BZAR – Hunting Adversary Behaviors with Zeek and ATT&CK

Mark Fernandez
John Wunder


@MITREattack

MITRE

What we'll talk about

- **Background: ATT&CK and Threat Hunting**
- **Threat Hunting with BZAR**
  - Zeek Network Security Monitor
  - How BZAR works and what it can see
- **Examples**
  - Service Execution
  - Remote File Copy to Windows Admin Shares
- **Takeaways**

What is ATT&CK™?

A knowledge base of adversary behavior

- Based on real-world observations
- Free, open, and globally accessible
- A common language
- Community-driven

MITRE

Tactics: the adversary's technical goals

Techniques: how the goals are achieved

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

Procedures: Specific technique implementation

Spearphishing Attachment

Examples

Name	Description
APT19	APT19 sent spearphishing emails with malicious attachments in RTF and XLSM formats to deliver initial exploits.[1]
APT28	APT28 sent spearphishing emails containing malicious Microsoft Office attachments.[2][3][4][5][6]

ATT&CK™

MITRE

How can we see these behaviors?

Image Source: Wikimedia Commons

Image Source: Pirates of the Caribbean

How can we identify the malicious ones?

ATT&CK™

MITRE

How can we see these behaviors?

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

Perimeter monitoring is not enough

so we do endpoint monitoring.

ATT&CK™

MITRE

Defense in depth, amirite?

Image Source: The Office

What can we do with internal network monitoring?

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

The Problem: ***Internal Network Traffic Can be Very Noisy***

Server Message Block (SMB) protocol

Remote Procedure Call (RPC) protocol

ATT&CK™

MITRE

The Technology: *Bro / Zeek Network Security Monitor*

Open-source, highly-customizable

Deep-packet inspection

MITRE

The Result: *B Z A R*

Bro / Zeek ATT&CK-based Analytics and Reporting

Bizarre – very strange or unusual

BZAR – open-source Bro/Zeek scripts

https://github.com/mitre-attack/bzar

MITRE

A little more about Zeek…

- **SMB Protocol Analyzer**
  - Message Types 145
- **DCE-RPC Protocol Analyzer**
  - Interface Definitions 81
  - Method Definitions 1,471
- **Authentication Protocol Analyzers**
  - Used in SMB and RPC Authentication
- **File Extraction Analyzer**
  - Extract Files from Network Traffic
  - Lateral Movement

How Many Exist in Windows?

How Many Exist in Windows?

Bonus!

Bonus!

ATT&CK™

MITRE

ATT&CK Techniques Detected with BZAR

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

Legend
White = No Confidence of Detection
Orange = Some Confidence of Detection

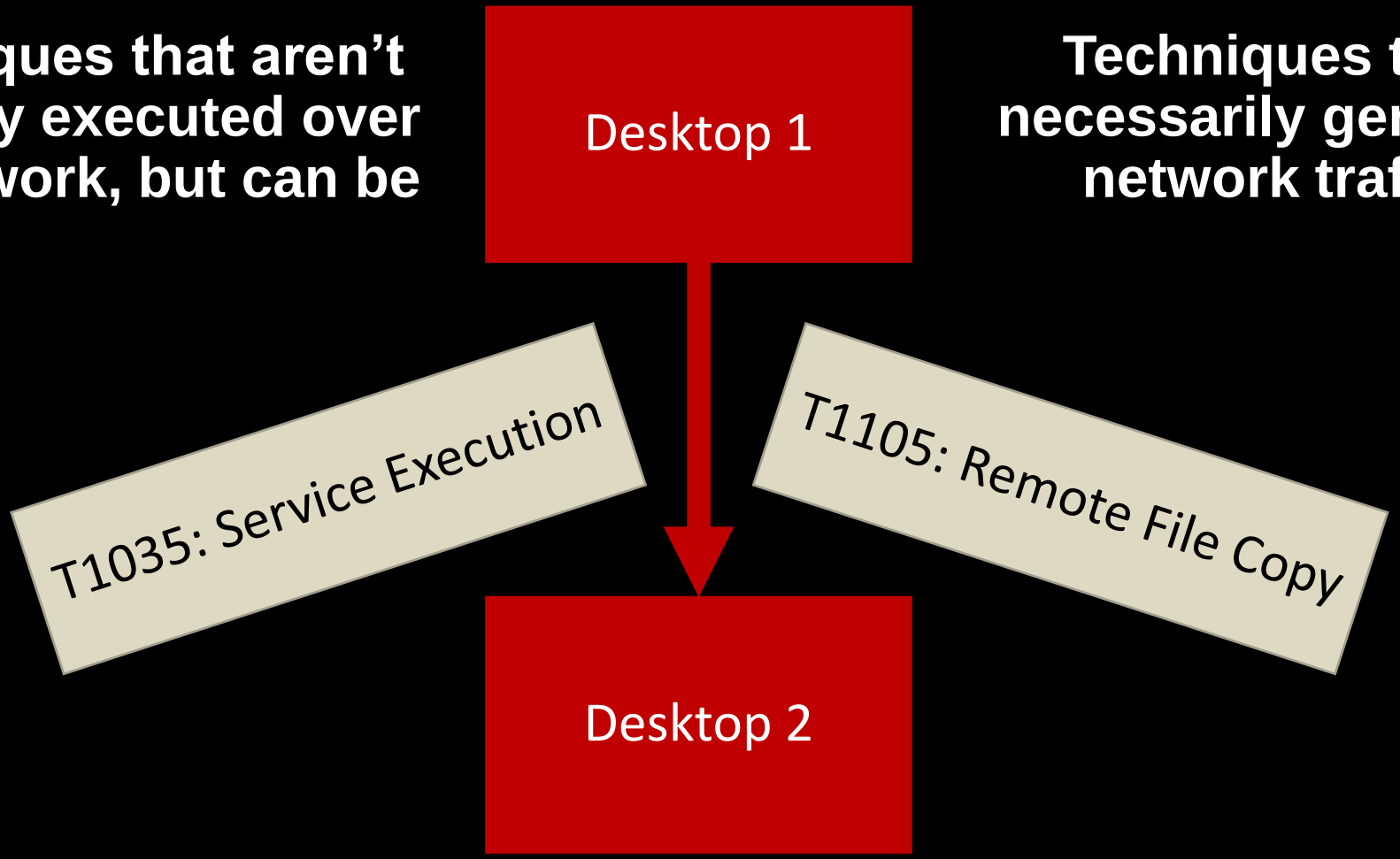
ATT&CK Techniques Detected with BZAR

Execution	Persistence	Defense Evasion	Credential Access	Discovery	Lateral Movement
T1035 Service Execution	T1004 Winlogon Helper DLL	T1070 Indicator Removal Host	T1003 Credential Dumping	T1016 System Network Configuration	T1077 Windows Admin Shares
T1047 Windows Mgmt Instrum. (WMI)	T1013 Port Monitors			T1049 System Networks Connections	T1105 Remote File Copy
T1053 Scheduled Task				T1018 Remote System	
				T1033 System Owner/User	
				T1069 Permission Groups	
				T1082 System Info	
				T1083 File and Directory	
				T1087 Account	
				T1124 System Time	
				T1135 Network Share	

MITRE

What you can see in network traffic…

Techniques that aren't normally executed over the network, but can be



Techniques that necessarily generate network traffic

ATT&CK™

MITRE

BZAR Example – Remote Execution

Execution	Persistence	Defense Evasion	Credential Access	Discovery	Lateral Movement
T1035 Service Execution	T1004 Winlogon Helper DLL	T1070 Indicator Removal Host	T1003 Credential Dumping	T1016 System Network Configuration	T1077 Windows Admin Shares
T1047 Windows Mgmt Instrum. (WMI)	T1013 Port Monitors			T1049 System Networks Connections	T1105 Remote File Copy
T1053 Scheduled Task				T1018 Remote System	
				T1033 System Owner/User	
				T1069 Permission Groups	
				T1082 System Info	
				T1083 File and Directory	
				T1087 Account	
				T1124 System Time	
				T1135 Network Share	

BZAR Example – T1035 Service Execution

Execution
T1035 Service Execution

- **Indicators**: ***Four (4) RPC Functions***
  - svcctl :: CreateServiceA
  - svcctl :: CreateServiceW
  - svcctl :: StartServiceA
  - svcctl :: StartServiceW

- **Analytics**: ***Simple***
  - Detect ***any*** of the 4 RPC functions

  - Zeek event handlers
    - dce_rpc_request()
    - dce_rpc_response()

BZAR Example – T1035 Service Execution

Execution
T1035 Service Execution

- **Reporting**: ***Write to Zeek Notice Log***
  - “ATTACK::Execution”
  - “svcctl::StartServiceW”
  - IP addresses & TCP/UDP ports
  - Zeek connection ID

Important: MUST be tuned for your environment!

BZAR Example – Lateral Movement

Execution	Persistence	Defense Evasion	Credential Access	Discovery	Lateral Movement
T1035 Service Execution	T1004 Winlogon Helper DLL	T1070 Indicator Removal Host	T1003 Credential Dumping	T1016 System Network Configuration	T1077 Windows Admin Shares
T1047 Windows Mgmt Instrum. (WMI)	T1013 Port Monitors			T1049 System Networks Connections	T1105 Remote File Copy
T1053 Scheduled Task				T1018 Remote System	
				T1033 System Owner/User	
				T1069 Permission Groups	
				T1082 System Info	
				T1083 File and Directory	
				T1087 Account	
				T1124 System Time	
				T1135 Network Share	

BZAR Example – Lateral Movement

- **Indicators**: ***Two (2) SMB Commands***
  - SMBv1 Write
  - SMBv2 Write

- **Analytics**: ***Complex***
  - Detect SMB Write to Windows Admin Shares
  - ADMIN$ or C$ *only*
  - Ignore IPC$ (e.g., names pipes)

  - Zeek event handlers
    - smb1_write_andx_response()
    - smb2_write_request()

Lateral Movement
T1077 Windows Admin Shares
T1105 Remote File Copy

BZAR Example – Lateral Movement

- **Reporting**: ***Write to Zeek Notice Log***
  - "ATTACK::Lateral_Movement"
  - "SMB::FILE_WRITE to admin file share"
  - IP addresses & TCP/UDP ports
  - Zeek connection ID
  - Full Universal Naming Convention (UNC) path and file name

Lateral Movement
T1077 Windows Admin Shares
T1105 Remote File Copy

Important: MUST be tuned for your environment!

Summary

- **Monitor your endpoints**
  - But don’t forget about your network
- **Think outside the box**
  - It’s not all about lateral movement
- **Think at different levels of abstraction**
  - Low-fidelity indicators can help you build-up analytics and reporting
- **Integrate into your overall monitoring approach**
  - Network alerts and endpoint alerts can co-exist
- **Tune for your environment!**

ATT&CK™

MITRE

ATT&CK™

attack.mitre.org

medium.com/mitre-attack

attack@mitre.org


@MITREattack

https://github.com/mitre-attack/bzar