Planning Successful Red Team Operations

By: Joe Christian

I just walked into the room… Who is this guy?

- Joe Christian
  - Security Risk Assessment team lead at Zappos.com, a subsidiary of Amazon based in Las Vegas, NV.
  - Enjoys all areas of security, but primarily focused on AppSec and Offensive Security.
  - Earliest memories of “security” date back to age 12.
  - Graduated from Nazareth College with a B.S. in Information Technology and Utica College with an M.S. Cybersecurity specializing in Cyber Operations.
  - Published research on bug bounty programs and vulnerability disclosure.
  - Co-Founded DEF CON AppSec Village.
  - Expressed interest in doing a Ph.D. in 2020. More student debt, why not?
  - Working on starting my own company called {REDACTED_NAME_HERE}.
  - Goal: Hit all the national parks in the US before the world chars to oblivion in 2030.

Agenda

- Penetration testing versus red team operations
- Pre-planning work
- Common pitfalls of planning a covert operation
- Avoiding pitfalls
- Staying on plan
- Automation
- Conclusion
- Q&A

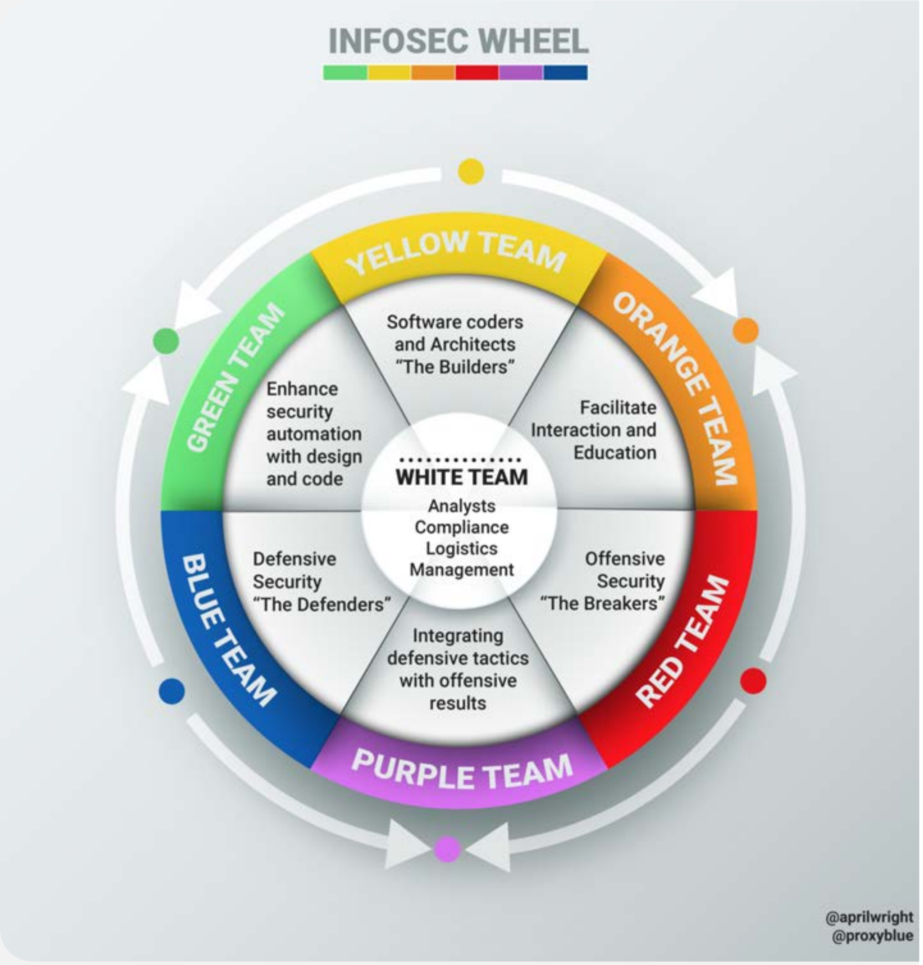
Disclaimer

The views and opinions expressed here represent my own and not those of the people, institutions or organizations that I may or may not be related with unless stated explicitly.

Operation: Ice Breaker

Raise your hand up if…

- You identify as a yellow team: development, architects, etc.
- You identify as a orange team: TPM’s, security awareness, etc.
- You identify as a red team: penetration tester or offensive security role.
- You identify as a blue team: SOC, IR, TI, engineering, etc.
- You identify as a purple team: blue + red.
- You identify as a green team: automation, etc.
- You identify as white team: leadership, compliance, risk, etc.
- You identify as academia: professors, students, researchers, etc.
- **None of the above: stand and state your role.**


INFOSEC WHEEL
YELLOW TEAM
Software coders and Architects "The Builders"
ORANGE TEAM
Facilitate Interaction and Education
RED TEAM
Offensive Security "The Breakers"
PURPLE TEAM
Integrating defensive tactics with offensive results
BLUE TEAM
Defensive Security "The Defenders"
GREEN TEAM
Enhance security automation with design and code
WHITE TEAM
Analysts
Compliance
Logistics
Management
@aprilwright
@proxyblue

InfoSec Color Wheel

So who can tell me what a red team operation is?

Penetration testing versus red team operations

Hint: They are not the same thing!

Penetration Testing

- A test to find as many vulnerabilities and configuration issues as possible in the time allotted, and exploiting those vulnerabilities to determine the risk of the vulnerability.
- Duration: Lasts between days to two weeks.
- Scope: Testing restrictions are placed.
- Tooling: Use of common industry tools.
- Overall: Butcher Knife

Red Teaming

- An adversarial test to determine the organization's detection and response capabilities against sophisticated attacks.
- Duration: Lasts between several weeks to months.
- Scope: Unlimited.
- Tooling: Everything including zero-day capabilities.
- Overall: Scalpel

Important, but miscellaneous information

Scope

- “If a system is used to perform a business function, it is in scope unless prohibited by law.”
- If the business is unwilling to compromise on this, then education is your top priority.

Mentality

- Treat everyone with respect.
- Systems and processes break. It is no one’s fault.

Exfiltration

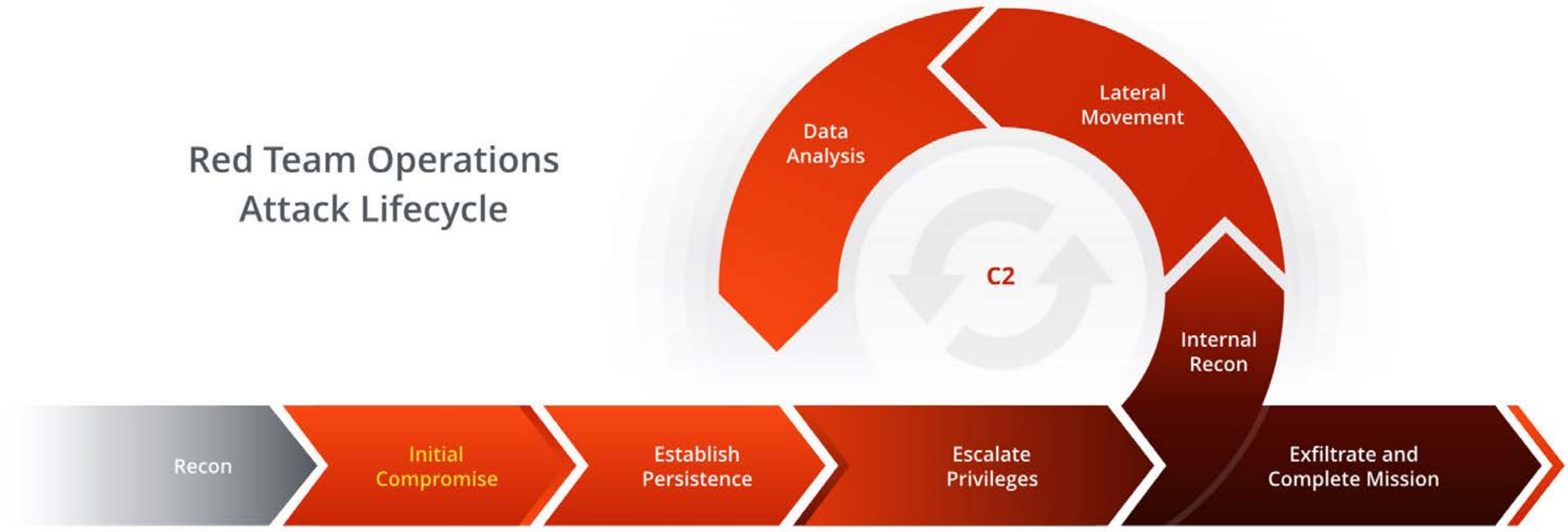
- If you want to exfiltrate real data, then treat it with the utmost professionalism.
- If you cannot treat data with professionalism, then exfiltrate fake information to spec.

Pre-planning work

Checklist prior to conducting a red team operation

- Education of C-level staff on why these tests need to be conducted.
- Authorization from C-level staff/legal to conduct an operation.
- Determine the approximate cost of running an operation and secure funding.
- Creation of key documents such as a code of conduct or an ethics agreement.
- Establish expectations from stakeholders.

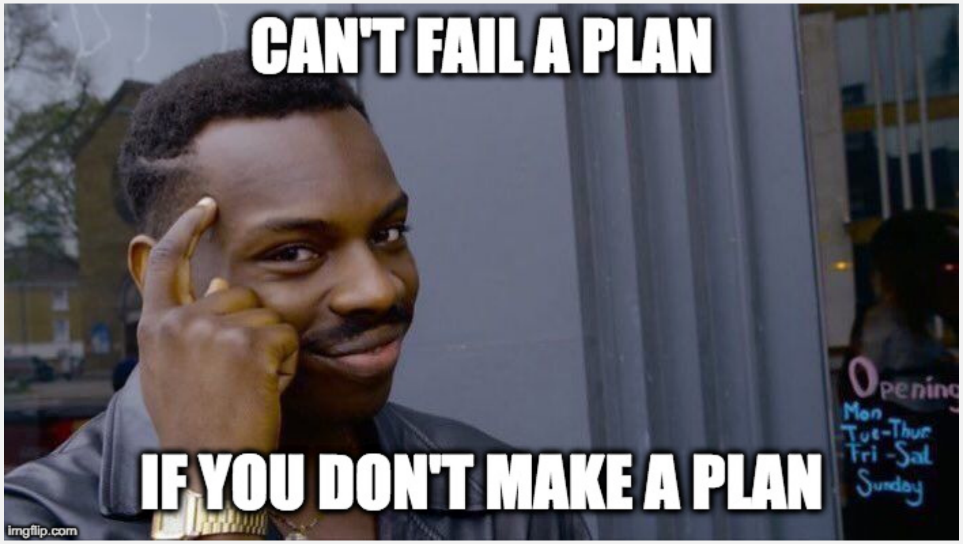
Where is the planning phase?



Sample Red Team Operation Lifecycle

Why is planning important?

- Planning is the SINGLE MOST IMPORTANT ASPECT! PERIOD.
- This is because life never works out as intended.
- The majority of planning should be conducted prior to the reconnaissance phase.
- However, planning occurs before every single phase.
- The best offensive based operations are planned out with excruciating detail, so don't think you can just "show up".



Roll Safe Think About It Meme

Common pitfalls of planning covert operations

#1 - Bad Operational Security

- Operational Security or (OPSEC) is a systematic process by which potential adversaries can be denied information about the capabilities and intentions of organizations by identifying, controlling, and protecting generally unclassified information that specifically relates to the planning and execution of sensitive organizational activities. (NIST SP.800-53r4)
- In most red team engagements, the organizations blue team will act as the adversary that the red team is attempting to deny information to.
- “Lose Lips Sink Ships”.
- DO NOT VOLUNTEER INFORMATION:
  - Don’t detail the operation on your viewable Outlook Calendar.
  - Don’t inform those who don’t have the need to know.
  - Secure physical plans and protect digital plans!

#2- Not Having Clear Objectives

- Objectives = Goals!
- Well defined objectives can be difficult to articulate.
- When we don't have clear objectives, we deviate from our plan. (That's bad!)
- Ask yourself these questions:
  - What are we testing?
  - What are we trying to accomplish?
  - What is valuable to the organization?
  - What adversary are we trying to simulate to the blue team?

Distracted Boyfriend Meme

#3 Picking The Wrong Adversary

- Adversary selection is extremely important.
- Selection should be based on the following criteria:
  - Threat Intelligence from your organization.
    - What does the blue team see?
  - Types of software, OS, or infrastructure you use.
  - Industry your organization operates in.
    - Healthcare, Financial, E-Commerce
  - Potential data you may have.
    - Source code, PII, PHI, etc.
  - Potential access you may provide to others.

APT that doesn't map to your organization
APT that maps to your organization
imgflip.com
JAKE-CLARK.TUMBLR

Two Button Meme

#4 The Unknown

- Not everything can be under your control.
- Something always goes wrong.
  - When has anyone executed a straight forward red team engagement with zero issues?
- Conservatively, we can maybe plan for 80%.
- It's a lot of work getting to that 80%!
  - Don't get lazy. Put in the time needed to succeed.
  - Make a checklist of "unknown problems" that could jeopardize the operation.
  - Have someone review your list checklist to help close the potential gap.

Avoiding pitfalls

#1 - Avoiding Bad Operational Security

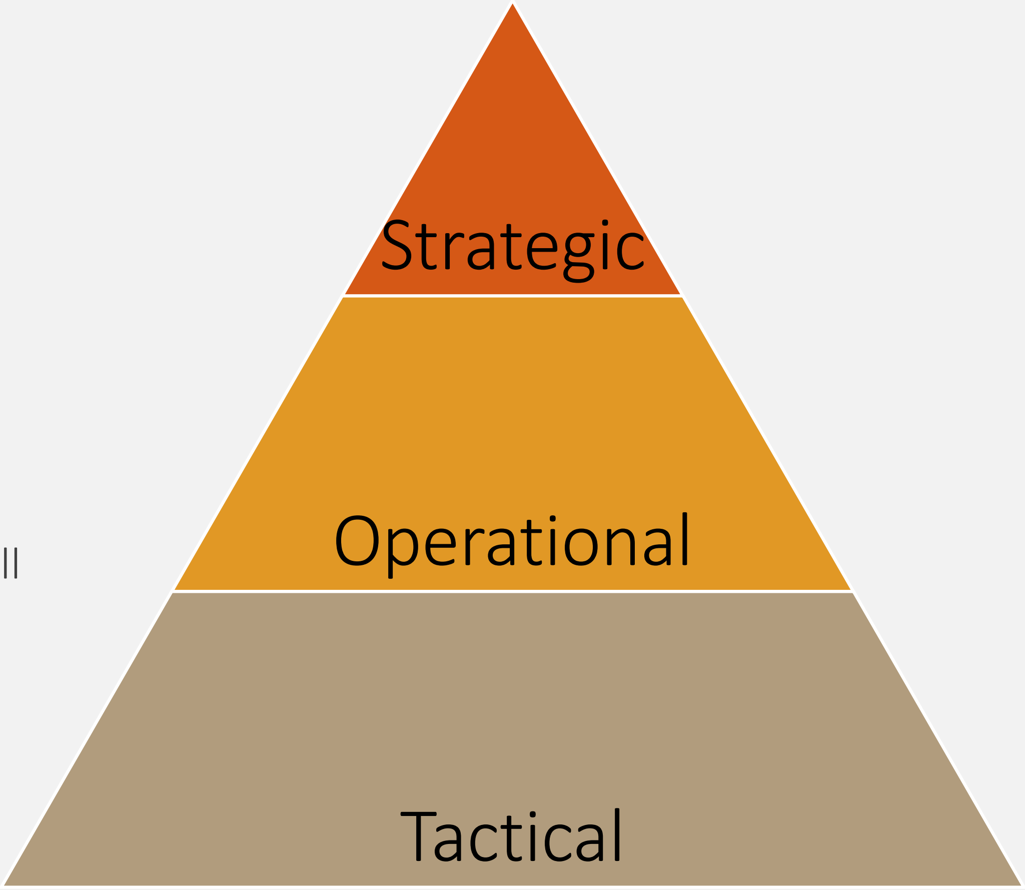
- We need to account for as much information leakage possible.
- Here's a starter list:
  - **Classify budgets/PO's as extremely sensitive information, until after engagement!**
    - If blue team sees a PO for several AWS instances for the red team…I wonder where the attack is coming from.
  - **Licensing, DNS, HTTPS Certificates, Emails, Phone Numbers, and more:**
    - If blue team discovers a "malicious" web server and the DNS contains the red teams information on it… OPSEC is ruined.
  - **Communication Channels:**
    - Traffic needs to be encrypted! Lots of people still run unencrypted internal chat services? Why!?
    - Blue team should not have access to information.
    - Risk analysis on 4th party collection when using 3rd party services.

#1 - Avoiding Bad Operational Security - Continued

- List continued from previous slide:
  - **Physical Security:**
    - Lock up any printed files and only keep them on out when needed.
    - Erase conference rooms where you might have used a whiteboard.
    - If blue/red team work in a confined space, don't just disappear as this will tip off the opposing team.
    - Computer screen protectors when working with digital items.
  - **Digital Security:**
    - Did I mention encryption? I'll say encryption again.
    - Access control to ensure only authorized personnel have access.
      - Be careful of things like JIRA, Confluence, File Shares, etc.
    - Use multifactor authentication where ever possible.

#2- Ensuring Clear Objectives

- US Airforce has some great public war doctrine available to model after.
- It can be used to create defined goals across all levels.
  - Strategic (Enterprise wide)
    - Transparency, education, ethics.
  - Operational (Each unique operation)
    - Actor selection and criteria for what will be deemed a successful operation.
  - Tactical (Each phase within an operation)
    - Tactics, Techniques, and Procedures. (TTPs)



Levels of War US Airforce Doctrine

#3 - Attempting to Avoid the Unknown

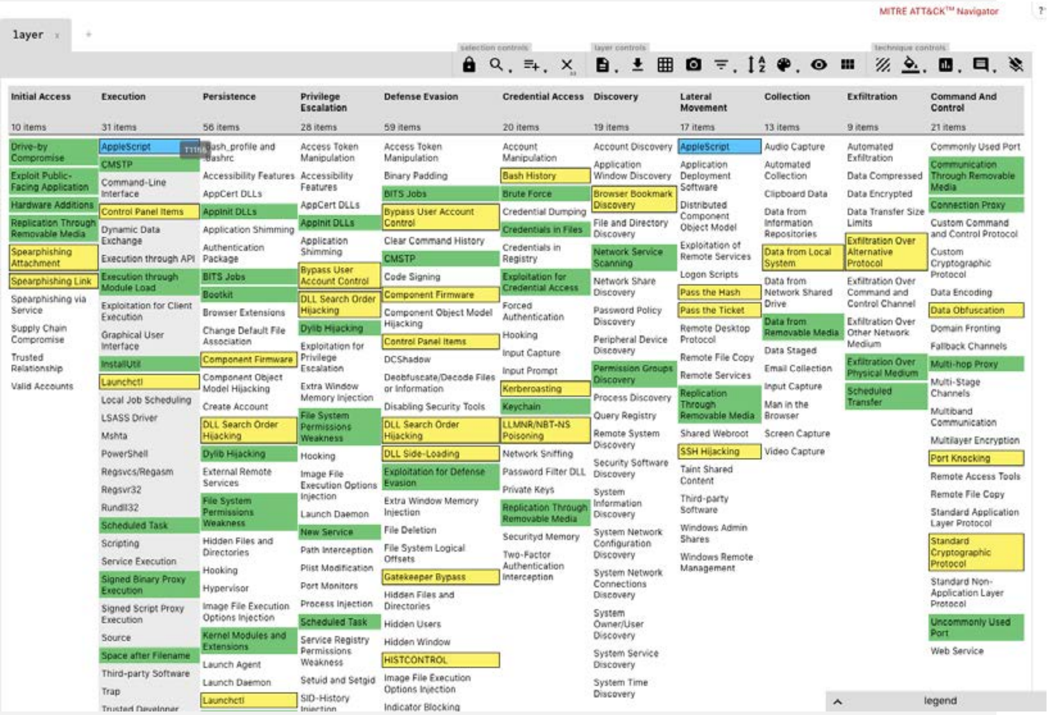
- Make your checklist for “unknown” items as discussed.
- Test tools and exploits on sample systems before hitting production.
  - This way you can anticipate how the system is going to react and have a plan incase it doesn’t go well!
- Anticipate someone or something ruining the plan.
  - Have a secondary and/or tertiary plan ready to go.
- “Deal with it” because it can’t be avoided.

“Doge Deal With It” Meme

Staying on plan

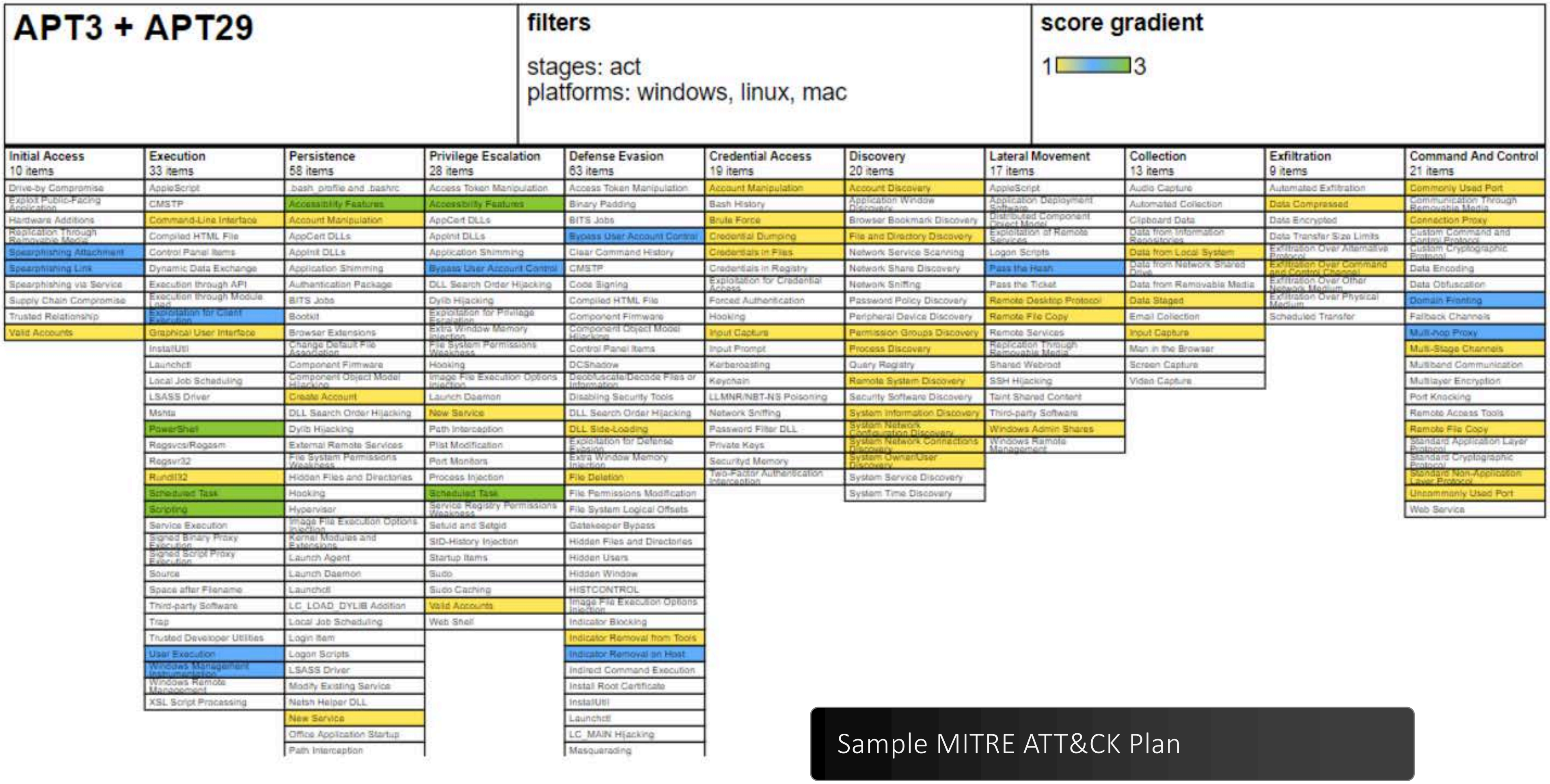
Staying On Plan

- Use MITRE ATT&CK Framework.
  - All adversaries are listed along with their TTP’s mapped!
  - An amazing matrix that can:
    - Be used to map out an organization’s susceptibility and progress over time.
    - Color code TTP’s for the adversary of your choice, which makes easy to use operation plans.
    - A collaborative toolset for both blue and red to work off of.
  - I use this daily! Go bookmark:
    - https://mitre-attack.github.io/attack-navigator/enterprise/



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	31 items	56 items	28 items	59 items	20 items	19 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	AppCert DLLs	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit 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	Dynamic Data Exchange	Application Shimming	Application Shimming	Clear Command History	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	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 Encoding
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Password Policy Discovery	Pass the Ticket	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Dylib Hijacking	Component Firmware	Forced Authentication	Peripheral Device Discovery	Remote Desktop Protocol	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Permission Groups Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Process Discovery	Remote Services	Input Capture		Multi-hop Proxy
	Launchctl	Component Firmware	File System Permissions Weakness	DCShadow	Input Prompt	Query Registry	Replication Through Removable Media	Man in the Browser		Multi-Stage Channels
	Local Job Scheduling	Component Object Model Hijacking	Hooking	Deobfuscate/Decode Files or Information	Kerberoasting	Remote System Discovery	Shared Webroot	Screen Capture		Multiband Communication
	LSASS Driver	Create Account	Image File Execution Options Injection	Disabling Security Tools	Keychain	Security Software Discovery	SSH Hijacking	Video Capture		Multilayer Encryption
	Mshta	DLL Search Order Hijacking	Launch Daemon	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning	System Information Discovery	Taint Shared Content			Port Knocking
	PowerShell	Dylib Hijacking	New Service	DLL Side-Loading	Network Sniffing	System Network Configuration Discovery	Third-party Software			Remote Access Tools
	Regsvcs/Regasm	External Remote Services	Path Interception	Exploitation for Defense Evasion	Password Filter DLL	System Network Connections Discovery	Windows Admin Shares			Remote File Copy
	Regsvr32	File System Permissions Weakness	Plist Modification	Extra Window Memory Injection	Private Keys	System Owner/User Discovery	Windows Remote Management			Standard Application Layer Protocol
	Rundll32	Hidden Files and Directories	Port Monitors	File Deletion	Replication Through Removable Media	System Service Discovery				Standard Cryptographic Protocol
	Scheduled Task	Hooking	Process Injection	File System Logical Offsets	Securityd Memory	System Time Discovery				Standard Non-Application Layer Protocol
	Scripting	Hypervisor	Scheduled Task	Gatekeeper Bypass	Two-Factor Authentication Interception					Uncommonly Used Port
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	Hidden Files and Directories						Web Service
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Setuid and Setgid	Hidden Users						
	Signed Script Proxy Execution	Launch Agent	SID-History Injection	Hidden Window						
	Source	Launch Daemon		HISTCONTROL						
	Space after Filename	Launchctl		Image File Execution Options Injection						
	Third-party Software			Indicator Blocking						
	Trap									
	Trusted Developer									

Sample MITRE ATT&CK Matrix



APT3 + APT29

filters

stages: act
platforms: windows, linux, mac

score gradient

1 ▭ 3

Initial Access 10 items	Execution 33 items	Persistence 58 items	Privilege Escalation 28 items	Defense Evasion 63 items	Credential Access 19 items	Discovery 20 items	Lateral Movement 17 items	Collection 13 items	Exfiltration 9 items	Command And Control 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
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	Exfiltration Over Command and Control Channel	Data Encoding
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	Exfiltration Over Other Network 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 Capture		Multilayer Encryption
	LSASS Driver	Create Account	Launch Daemon	Disabling Security Tools	LLMNR/NBT-NS Poisoning	Security Software Discovery	Taint Shared Content			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 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						

Sample MITRE ATT&CK Plan

Automation

Automation

- Use MITRE's API to directly interact with ATT&CK.
- MITRE also open sources their adversary data as raw JSON.
  - Download the raw data and import into other frameworks as needed.
  - https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterprise-attack.json
- Using Red Canary's Atomic Red Team for testing and mapping to ATT&CK.
  - https://github.com/redcanaryco/atomic-red-team
- Using Scythe to quickly to automate and map back to ATT&CK.
  - https://www.scythe.io/platform
- Using Unfetter to build out an operations planner.
  - https://nsacyber.github.io/unfetter/
- Praetorian's Purple Team ATT&CK for testing.
  - https://github.com/praetorian-code/purple-team-attack-automation

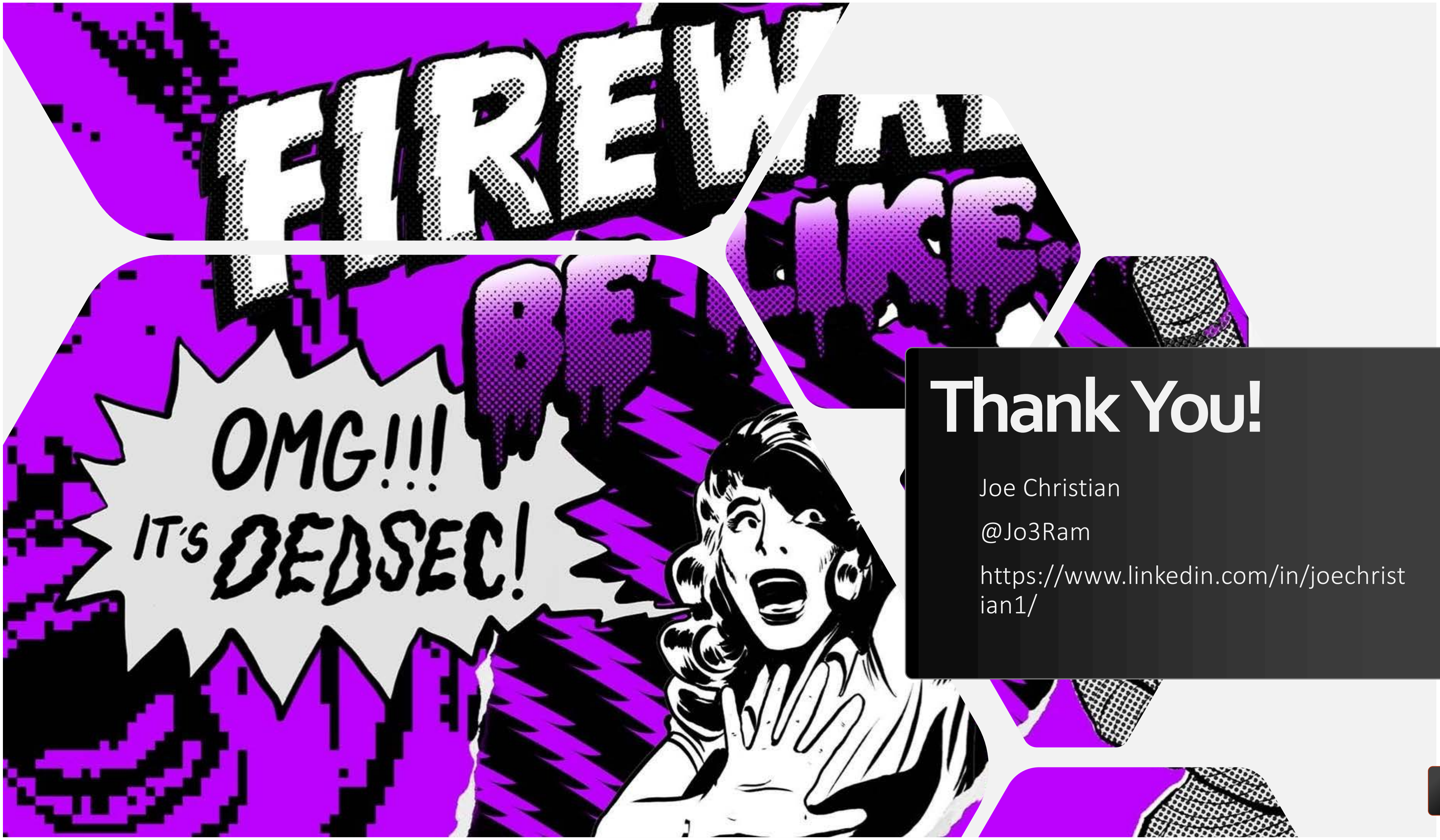
Conclusion

Conclusion

- Educating more people on planning makes the world a better place.
- Plan operations meticulously because it will make your life much easier.
  - Determine potential pitfalls and avoid them where possible.
- Use the defined Strategic, Operational, and Tactical methodology.
- Stay on plan with MITRE's ATT&CK Framework.
- Work "smarter, not harder" and use tooling to automate your workflow.

Frodo Its Over Its Done Meme

Questions?



Thank You!

Joe Christian

@Jo3Ram

https://www.linkedin.com/in/joechristian1/