ATT&CK IN THREAT MODELING AND USE CASE GENERATION

Ion Santotomas

I HAD NO IDEA AND TOO MANY QUESTIONS

so I went to the **internet**

VAST

STRIDE

LINDDUN

PASTA

DREAD

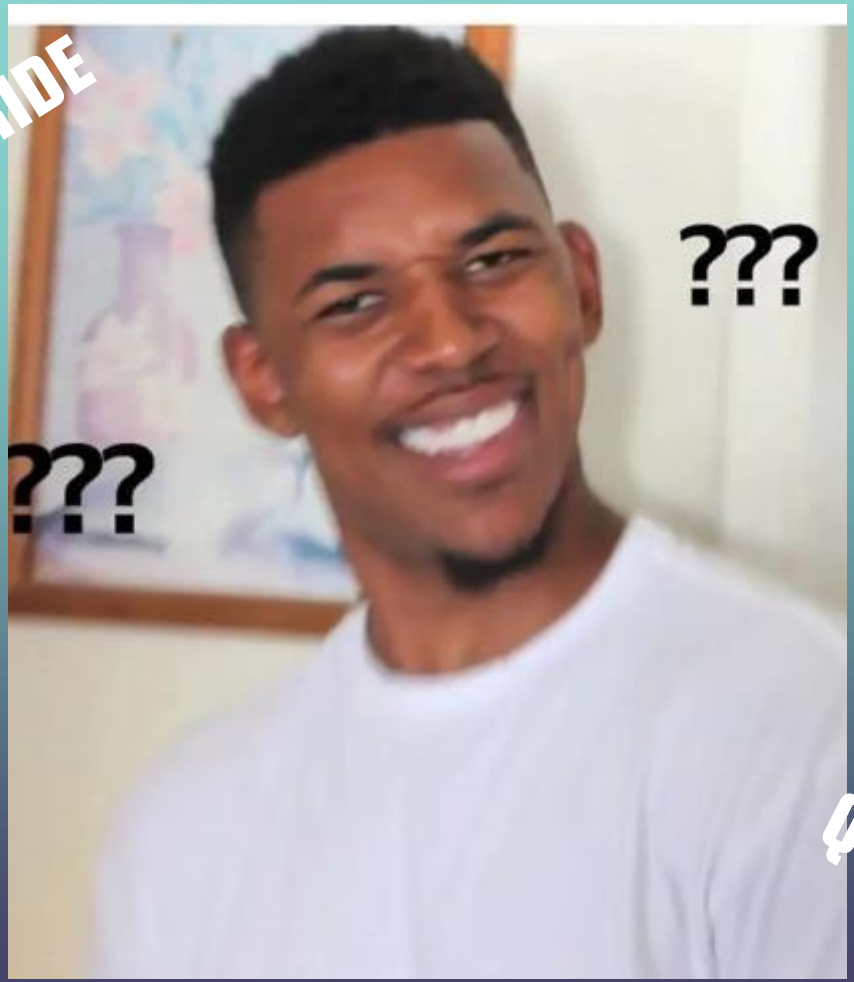
CVSS

hTMM

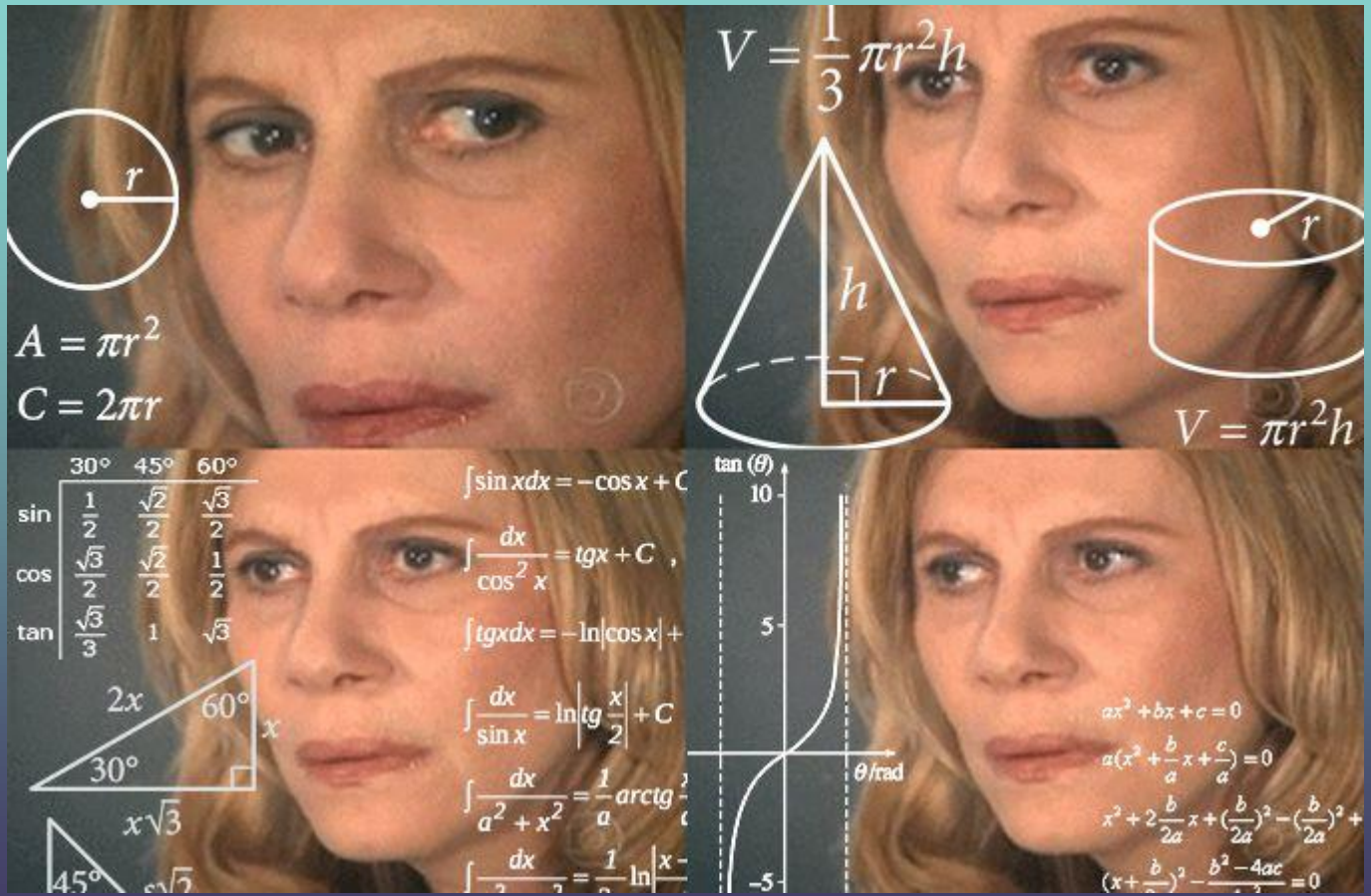
OCTAVE

TRIKE

qTMM



This is too hard… Isn't there a better way?



USING ATT&CK FOR THREAT MODELING

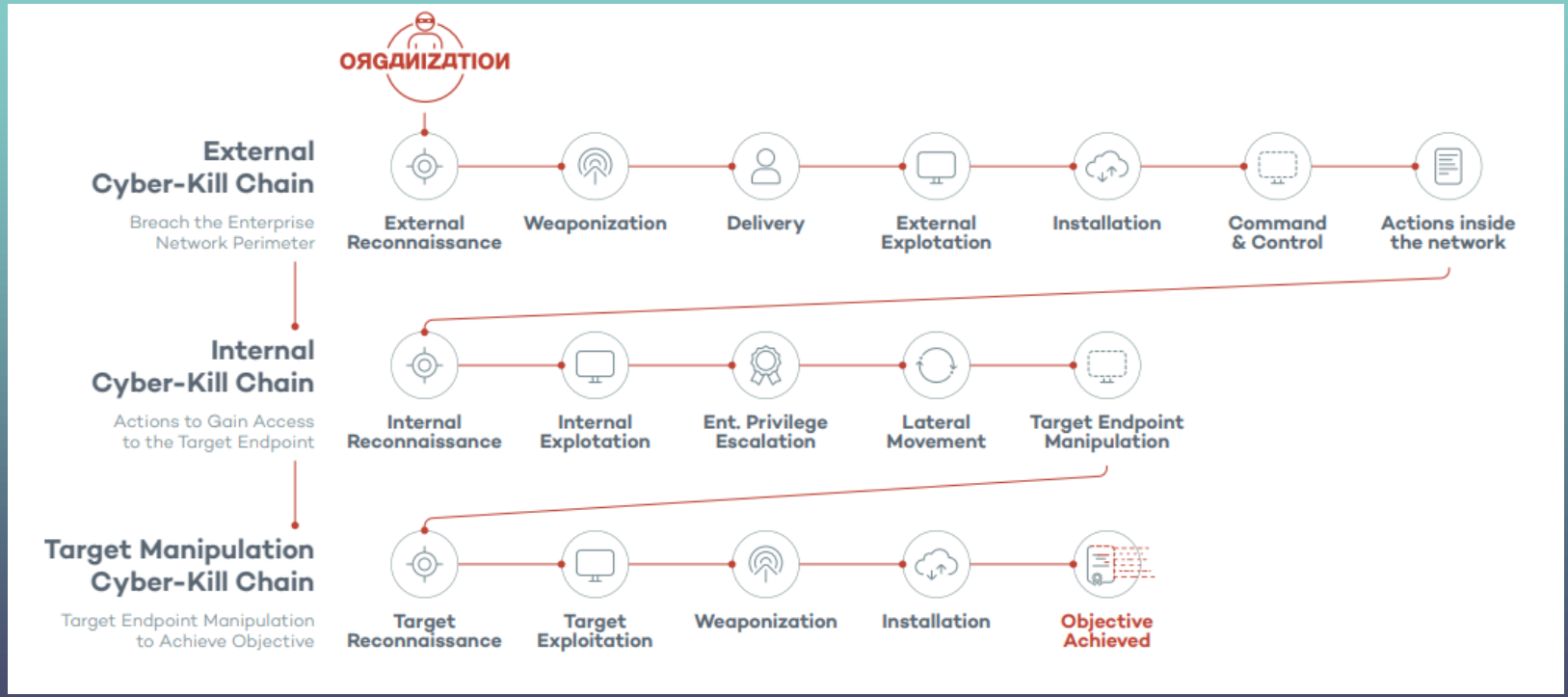
What methods and tools are at my disposal?

ATT&CK Technique name & ID
ATT&CK Tactic

Lockheed's Kill Chain

USING ATT&CK FOR THREAT MODELING

Extended Kill Chain



Source: https://www.pandasecurity.com/rfiles/enterprise/solutions/ad360/1704-WHITEPAPER-CKC-EN.pdf
Also, Black Hat talk: https://www.blackhat.com/docs/us-16/materials/us-16-Malone-Using-An-Expanded-Cyber-Kill-Chain-Model-To-Increase-Attack-Resiliency.pdf

USING ATT&CK FOR THREAT MODELING

What **else** can I use to add depth and defense for these techniques?

Extended Kill Chain

ATT&CK Technique name & ID
ATT&CK Tactic
Lockheed's Courses of Action Matrix

Table 1: Courses of Action Matrix

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

Source: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

USING ATT&CK FOR THREAT MODELING

Technique: Modify Existing Service
Technique ID: T1031
Tactic: Persistence
Extended Kill Chain Phase: Internal Exploitation

Detect	Deny	Disrupt	Degrade	Deceive
Windows Registry, File monitoring, Process monitoring, Process command-line parameters	User Account Management: Limit privileges of user accounts and groups	Use system firewall to drop unauthorized connections and restore service	Apply ad-hoc QoS rule	Honeypot VM

Detection use cases
IR Playbooks

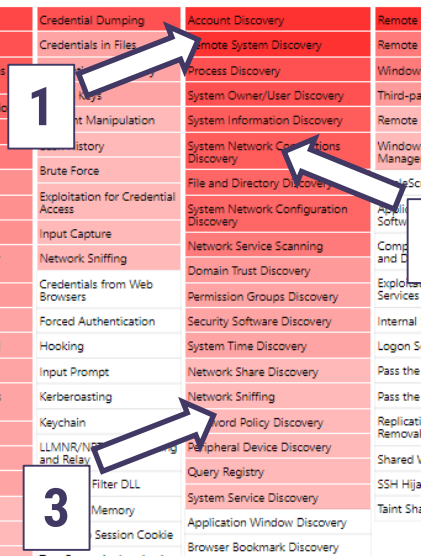
Architecture
Engineering
Network
PM

PUTTING THINGS IN ORDER

What are the most **important** techniques to consider?

- Select the **top 5** threat actor groups for your industry
- Create a Navigator heatmap layer and **order** by frequently used
- **Prioritize** those techniques

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items	22 items	9 items	16 items
Valid Accounts	Command-Line Interface	Valid Accounts	Valid Accounts	Valid Accounts	Credential Dumping	Account Discovery	Remote File Copy	Data from Local System	Remote File Copy	Data Compressed	Data Encrypted for Impact
Spearphishing Attachment	PowerShell	Registry Run Keys / Startup Folder	Web Shell	Scripting	Credentials in Files	Remote System Discovery	Remote Desktop Protocol	Automated Collection	Commonly Used Port	Exfiltration Over Alternative Protocol	Inhibit System Recovery
Exploit Public-Facing Application	Scripting	Create Account	Scheduled Task	File and Directory Permissions Modification	Credentials in Registry	Process Discovery	Windows Admin Shares	Data Staged	Standard Application Layer Protocol	Exfiltration Over Command and Control Channel	Resource Hijacking
External Remote Services	Regsvr32	Web Shell	Accessibility Features	Obfuscated Files or Information	Exploitation for Credential Access	System Owner/User Discovery	Third-party Software	Clipboard Data	Uncommonly Used Port	Automated Exfiltration	Runtime Data Manipulation
Spearphishing Link	Graphical User Interface	Scheduled Task	Bypass User Account Control	Regsvr32	Forced Authentication	System Information Discovery	Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Encrypted	Service Stop
Drive-by Compromise	Rundll32	Accessibility Features	Image File Execution Options Injection	Rundll32	Hooking	System Network Connections Discovery	Windows Remote Management	Data from Network Shared Drive	Remote Access Tools	Data Transfer Size Limits	Account Access Removal
Hardware Additions	Windows Management Instrumentation	BITS Jobs	New Service	Disabling Security Tools	Input Prompt	File and Directory Discovery	AppleScript	Input Capture	Connection Proxy	Exfiltration Over Other Network Medium	Data Destruction
Replication Through Removable Media	Scheduled Task	External Remote Services	Process Injection	Masquerading	Kerberoasting	System Network Configuration Discovery	Application Deployment Software	Audio Capture	Custom Cryptographic Protocol	Exfiltration Over Physical Medium	Defacement
Spearphishing via Service	Third-party Software	Hidden Files and Directories	Access Token Manipulation	Modify Registry	Keychain	Network Service Scanning	Component Object Model and Distributed COM	Data from Removable Media	Data Encoding	Scheduled Transfer	Disk Content Wipe
Supply Chain Compromise	Exploitation for Client Execution	Image File Execution Options Injection	AppInit DLLs	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Domain Trust Discovery	Exploitation of Remote Services	Email Collection	Data Obfuscation		Disk Structure Wipe
Trusted Relationship	CMSTP	New Service	DLL Search Order Hijacking	File Deletion	Network Sniffing	Permission Groups Discovery	Internal Spearphishing	Man in the Browser	Multiband Communication		Endpoint Denial of Service
	Control Panel Items	Redundant Access	Exploitation for Privilege Escalation	BITS Jobs	Password Filter DLL	Security Software Discovery	Logon Scripts	Screen Capture	Standard Cryptographic Protocol		Firmware Corruption
	InstallUtil	Account Manipulation	Service Registry Permissions Weakness	Bypass User Account Control	Private Keys	System Time Discovery	Pass the Hash	Video Capture	Standard Non-Application Layer Protocol		Network Denial of Service
	Local Job Scheduling	AppInit DLLs	Setuid and Setgid	Hidden Files and Directories	Securityd Memory	Network Share Discovery	Pass the Ticket		Web Service		Stored Data Manipulation
	Mshta	Browser Extensions	Sudo	Image File Execution Options Injection	Steal Web Session Cookie	Network Sniffing	Replication Through Removable Media		Communication Through Removable Media		System Shutdown/Reboot
	Service Execution	DLL Search Order Hijacking	AppCert DLLs	Indicator Removal on Host	Two-Factor Authentication Interception	Password Policy Discovery	Shared Webroot		Domain Fronting		Transmitted Data Manipulation
	User Execution	Kernel Modules and Extensions	Application Shimming	Process Injection		Peripheral Device Discovery	SSH Hijacking		Domain Generation Algorithms		
	Windows Remote Management	Launch Agent	Dylib Hijacking	Redundant Access		Query Registry	Taint Shared Content		Fallback Channels		
	XSL Script Processing	Local Job Scheduling	Elevated Execution with Prompt	Access Token Manipulation		System Service Discovery			Multi-hop Proxy		
	AppleScript	Modify Existing Service	Emond	Clear Command History		Application Window Discovery			Multi-Stage Channels		
	Compiled HTML File	Service Registry Permissions Weakness	Extra Window Memory Injection	CMSTP		Browser Bookmark Discovery			Multilayer Encryption		
	Component Object Model and Distributed COM	Setuid and Setgid	File System Permissions Weakness	Code Signing		Software Discovery			Port Knocking		
	Dynamic Data Exchange	.bash_profile and .bashrc	Hooking	Compile After Delivery		Virtualization/Sandbox Evasion					
	Execution through API	AppCert DLLs	Launch Daemon	Connection Proxy							
	Execution through Module Load	Application Shimming	Parent PID Spoofing	Control Panel Items							
	Launchctl	Authentication Package	Path Interception	DLL Search Order Hijacking							
	LSASS Driver	Bootkit	Plist Modification	DLL Side-Loading							
	Regsvcs/Regasm	Change Default File Association	Port Monitors	Hidden Users							
	Signed Binary Proxy Execution	Component Firmware	PowerShell Profile	Indicator Removal from Tools							
	Signed Script Proxy Execution	Component Object Model Hijacking	SID-History Injection	InstallUtil							
	Source	Dylib Hijacking	Startup Items	Mshta							
	Space after Filename	Emond	Sudo Caching	Network Share Connection Removal							
	Trap	File System Permissions Weakness		Process Hollowing							
	Trusted Developer Utilities	Hooking		Rootkit							
		Hypervisor		Software Packing							
		Launch Daemon		Timestomp							
		Launchctl		Web Service							
				XSL Script Processing							
				Binary Padding							



SUPERCHARGING USE CASES

How can I convert the prioritized techniques into structured, **actionable** use cases?

- Create a matrix and **group tactics** as categories
- Map the kill chain to **each** technique
- Create as much use cases as **aspects** you want to cover from a technique
- Assign scores and **follow up** improvement

Tactic	Technique	ID	Ext Kill Chain Phase	Criticality 1-5	Use Case	Event Ref	Calculation	Detection Rule	Reliability 1-5
Defense Evasion	Disabling Security Tools	T1089	Target Manipulation	5	Clearing of event logs	104	If event happens, trigger alert	Sigma detection rule for SIEM of choice	3

I FOUND ATT&CK EXCELLENT

at making myself ask **better** questions

THANK YOU

Ion Santotomas
ionsantotomas@protonmail.com
@ionsantotomas