

DESIGNING, DEVELOPING AND RUNNING PURPLE TEAMING EXERCISES

FATIH OZAVCI

Fatih Ozavci

Adversary Simulations and Research

UNSW (ADFA) - Master of Cyber Security

Security Researcher

- *Vulnerabilities: Microsoft, Cisco, SAP*

Speaker & Trainer

- *Sessions: Black Hat USA, Def Con*

Open Source Software Projects

- *Petaq Purple Team C2 & Malware*
- *Viproj VoIP Penetration Testing Kit*



<https://linkedin.com/in/fozavci>

Agenda

Threat Actors and Landscape

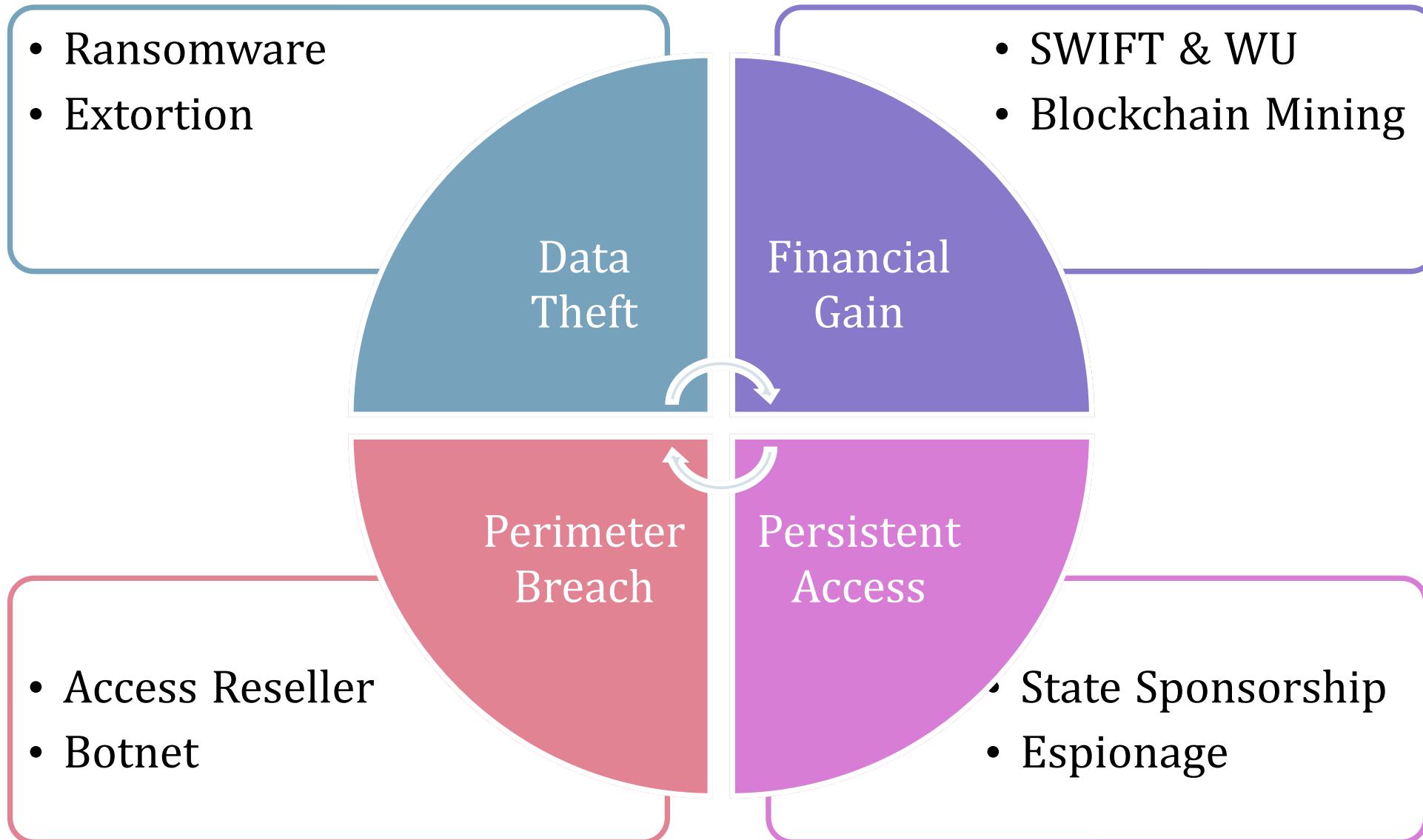
Adversary Simulations

Purple Team Exercises



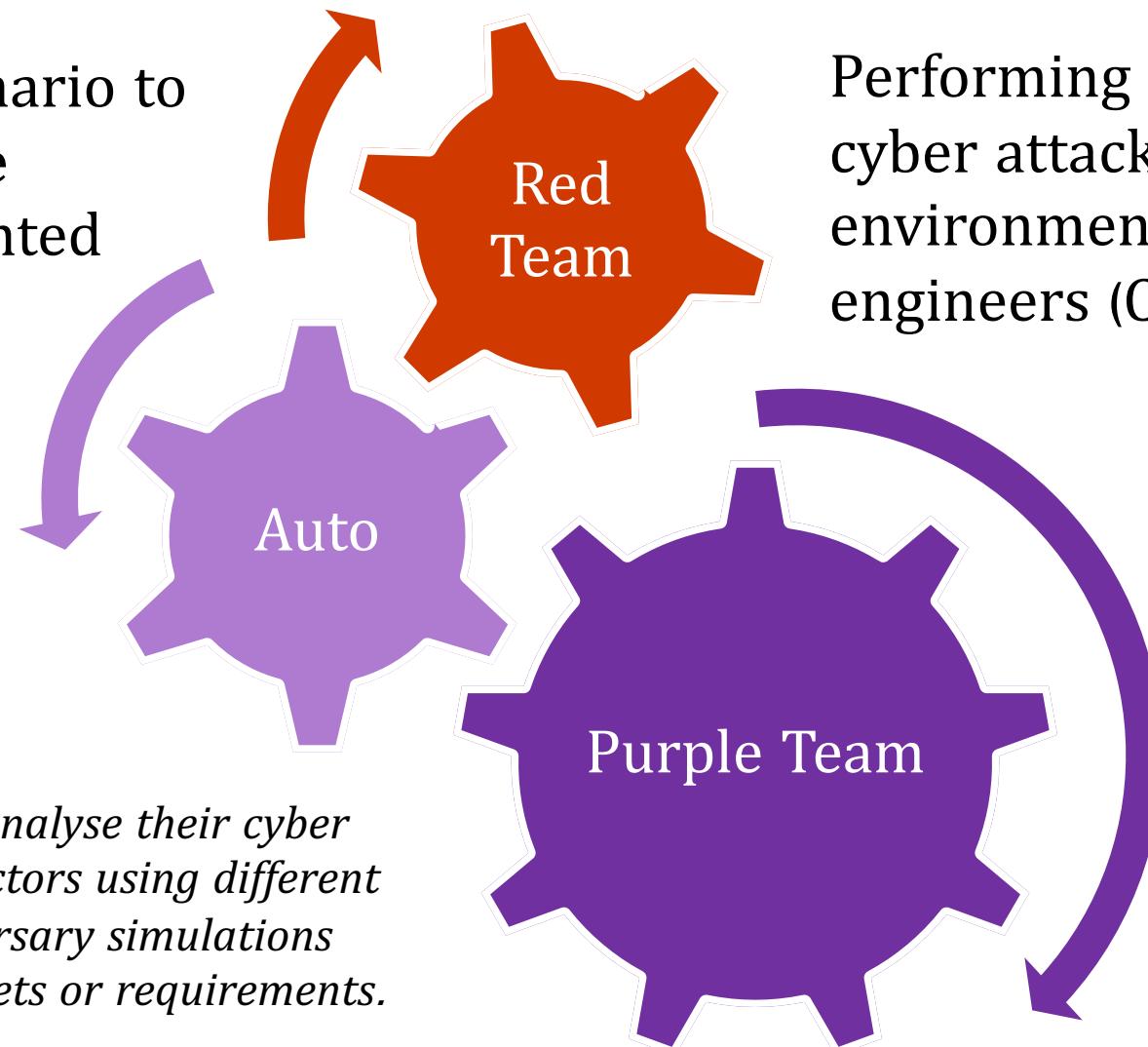
Scenario Run - Demo

Threat Actors and Motives



Adversary Simulation Types

Automating a scenario to assess the defence controls implemented (MITRE ATT&CK)



Performing a Threat Intelligence-Led cyber attack against the targeted environment with a team of engineers (CBEST, CORIE, ICAST)

Organisations desire to analyse their cyber defence against threat actors using different implementations of adversary simulations depending on their budgets or requirements.

Performing a cyber attack with blue team collaboration to improve people and defence together (MITRE ATT&CK)

What Are We Simulating, Again?

Design

Because, the regulation said so? (CBEST, CORIE, ICAST, MITRE)

Security Breach Experienced

External/Internal Red Team Exercise

General Assessment of the Security Controls and Perimeter

Threat Actor actively/potentially targeting the organisation

- *Ransomware & Extortion*
- *Blockchain Mining*
- *Long Term Access*



Coverage: Mitre Att&ck

Design

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
9 techniques	10 techniques	18 techniques	12 techniques	34 techniques	14 techniques	24 techniques	9 techniques	16 techniques	16 techniques	9 techniques	13 techniques
Drive-by Compromise	Command and Scripting Interpreter (7)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Credentials from Password Stores (3)	Application Window Discovery	Internal Spearphishing	Communication Through Removable Media	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction	Data Encrypted for Impact
External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (11)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Automated Collection	Clipboard Data	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Manipulation (3)	Data Manipulation (3)
Hardware Additions	Native API	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Lateral Tool Transfer	Data Obfuscation (3)	Data from Cloud Storage Object	Defacement (2)	Defacement (2)	Defacement (2)
Phishing (3)	Scheduled Task/Job (5)	Boot or Logon Initialization Scripts (5)	Direct Volume Access	Execution Guardrails (1)	Cloud Service Discovery	Remote Service Session Hijacking (2)	Dynamic Resolution (3)	Dynamic Resolution (3)	Exfiltration Over C2 Channel	Disk Wipe (2)	Disk Wipe (2)
Replication Through Removable Media	Shared Modules	Browser Extensions	Create or Modify System Process (4)	Input Capture (4)	Domain Trust Discovery	Remote Services (6)	Encrypted Channel (2)	Data from Information Repositories (2)	Exfiltration Over Other Network Medium (1)	Endpoint Denial of Service (4)	Endpoint Denial of Service (4)
Supply Chain Compromise (3)	Software Deployment Tools	Compromise Client Software Binary	Event Triggered Execution (15)	Exploitation for Defense Evasion	File and Directory Discovery	Replication Through Removable Media	Fallback Channels	Data from Local System	Firmware Corruption	Inhibit System Recovery	Inhibit System Recovery
Trusted Relationship	System Services (2)	Create Account (3)	Exploit for Privilege Escalation	Man-in-the-Middle (1)	Network Service Scanning	Software Deployment Tools	Ingress Tool Transfer	Data from Network Shared Drive	Exfiltration Over Physical Medium (1)	Network Denial of Service (2)	Network Denial of Service (2)
Valid Accounts (4)	User Execution (2)	Create or Modify System Process (4)	Group Policy Modification	Modify Authentication Process (3)	Network Share Discovery	Taint Shared Content	Multi-Stage Channels	Data from Removable Media	Exfiltration Over Web Service (2)	Resource Hijacking	Resource Hijacking
	Windows Management Instrumentation	Event Triggered Execution (15)	Hide Artifacts (6)	Network Sniffing	Network Sniffing	Use Alternate Authentication Material (4)	Non-Application Layer Protocol	Data Staged (2)	Non-Standard Port	Scheduled Transfer	Scheduled Transfer
	External Remote Services	Hijack Execution Flow (11)	Hijack Execution Flow (11)	OS Credential Dumping (8)	Passport Policy Discovery	Email Collection (3)	Protocol Tunneling	Email Collection (3)	Protocol Tunneling	Service Stop	Service Stop
	Hijack Execution Flow (11)	Process Injection (11)	Impair Defenses (6)	Steal Application Access Token	Peripheral Device Discovery	Input Capture (4)	Proxy (4)	Input Capture (4)	Proxy (4)	Transfer Data to Cloud Account	Transfer Data to Cloud Account
	Implant Container Image	Scheduled Task/Job (5)	Indicator Removal on Host (6)	Steal or Forge Kerberos Tickets (3)	Permission Groups Discovery (3)	Man in the Browser	Remote Access Software	Man in the Browser	Remote Access Software	System Shutdown/Reboot	System Shutdown/Reboot
	Office Application	Valid Accounts (4)	Indirect Command Execution	Steal Web Session Cookie	Process Discovery						
			Masquerading (6)	Two-Factor	Query Registry						
					Remote System						

<https://attack.mitre.org/>

Essential Decisions

Design

Uninformed vs Informed

External Offensive Team vs Internal Offensive Team

Purple Team Exercise Types

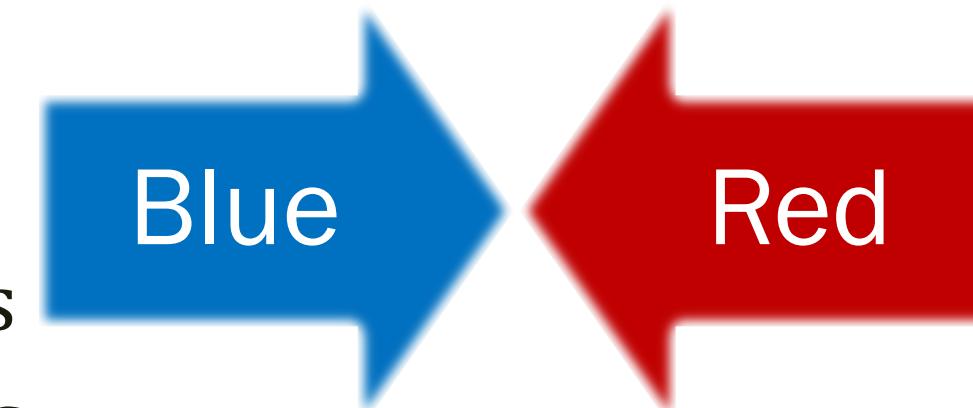
- *Scenario Automation*
- *Capture the Flag (Red vs Blue)*
- *Assume Breach*



Team Structure

Design

Threat Intelligence
Cyber Response
Cyber Detection
Security Awareness
Security Operations



Red Team
Offensive Security
Penetration Testing
External Provider

Consider Some Guest Players

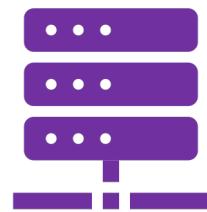
Essential Requirements

Design

Threat Intelligence Data and/or Simulation Scenario

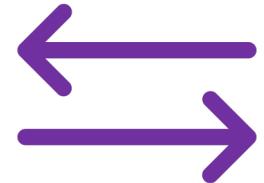
Technical Requirements

- *Accounts, Credentials*
- *Laptops, Servers*



Business Requirements

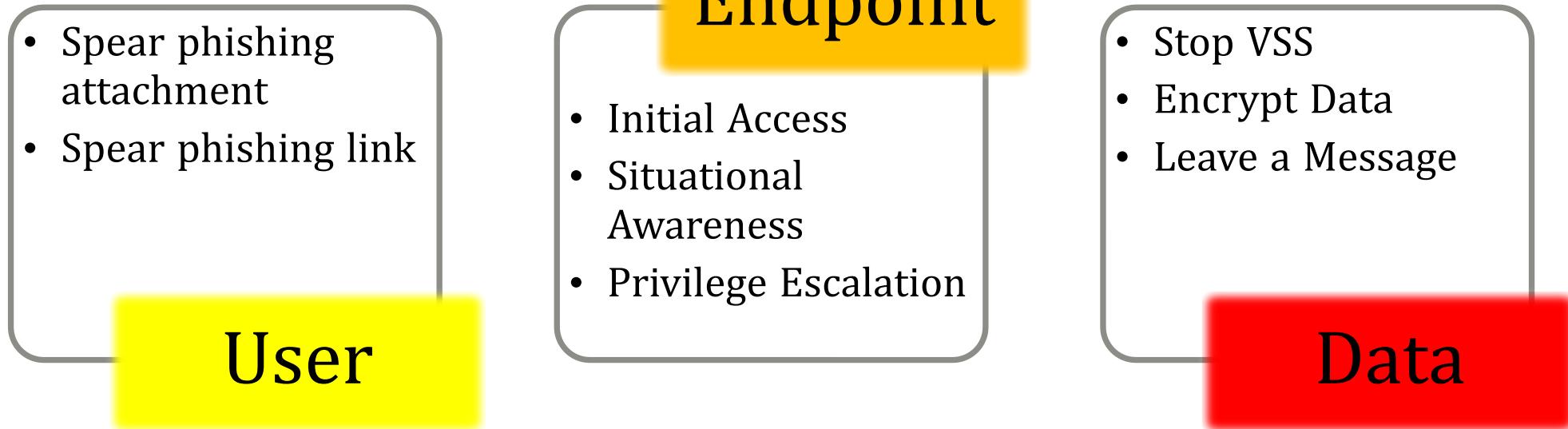
- *Resource Requirements*
- *Change Requests, Approvals*



Scenarios (Ransomware)

Design

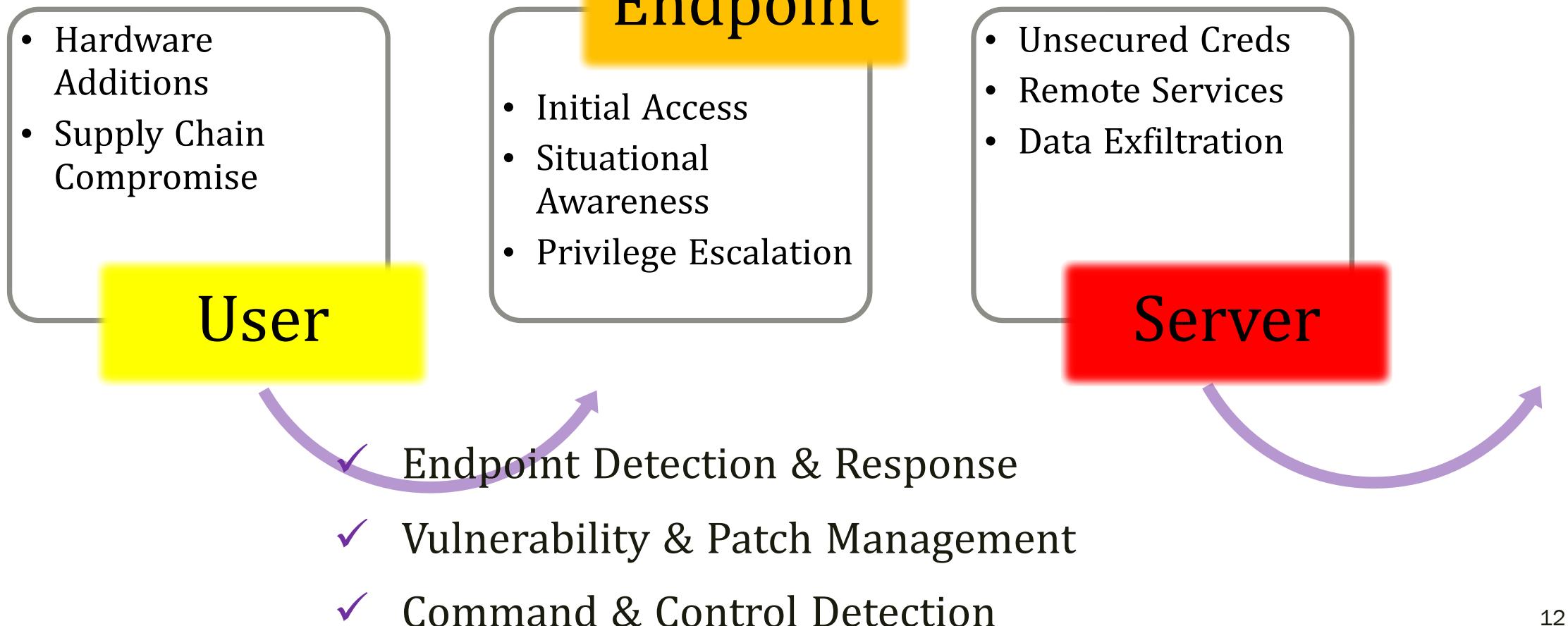
- ✓ Mail Gateway & Controls
- ✓ Proxy & Secure Internet
- ☐ User Awareness
 - Spear phishing attachment
 - Spear phishing link



Scenarios (Supply Chain)

Design

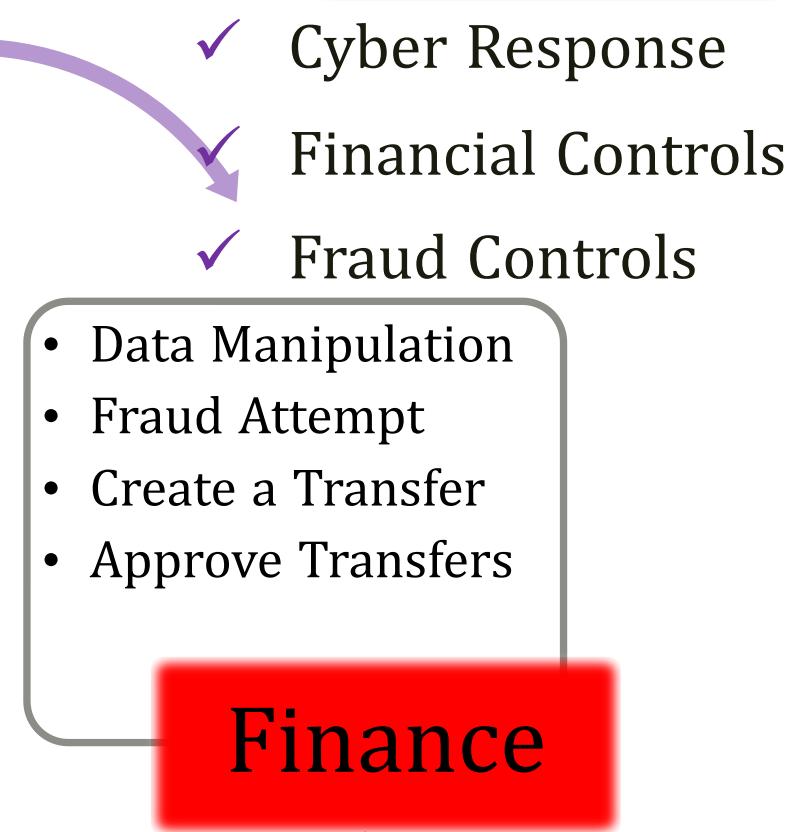
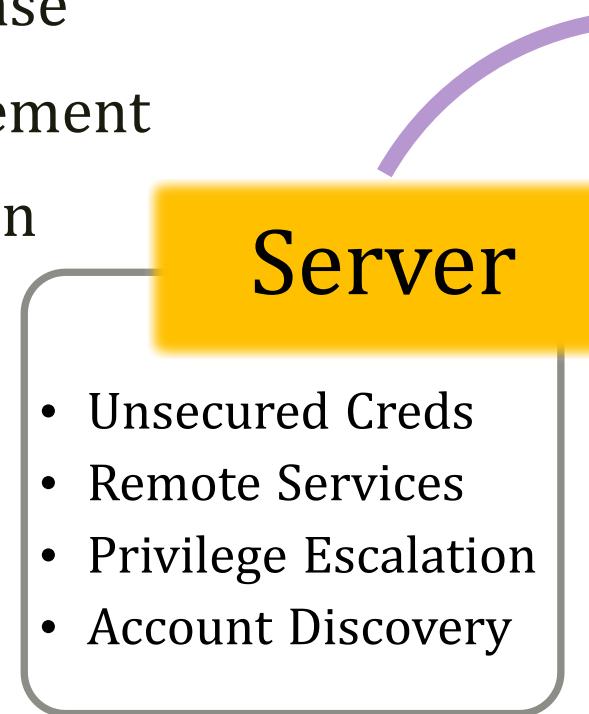
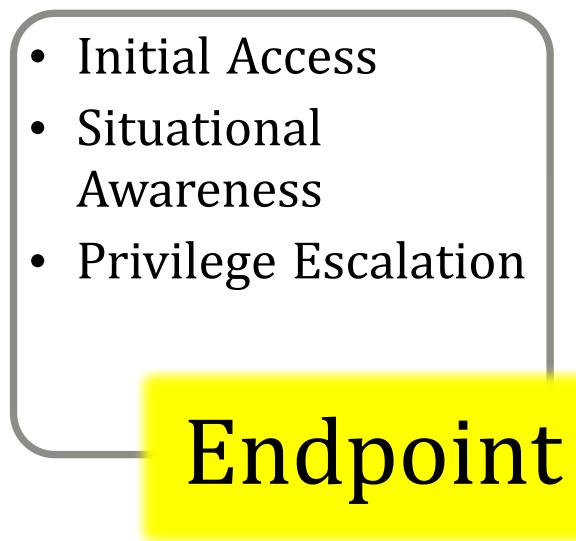
- ✓ Physical Access
- ✓ Software & Inventory Management
- ✓ Hardware Monitoring & Detection



Scenarios (Assume Breach)

Design

- ✓ Endpoint Detection & Response
- ✓ Vulnerability & Patch Management
- ✓ Command & Control Detection



- ✓ Cyber Response
- ✓ Lateral Movement Detection

Scenario Automation

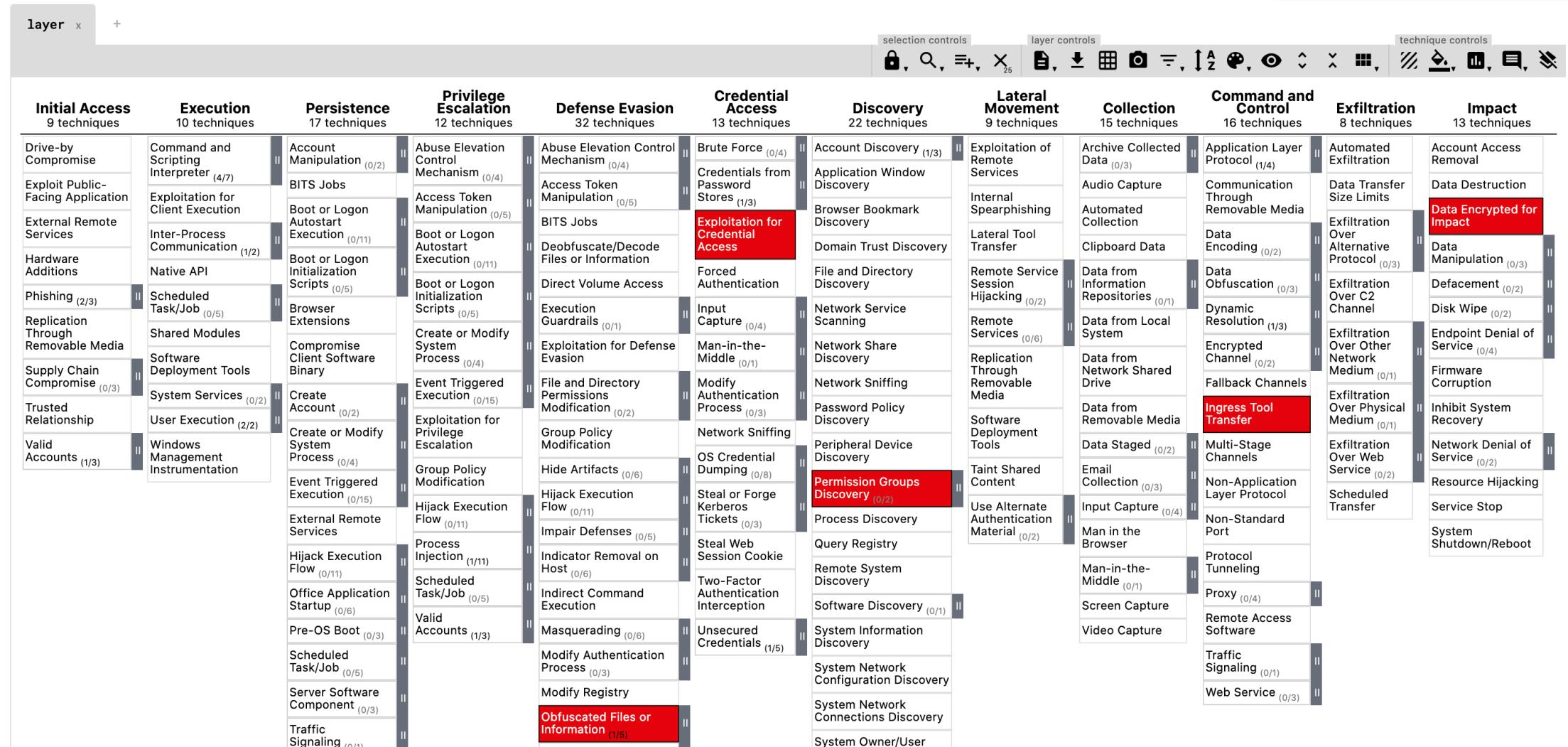
Design

Since 2016, there are active researches on automating the adversary behaviours and tradecraft for continuous defence improvements. While MITRE teams lead the researches in this area [ref:1,2,3,4]; there are also other researchers [ref:5,6] proposing additional aspects of the automation.

- *Efficient ways of simulating the threat actors*
- *Planning and execution phases are as important as techniques*
- *Developing open source projects and tools to implement it*
- *Scenario runs to demonstrate the efficiency*
- *Demonstrating the Kill Chain similar approach to stop the attacks*

Coverage: Mitre Att&ck Navigator

Design



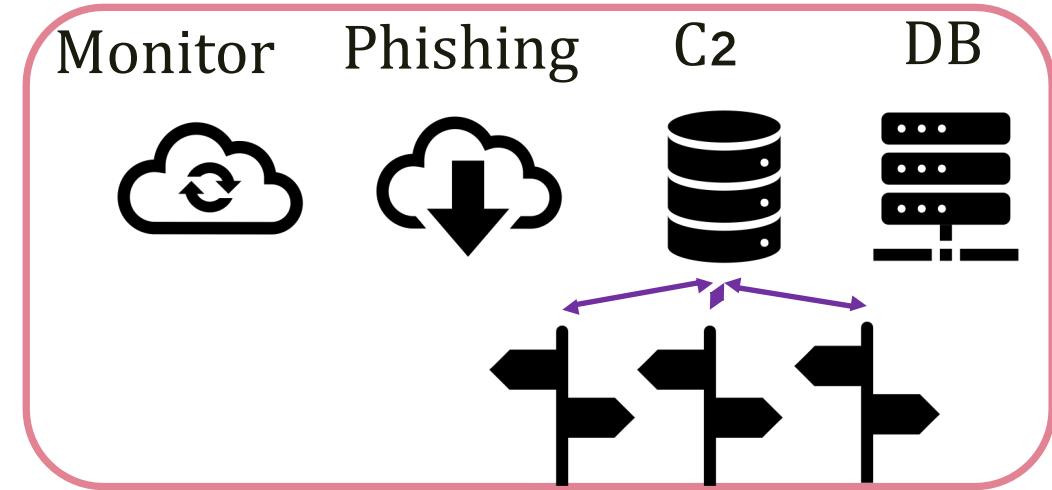
<https://mitre-attack.github.io/attack-navigator/enterprise/>

Platform

Development

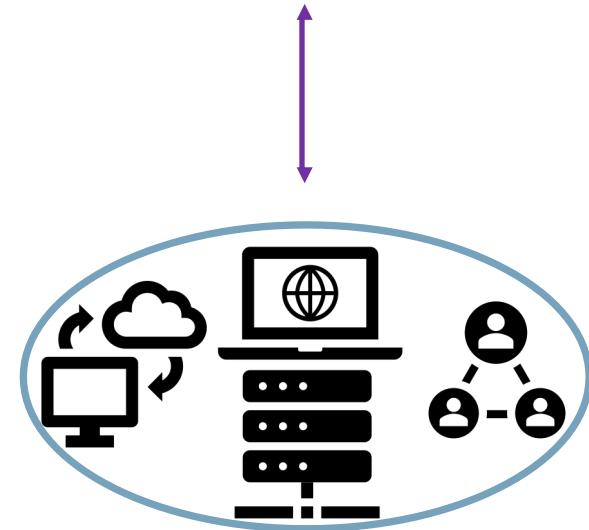
Cloud Deployment

- *Provider Selection*
- *Services: Storage, DB, VM, OS*
- *Domains: Fronted, Aged, Classified*



Operational Security

- *Real-Time Monitoring*
- *Encrypting Data in Transit and at Rest*
- *Implement Compliance Requirements*

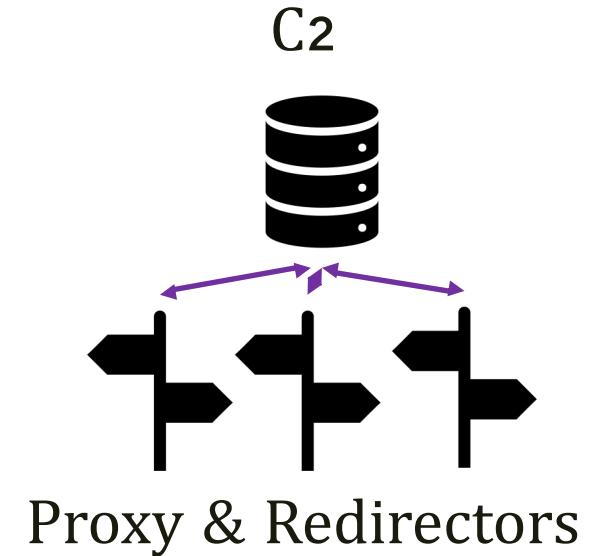


Software: Command & Control

Development

Command & Control Service Selection

- *What does the threat actor use?*
- *What operating systems are targeted?*
- *Multi Instance: Long Term, Short Term, Interactive*
- *C2 Protocols, Cloud Native, Multi User, Logging...*



Safer C2 Choices

- *Cobalt Strike (Commercial, Favorite of Threat Actors and Red Teams)*
- *Covenant (C#, Open Source, Mostly Stable)*
- *SilentTrinity (.NET and Python, Open Source, Stable)*

Software: Command & Control

Development

C2 Matrix

- *Keeping a C2 List*
- *Filtering for C2 features*

If threat actor uses Metasploit or PS Empire, and you want to emulate it, then consider using that



ABOUT ASK DOCUMENTATION FEEDBACK GUI MATRIX

Information	Code + UI	Channels	Agents	Capabilities	Support
C2	Version Reviewed	Implementation			
Apfell	1.3	Docker			
Caldera	2	pip3			
Cobalt Strike	2	binary			
Covenant	0.3	Docker			
Dali	POC	pip3			
Empire	2.5	install.sh			
EvilOSX	7.2.1	pip3			
Faction C2	N/A	install.sh			
FlyingAFalseFlag	POC	pip3			
godoh	1.6	binary			
ibombshell	0.0.3b	pip3			
INNUENDO	1.7	install.sh			
Koadic C3	0xA (10)	pip3			
MacShellSwift	N/A	python			
Metasploit	5.0.62	Ruby			
Merlin	0.8.0	Binary			
Nuages	POC	setup.sh			
Octopus	v1.0 Beta	pip3			
PsExec		install.sh			

<https://www.thec2matrix.com/matrix>

Software: Scenario Automation

Development

Mitre Att&ck - Caldera (Apache License)

User Interface, Custom Implant (Sandcat),

<https://github.com/mitre/caldera> , https://www.youtube.com/watch?v=_mVGjqu03fg

Red Canary - Atomic Red team (MIT License)

A repository for Powershell/.NET/Command Scripts for Mitre Att&ck PoC

<https://redcanary.com/atomic-red-team/>, <https://atomicredteam.io/testing>

Mordor (GNU Public License)

Better Integration with Defense tools.

<https://github.com/hunters-forge/Mordor>

<https://github.com/hunters-forge/ThreatHunter-Playbook>

Software: Petaq C2

Development

Petaq Purple Team Command & Control Server (MIT License)

- *P'takh (petaQ) is a Klingon insult, meaning something like "weirdo"*
- *Protocols : HTTPS, WebSocket, SMB Named Pipe, TCP, UDP*
- *Execution : CMD, .NET Assembly, Source, Shellcode Injection, PowerShell*
- *Features : WMI Lateral Movement, Nested Implant Linking, Encryption*
- *Scenario Based Automation and TTP Support*

Petaq is suitable to interactive and scenario based exercises, both

<https://github.com/fozavci/petaqc2>

Software: Support Environment

Development

Kill Chain

- *Spear phishing : GoPhish*
- *Initial Access, Evasion, Awareness : Unicorn, SharpShooter, Ghost Pack*
- *Active Directory : Bloodhound, Ping Castle, Rubeus, Kekeo*
- *Lateral Movement : SharpMove, SharpWMI, PSEexec, ScShell*

Support Services for Deployment or Redirection

- *Cloud Services : S3, DynamoDB, Lambda, Azure Blob, Office 365 Tasks*
- *Proxies : Nginx, Apache, Haproxy*

Software: Operational Security

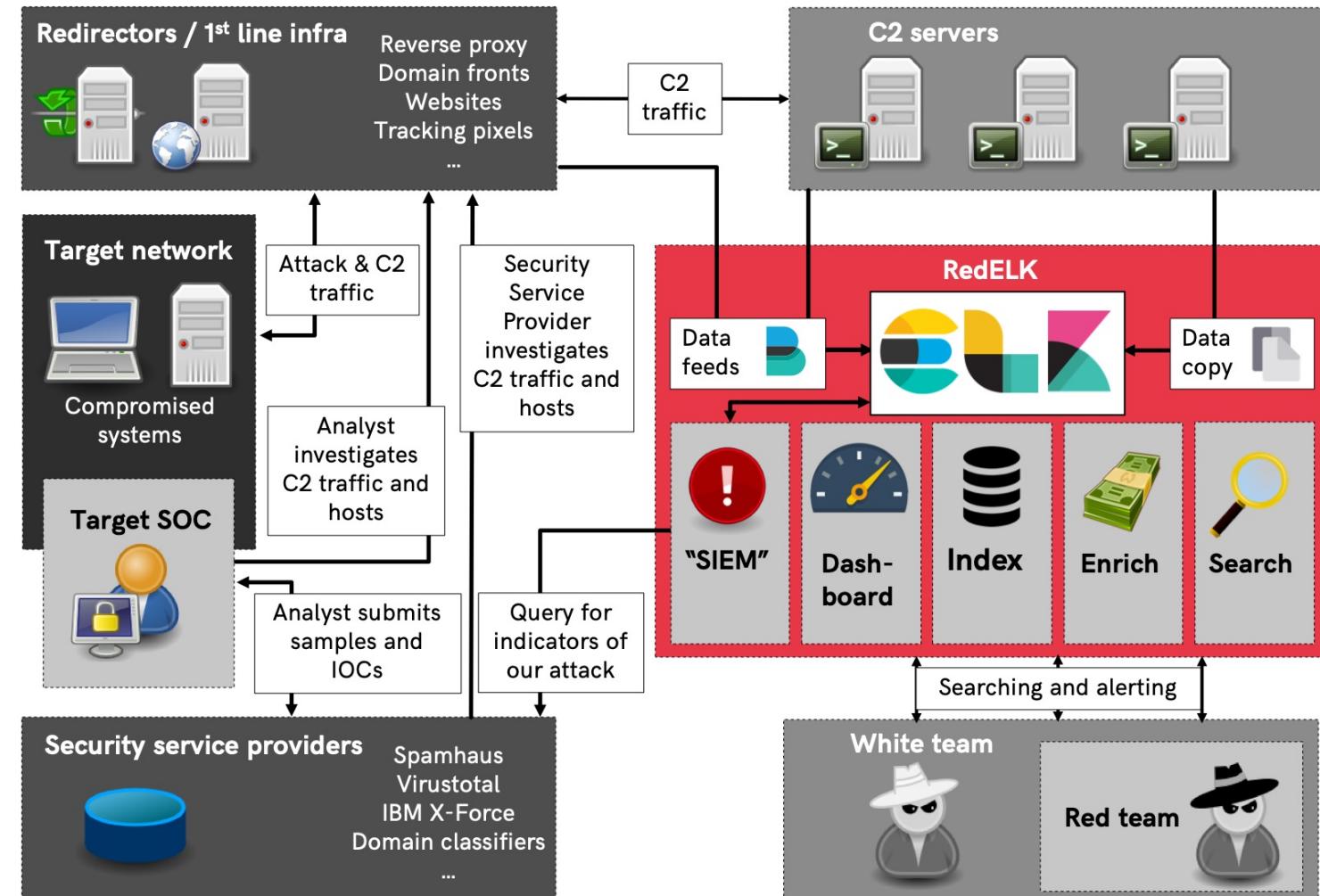
Development

RedELK

- *Open Source*
- *Processing C2 Logs*
- *Processing Proxy Logs*
- *Check IOC Websites/Feeds*

Benefits

- *Protect the Platform*
- *Observe the Blue Team*
- *Avoid Unwanted Victims*



<https://github.com/outflanknl/RedELK>

Planting the Flags

Development

Flags are useful to assess the team capabilities such as reverse engineering, malware analysis and utilising the security controls.

- *Phishing email (e.g. headers, content)*
- *Initial malware stages (e.g. command, dropper, stage 1, stage 2)*
- *C2 communications (e.g. profile, protocol)*
- *Persistency options (e.g. registry, file IOCs, services)*
- *Lateral movement (e.g. remote service, WMI query, creds)*
- *Data exfiltration (e.g. fake DLP flags, C2 channels, WebDAV)*

Use a Capture the Flag scoring website or application



Exercise Run Tips

Run

Attacks take time to show up on SOC monitors and alerts.

- *Run the attacks or scenario, and give a grace period*
- *The exercise duration may be 2-3 days due to scope*



Use a CTF or reporting software to give a metric to all parties.

Assign a facilitator to the exercise.

- *Maintain the pressure like the real life exercise*
- *It's not a race, but a friendly competition*



Blue team should receive all tradecraft, logs and IOCs

Vectr - Monitoring and Reporting

Run

Vectr is designed to provide metrics to the Red and Blue teams during the Purple Team exercises.

- *TTP Details*
- *Mitre Att&ck Mapping*
- *Detection/Prevention*
- *Response/Flags*

The screenshot shows a detailed view of a test case titled "Edit Extract Logonpasswords via Dumper Test Case". The interface is divided into several sections:

- Status:** Completed
- Attack Start:** 07/01/2020 09:54:20, status changed to InProgress
- Attack Stop:** 07/01/2020 09:54:21, status changed to Completed
- Source IPs:** Linux VM
- Red Team Details:** Name: Extract Logonpasswords via Dumper, Description: Use dumper to extract credentials from LSASS process memory, Technique: Credential Dumping, Phase: Credential Access, Operator Guidance: beacon> dumper, References: +
- Blue Team Details:** Outcome: Blocked (checked), Detected, NotDetected, Detecting Blue Tool(s): EDR platform, Was an alert triggered?: Yes (checked), SIEM, EDR, Endpoint Protection
- Detection Time:** 07/01/2020 09:55:48, outcome changed to Blocked
- Expected Detection Layers:** SIEM, EDR, Endpoint Protection
- Tags:** High Priority, RE-TEST
- Rules:** +
- Detection:** 1) Suspicious process execution is detected by EDR or other endpoint security tool, or alerted in SIEM based on Windows or sysmon event IDs
- Prevention:** 1) Suspicious process execution is blocked by EDR or other endpoint security tool

<https://vectr.io/>

Uplift the Game



Run

Add Variations to Command & Control

- *Cloud Native C2s (e.g. Serverless Apps, Direct DB Connections, JavaScript Everywhere)*
- *C2 Traffic Cloud to Cloud (e.g. Deploying the C2 in another tenant of target cloud)*
- *Domain Fronting (e.g. Leveraging Cloud Fronting services with Domain/SNI masking)*
- *Newest HTTP Protocols (e.g. Mobile push on HTTP/2 or HTTP/3, WebRTC, WebSocket)*

Improve Evasion Techniques

- *Reloading a clean NTDLL and remapping API Calls*
- *Protecting the processes with Parent ID spoofing, Microsoft Process Tags and Hollowing*
- *Disabling the EDR monitoring in Kernel Space*

Adjust the Pace of Exercise for the Scenario Requirement



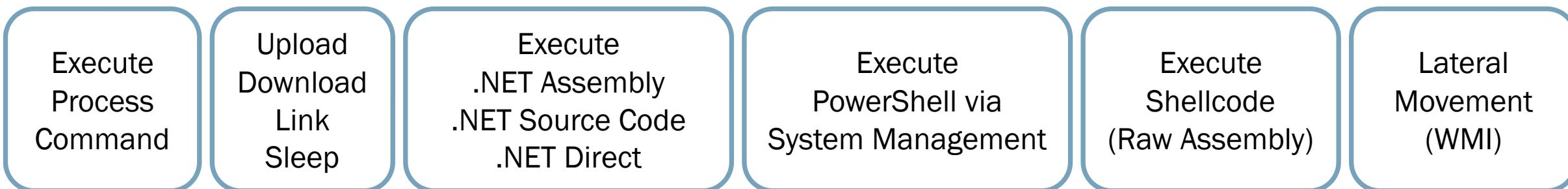
DEMO

Running Scenarios Through Petaq

```
{  
    "threat_actor": "Demo Threat Actor!", ← Threat Actor  
    "ttps": [  
        "T1087.001", ← TTP IDs (Filenames)  
        "T1087.002",  
        "T1059.001",  
        "T1127.001-v2",  
        "T1041",  
        "Seatbelt",  
        "ShellcodeInvoke",  
        "InlineCSharp",  
        "T1562.004",  
        "T1047",  
        "T1571"  
    ]  
}
```

Preparing TTPs for Petaq

```
{  
  "name": "Enumerate users and groups", ← Name  
  "mitreid": "T1087.001", ← Mitre Att&ck ID  
  "description": "Getting the users and groups via net command.", ← Description  
  "instructions": [  
    "exec cmd /cnet users", ← Instructions  
    "exec cmd /cnet groups"  
  ]  
}
```



Use real tradecraft such as PowerUp, Mimikatz, Seatbelt, SharpMove, WMI, SC, PSExec

Preparing TTPs for Petaq

```
{  
  "name": "Non-Standard Port",  
  "mitreid": "T1571",  
  "description": "Adversaries may communicate using a protocol and port pairing  
  that are typically not associated. For example, HTTPS over port 8088[1] or port  
  587[2] as opposed to the traditional port 443. Adversaries may make changes to  
  the standard port used by a protocol to bypass filtering or muddle analysis/  
  parsing of network data.",  
  "instructions": [  
    "link tcp://10.0.0.2/8002"  
  ]  
}
```

```
Administrator: TrustedCS
Connecting to the websocket at ws://172.16.121.1/ws.
Connecting to ws://172.16.121.1/v TrustedCS
Linking to the C2 via websocket.
The websocket connection is successfully established.
Registering the implant information.
Registering the linked sessions.
Registering the linked sessions.
registerlinks e30=
Waiting for an instruction...
PetaqC2-PC
TrustedCS
```

```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>
C:\Users\Administrator>

Administrator: C:\Windows\system32\cmd.exe - powershell
PS C:\Users\exchangeadmin>
```

2020-8-26---17-20-38
Hosting environment: Development
Content root path: /Users/case/Documents/Research/PetProjects/petaq_videos/petaqc2_v0.2_auscert/petaqservice
Now listening on: https://0.0.0.0:443
Now listening on: http://0.0.0.0:80
Application started. Press Ctrl+C to shut down.
Petaq - Purple Team Simulation Kit
Log file Logs/2020-8-26---17-20-38/WK4P9QQ10JW1WN8N48E.txt created.
Registering the implant...
Implant registration for WK4P9QQ10JW1WN8N48E is done.
Links are adding to the implant...
Log file Logs/2020-8-26---17-20-38/WNOVOD22XSS9LGWL1G7L.txt created.
Registering the implant...
Implant registration for WNOVOD22XSS9LGWL1G7L is done.
Links are adding to the implant...
list

Session ID	User Name	Hostname	IP Address	Status	Link URI
WNOVOD22XSS9LGWL1G7L	GALAXY\exchangeadmin	geonosis	172.16.121.137	connected	ws://172.16.121.1:80/ws
WK4P9QQ10JW1WN8N48E	GALAXY\anakin	geonosis	172.16.121.137	connected	ws://172.16.121.1:80/ws

```
# [ ]
```

Conclusion

Various exercise types exist, find/develop a tailor fit exercise

- *Your adversary, your environment, your people, your software*

Benefits of Purple Team Exercises

- *Overall defence level for certain threats*
- *Security weaknesses or vulnerabilities*
- *Uplifting the existing skills sets and resources*
- *Measuring software and solution efficiency*

Specialists first, software later...

Research

1. Applebaum, A., Miller, D., Strom, B., Korban, C., & Wolf, R. (2016, December). Intelligent, automated red team emulation. In Proceedings of the 32nd Annual Conference on Computer Security Applications (pp. 363-373).
2. Applebaum, A., Miller, D., Strom, B., Foster, H., & Thomas, C. (2017, July). Analysis of automated adversary emulation techniques. In Proceedings of the Summer Simulation Multi-Conference (pp. 1-12).
3. Strom, B. E., Battaglia, J. A., Kemmerer, M. S., Kupersanin, W., Miller, D. P., Wampler, C., ... & Wolf, R. D. (2017). Finding cyber threats with ATT&CK-based analytics. The MITRE Corporation, Bedford, MA, Technical Report No. MTR170202.
4. Miller, D., Alford, R., Applebaum, A., Foster, H., Little, C., & Strom, B. (2018). Automated adversary emulation: A case for planning and acting with unknowns. MITRE: McLean, VA, USA.
5. Yoo, J. D., Park, E., Lee, G., Ahn, M. K., Kim, D., Seo, S., & Kim, H. K. (2020). Cyber Attack and Defense Emulation Agents. Applied Sciences, 10(6), 2140.
6. Klosa, C., Schoenborn, J. M., & Althoff, K. D. Evaluation of CEBRAS: A Case-based Reasoning Adversary Emulation System.

References

- *Petaq C2* (<https://github.com/fozavci/petaqc2>)
- *Cobalt Strike* (<https://www.cobaltstrike.com>)
- *Covenant* (<https://github.com/cobbr/Covenant>)
- *SilentTrinity* (<https://github.com/byt3bl33d3r/SILENTTRINITY>)
- *Caldera* (<https://github.com/mitre/caldera>)
- *Ghost Pack* (<https://github.com/GhostPack/>)
- *GoPhish* (<https://getgophish.com/>)
- *SCShell* (<https://github.com/Mr-Un1kod3r/SCShell>)
- *RedELK* (<https://github.com/outflanknl/RedELK>)

THANKS