							
		System Firmware		Regsvr32							
		Systemd Service		Rootkit							
		Time Providers		Rundll32							
		Trap		SIP and Trust Provider Hijacking							
		Valid Accounts		Scripting							
		Web Shell		Signed Binary Proxy Execution							
		Windows Management Instrumentation Event Subscription		Signed Script Proxy Execution							
		Winlogon Helper DLL		Software Packing							
				Space after Filename							
				Template Injection							
				Timestomp							
				Trusted Developer Utilities							
				Valid Accounts							
				Virtualization/Sandbox							

MITRE Enterprise ATT&CK Framework

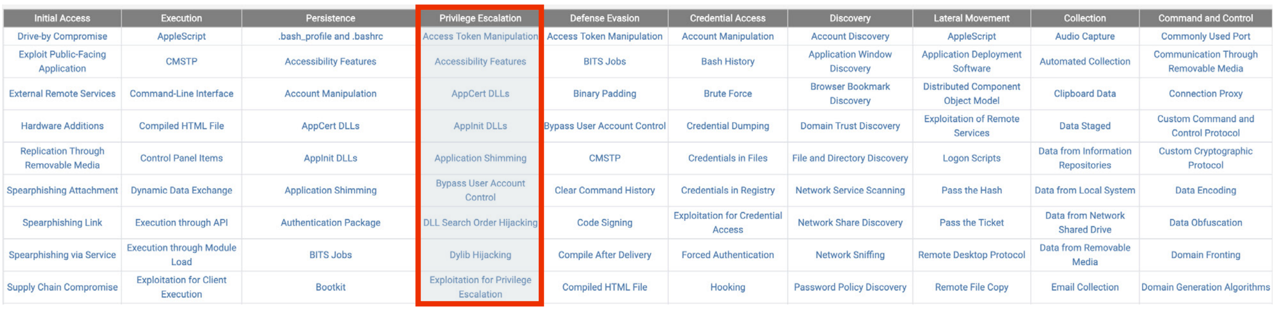
The matrix lists the following tactics:



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control
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
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 Algorithms

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	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
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 Algorithms

MITRE ATT&CK Techniques

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

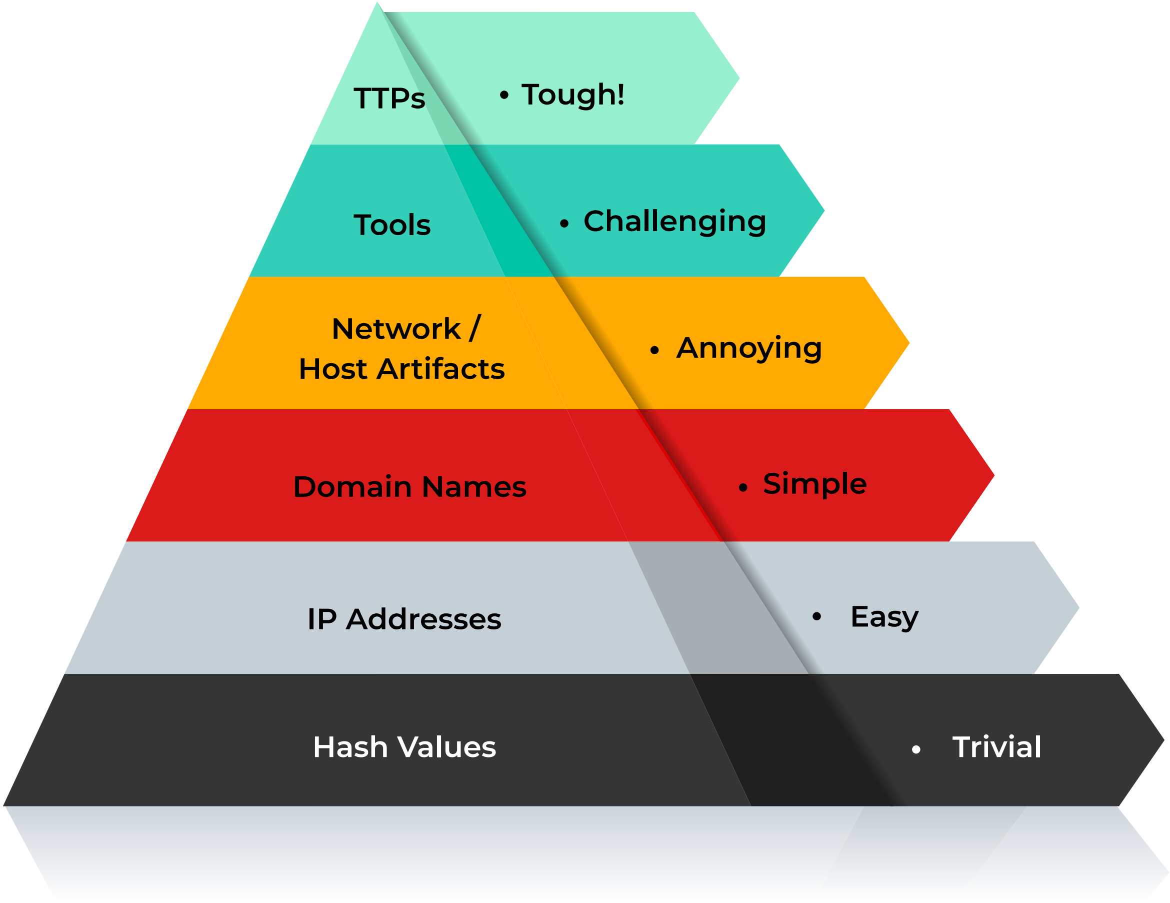
The MITRE ATT&CK framework is used to identify and map out which threats an organization is currently protected against, and then uncovers where it's vulnerable to attack. CyberProof builds upon the matrix, using various threat intelligence means, to identify new threats and provide a unique means of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

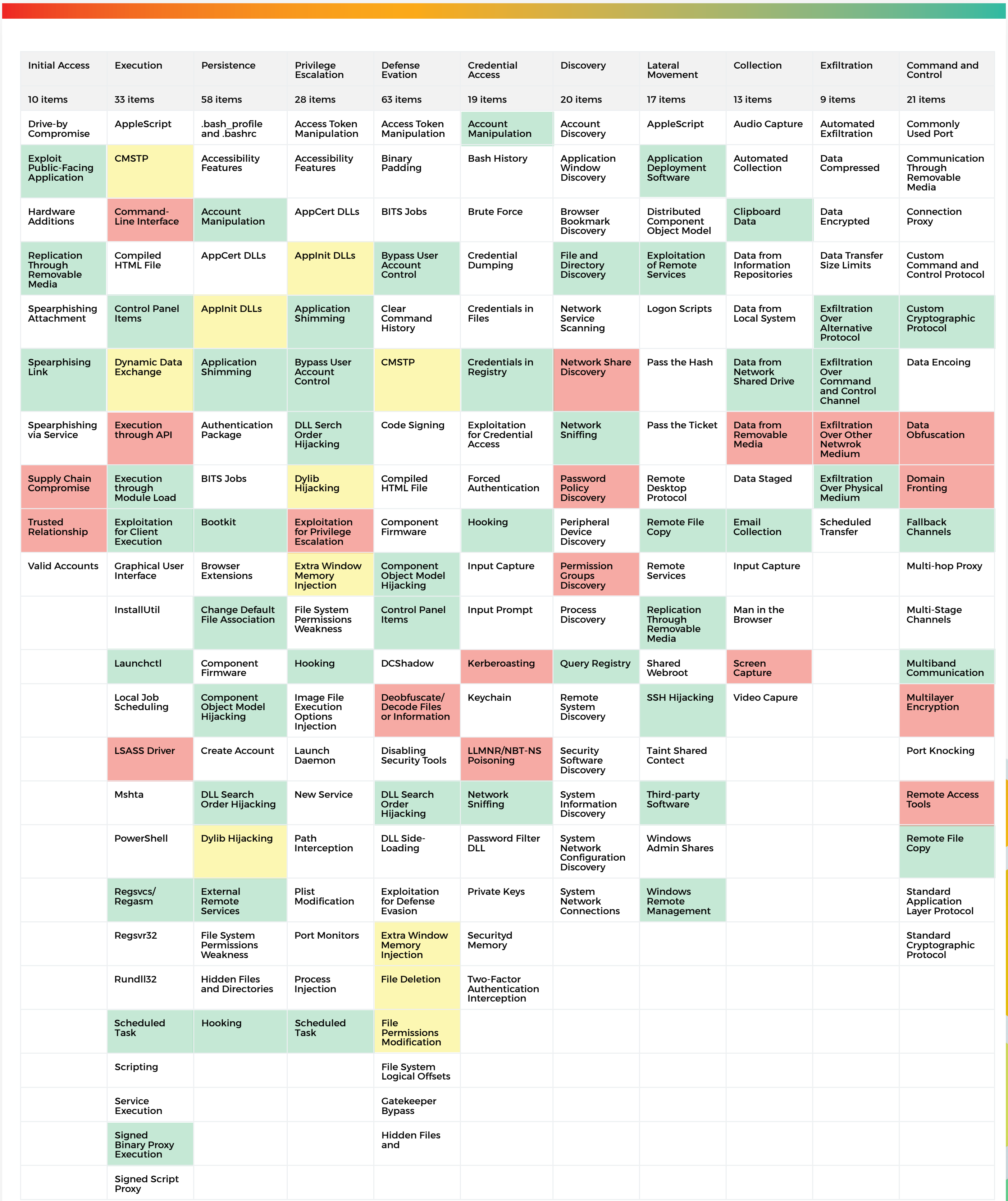
1 MAPPING ATTACK METHODOLOGIES

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.



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evation	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
10 items	33 items	58 items	28 items	63 items	19 items	20 items	17 items	13 items	9 items	21 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	🟩 Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
🟩 Exploit Public-Facing Application	🟨 CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	🟩 Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	🟥 Command-Line Interface	🟩 Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	🟩 Clipboard Data	Data Encrypted	Connection Proxy
🟩 Replication Through Removable Media	Compiled HTML File	AppCert DLLs	🟨 AppInit DLLs	🟩 Bypass User Account Control	Credential Dumping	🟩 File and Directory Discovery	🟩 Exploitation of Remote Services	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Control Panel Items	🟨 AppInit DLLs	🟩 Application Shimming	Clear Command History	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Local System	🟩 Exfiltration Over Alternative Protocol	🟩 Custom Cryptographic Protocol
🟩 Spearphising Link	🟨 Dynamic Data Exchange	🟩 Application Shimming	🟩 Bypass User Account Control	🟨 CMSTP	🟩 Credentials in Registry	🟥 Network Share Discovery	Pass the Hash	🟩 Data from Network Shared Drive	🟩 Exfiltration Over Command and Control Channel	Data Encoing
Spearphishing via Service	🟥 Execution through API	Authentication Package	🟩 DLL Serch Order Hijacking	Code Signing	Exploitation for Credential Access	🟩 Network Sniffing	Pass the Ticket	🟥 Data from Removable Media	🟥 Exfiltration Over Other Netwrok Medium	🟥 Data Obfuscation
🟥 Supply Chain Compromise	🟩 Execution through Module Load	BITS Jobs	🟨 Dylib Hijacking	Compiled HTML File	Forced Authentication	🟥 Password Policy Discovery	Remote Desktop Protocol	Data Staged	🟩 Exfiltration Over Physical Medium	🟥 Domain Fronting
🟥 Trusted Relationship	🟩 Exploitation for Client Execution	🟩 Bootkit	🟥 Exploitation for Privilege Escalation	Component Firmware	🟩 Hooking	Peripheral Device Discovery	🟩 Remote File Copy	🟩 Email Collection	Scheduled Transfer	🟩 Fallback Channels
Valid Accounts	Graphical User Interface	🟩 Browser Extensions	🟨 Extra Window Memory Injection	🟩 Component Object Model Hijacking	Input Capture	🟥 Permission Groups Discovery	Remote Services	Input Capture		Multi-hop Proxy
	InstallUtil	🟩 Change Default File Association	File System Permissions Weakness	🟩 Control Panel Items	Input Prompt	Process Discovery	🟩 Replication Through Removable Media	Man in the Browser		Multi-Stage Channels
	🟩 Launchctl	Component Firmware	🟩 Hooking	DCShadow	🟥 Kerberoasting	🟩 Query Registry	Shared Webroot	🟥 Screen Capture		🟩 Multiband Communication
	Local Job Scheduling	🟩 Component Object Model Hijacking	Image File Execution Options Injection	🟥 Deobfuscate/ Decode Files or Information	Keychain	Remote System Discovery	🟩 SSH Hijacking	Video Capure		🟥 Multilayer Encryption
	🟥 LSASS Driver	Create Account	Launch Daemon	Disabling Security Tools	🟥 LLMNR/NBT-NS Poisoning	Security Software Discovery	Taint Shared Contect			Port Knocking
	Mshta	🟩 DLL Search Order Hijacking	New Service	🟩 DLL Search Order Hijacking	🟩 Network Sniffing	System Information Discovery	🟩 Third-party Software			🟥 Remote Access Tools
	PowerShell	🟨 Dylib Hijacking	Path Interception	DLL Side-Loading	Password Filter DLL	System Network Configuration Discovery	Windows Admin Shares			🟩 Remote File Copy
	🟩 Regsvcs/ Regasm	🟩 External Remote Services	Plist Modification	Exploitation for Defense Evasion	Private Keys	System Network Connections	🟩 Windows Remote Management			Standard Application Layer Protocol
	Regsvr32	File System Permissions Weakness	Port Monitors	🟨 Extra Window Memory Injection	Securityd Memory					Standard Cryptographic Protocol
	Rundll32	Hidden Files and Directories	Process Injection	🟨 File Deletion	Two-Factor Authentication Interception					
	🟩 Scheduled Task	🟩 Hooking	🟩 Scheduled Task	🟨 File Permissions Modification						
	Scripting			File System Logical Offsets						
	Service Execution			Gatekeeper Bypass						
	🟩 Signed Binary Proxy Execution			Hidden Files and						
	Signed Script Proxy									

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).

3 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.

4 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 www.cyberproof.com or reach out to us at: info@cyberproof.com

LOCATIONS

Aliso Viejo | London | Tel Aviv | Trivandrum | Singapore