Learn to Think Like the Enemy

Improve your Detection & Response Capabilities

Semih Gelişli
MANAGER, IT SECURITY INCIDENT MANAGEMENT

Ozan Olalı
IBM SECURITY SERVICES LEADER

IBM Security

YapıKredi Teknoloji

IBM

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 it’s 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 it’s limits

Penetration Testing

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

Red Teaming & Adversary Simulation

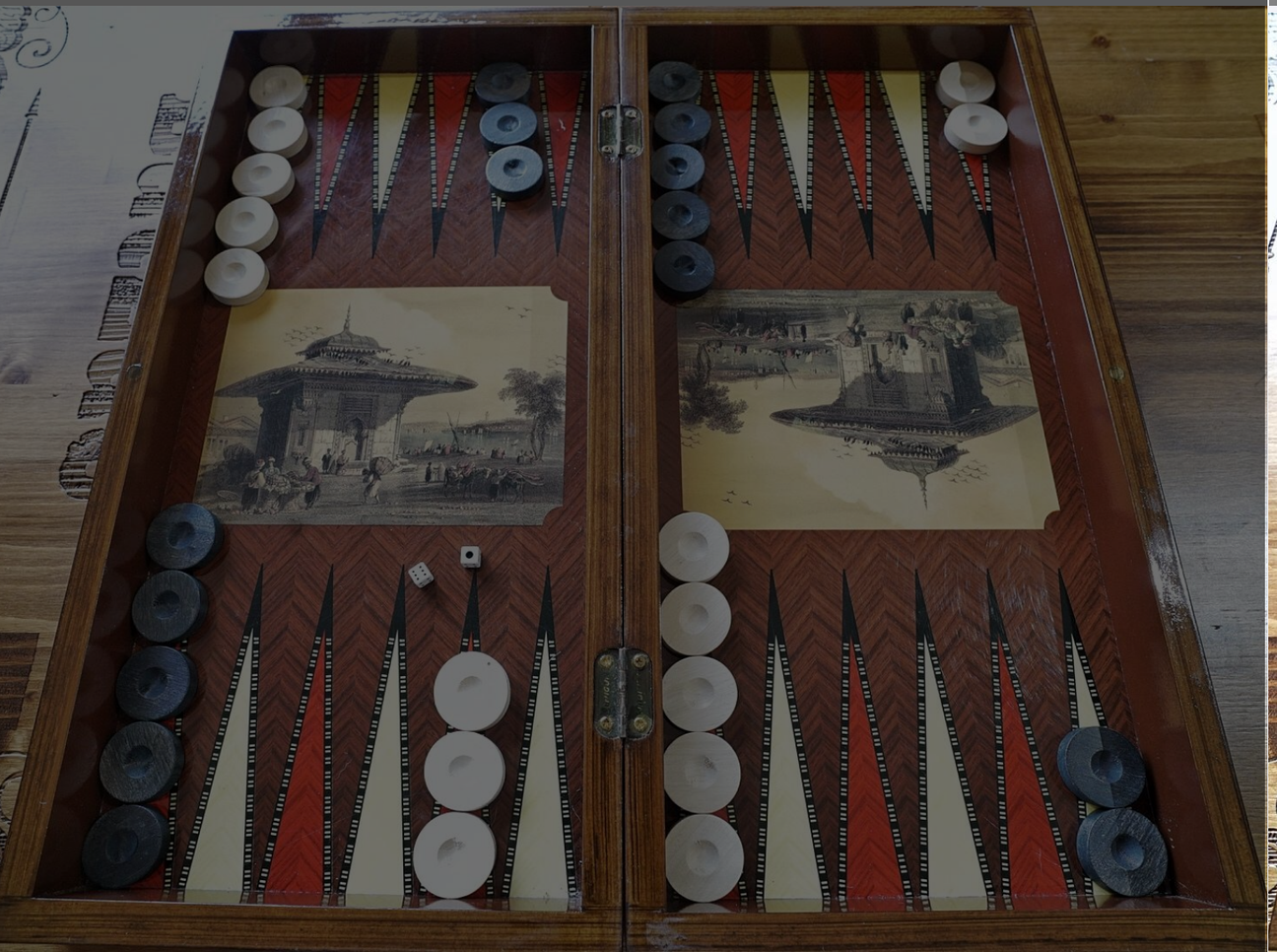
- Not limited with the artificial constraint
- More Opportunities to Consider
- Close to Motivated Adversary
- Business Risks
- Adds Value to Detection & General Posture
- Prepares & Educates Defensive Teams

Motivated Campaign with Adversary Simulation

Motivated Campaign with Adversary Simulation

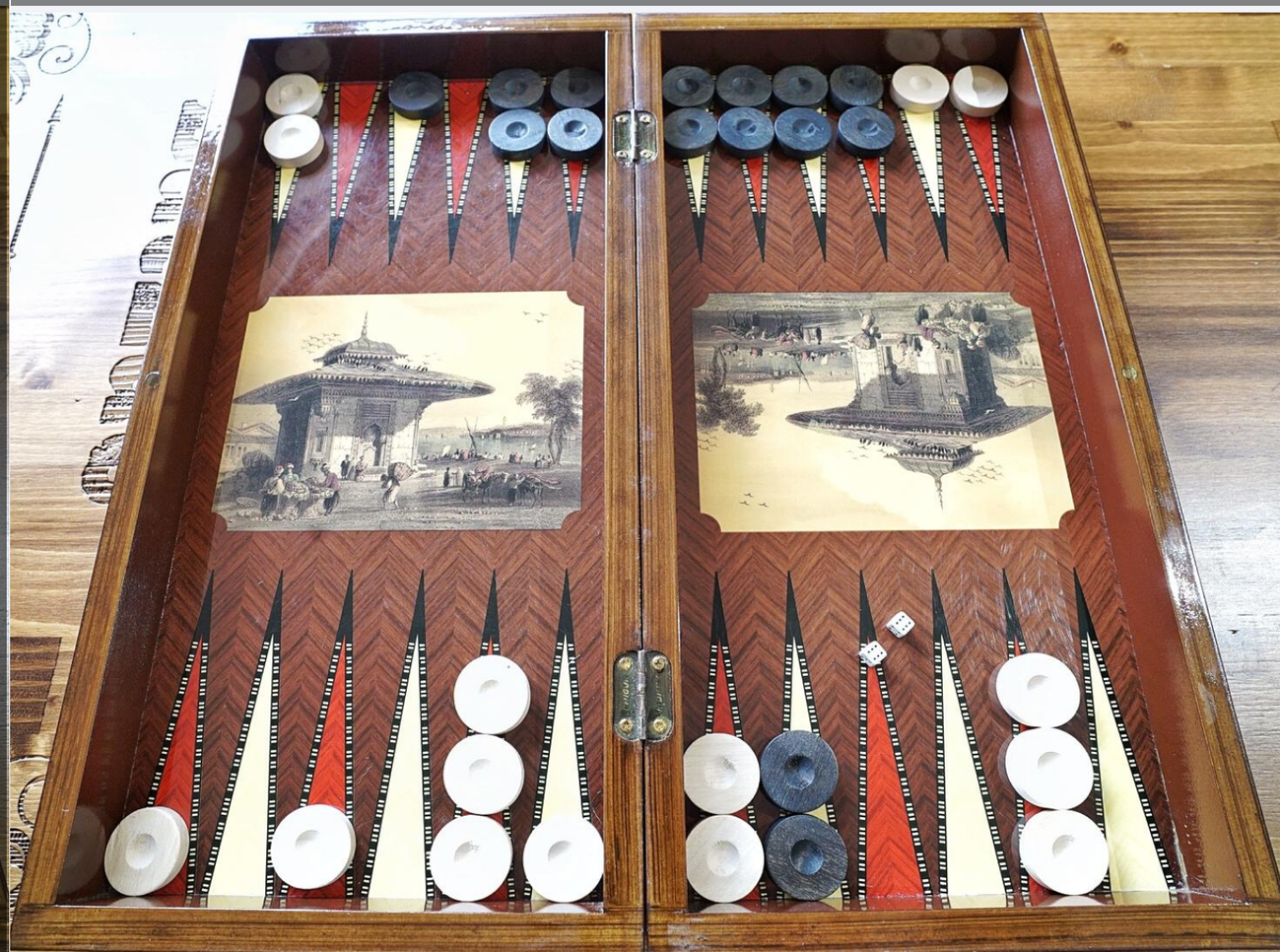
Testing & Simulations

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



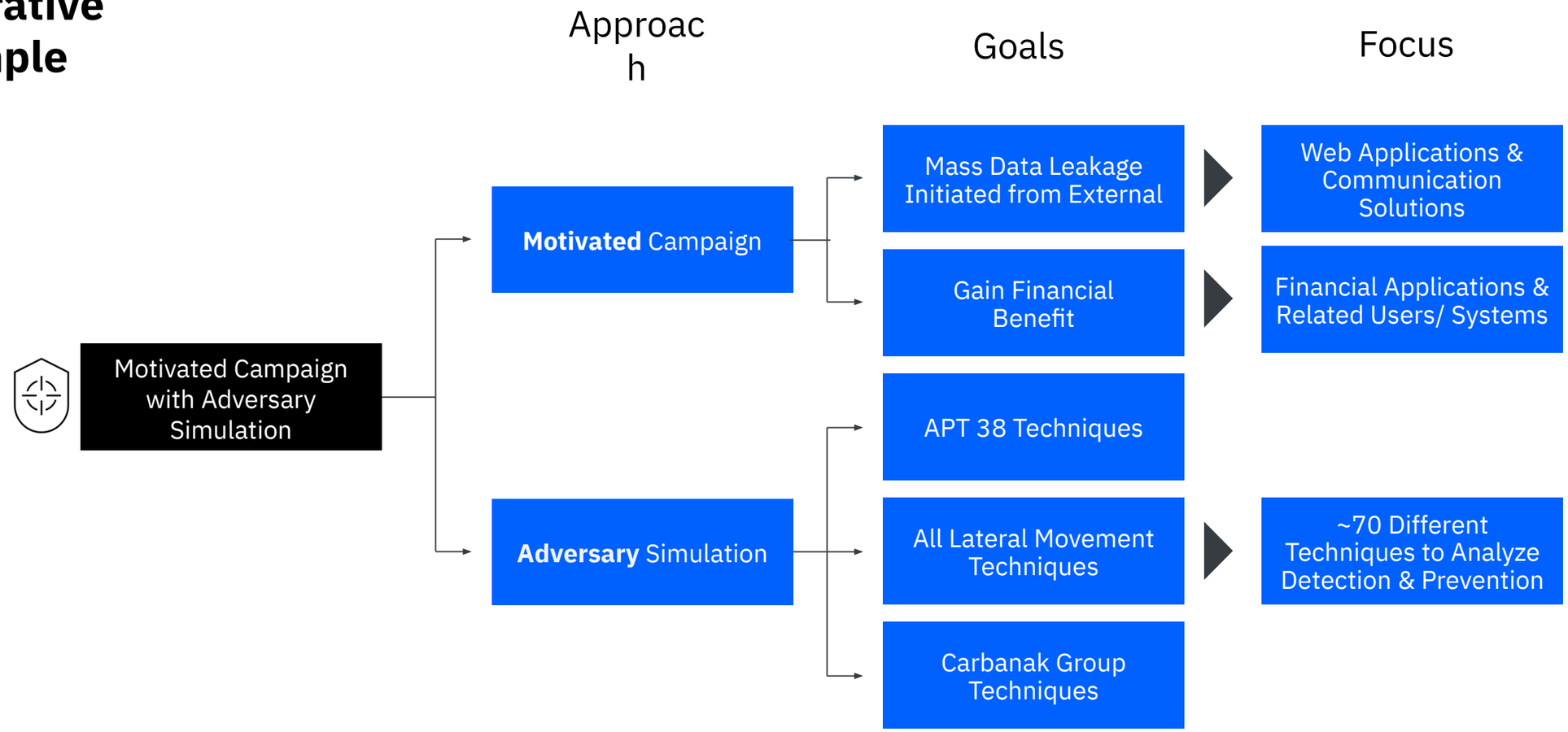
Real Life Situation

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.



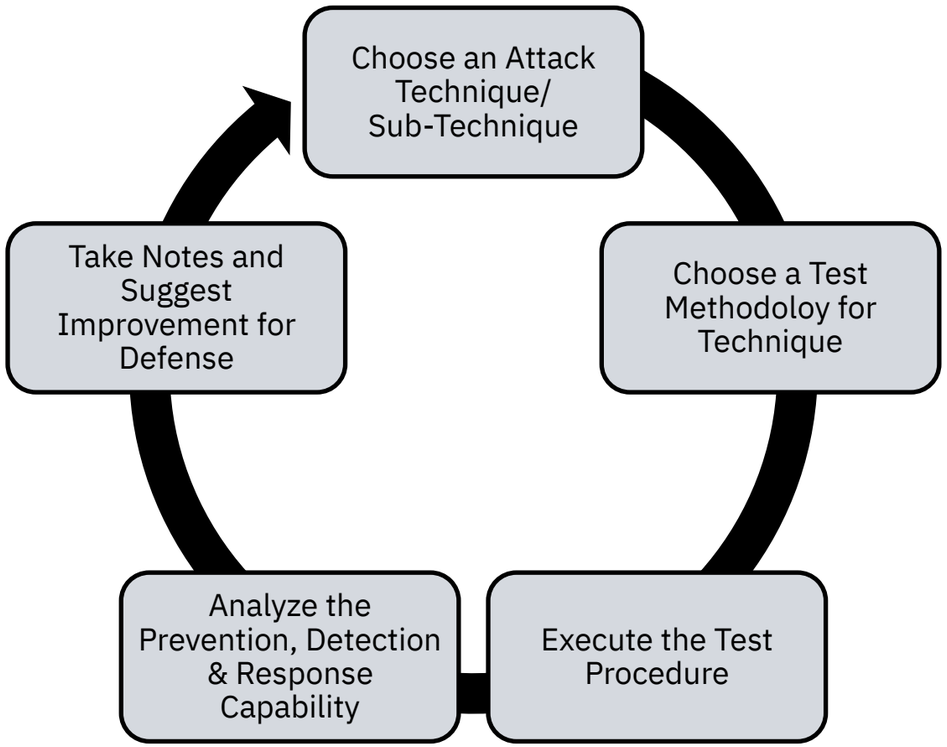
Defining the Goals, Focus Points, Tactics & Techniques

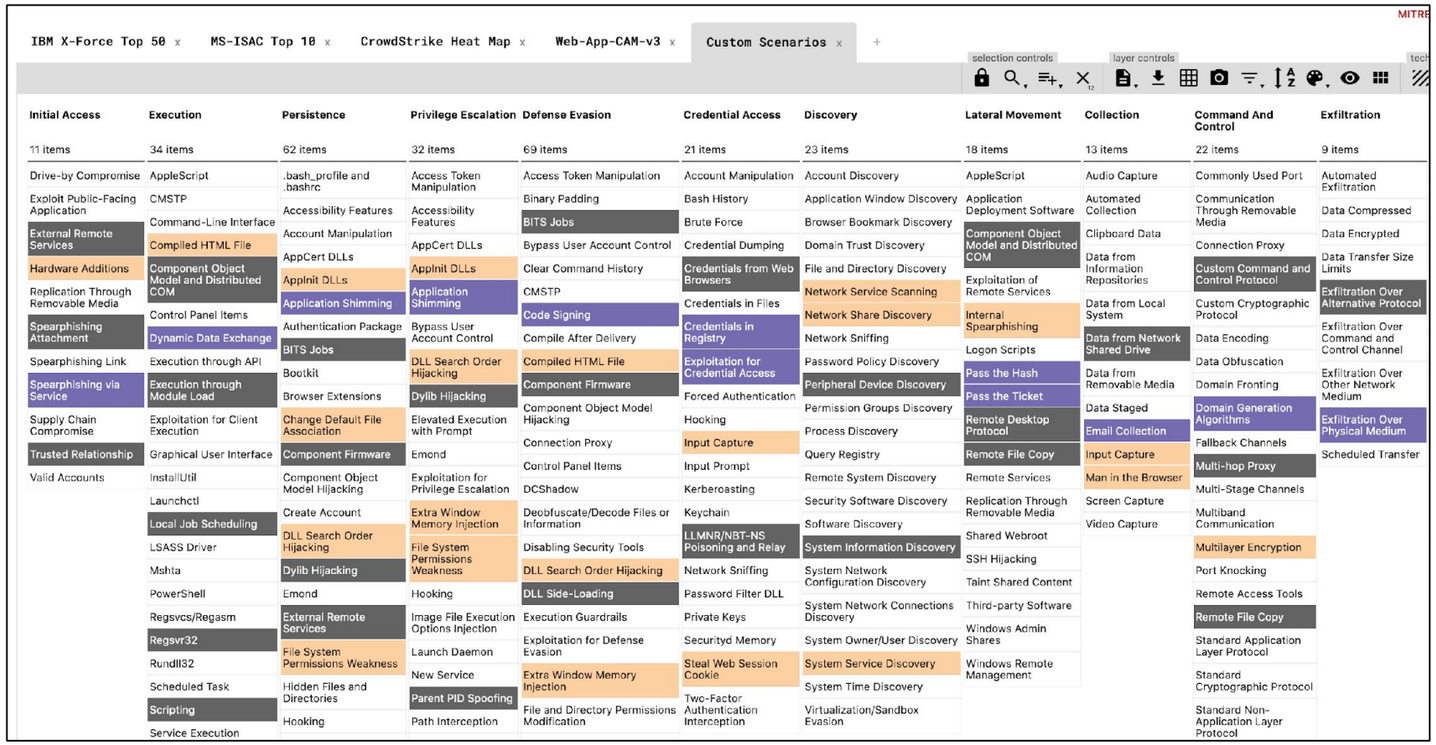
Illustrative Sample



Adversary Simulation

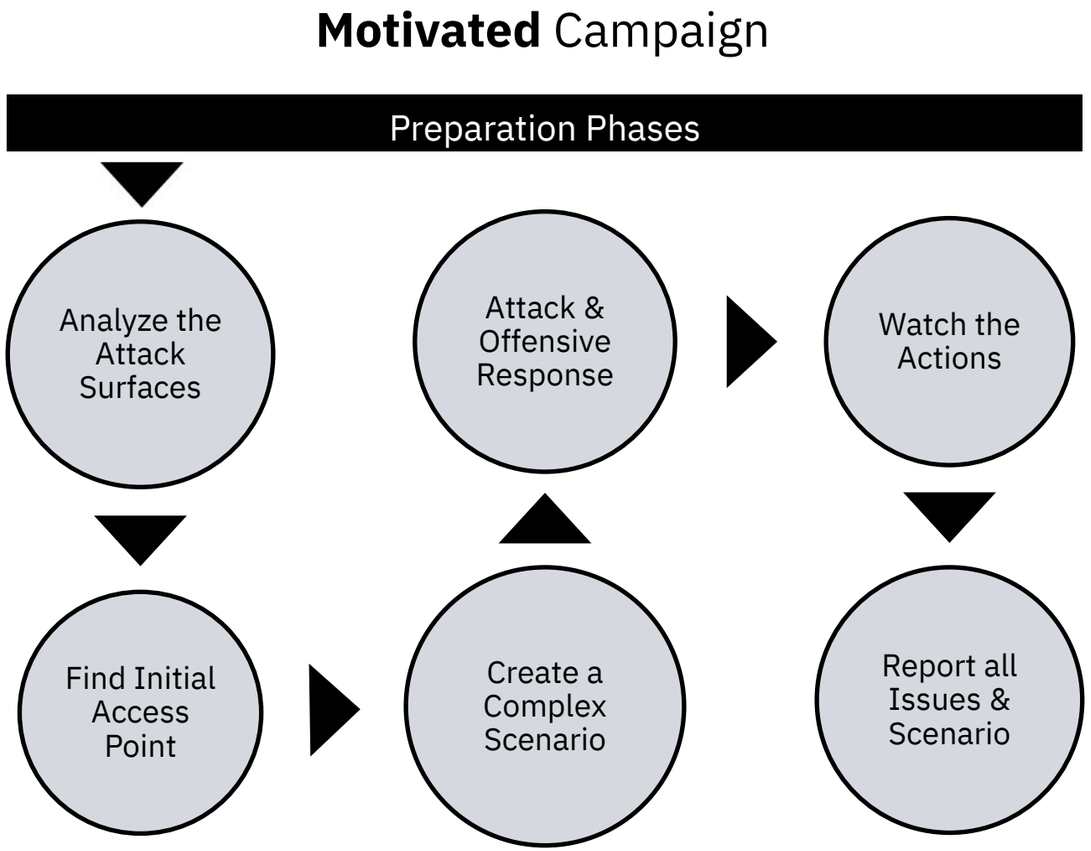
Adversary Simulation





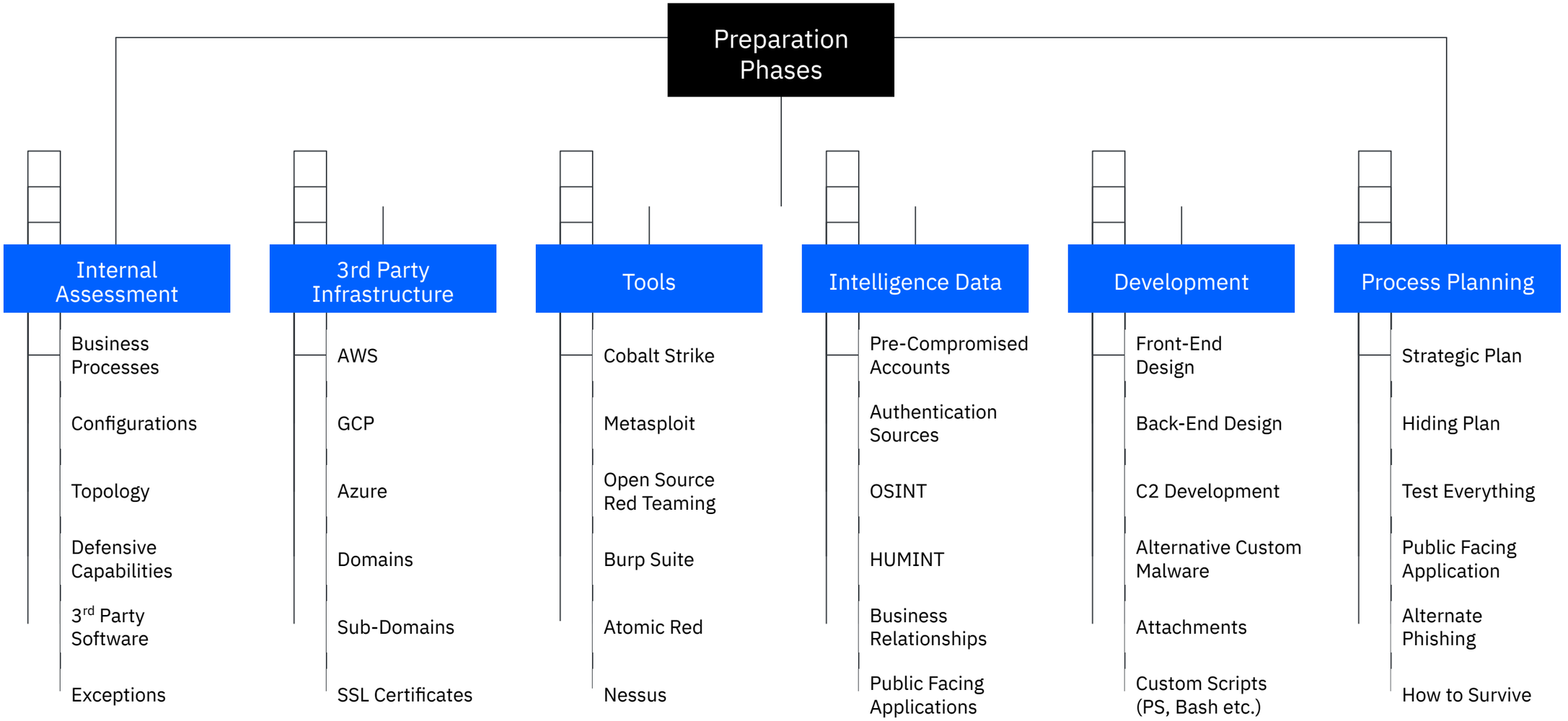
Gather the Information like Adversary Actors, Fast Forward their behavior

Motivated & Targeted Campaign Simulation



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

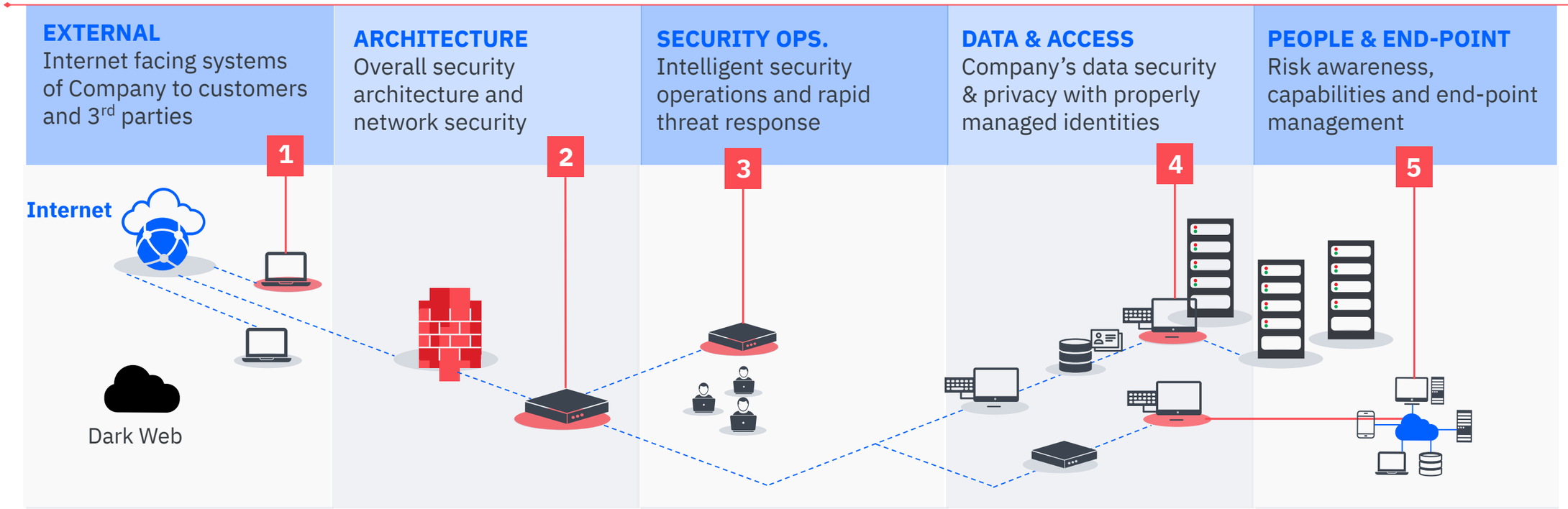
Accelerate Preparation for Campaign



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

The Preparation Assessments

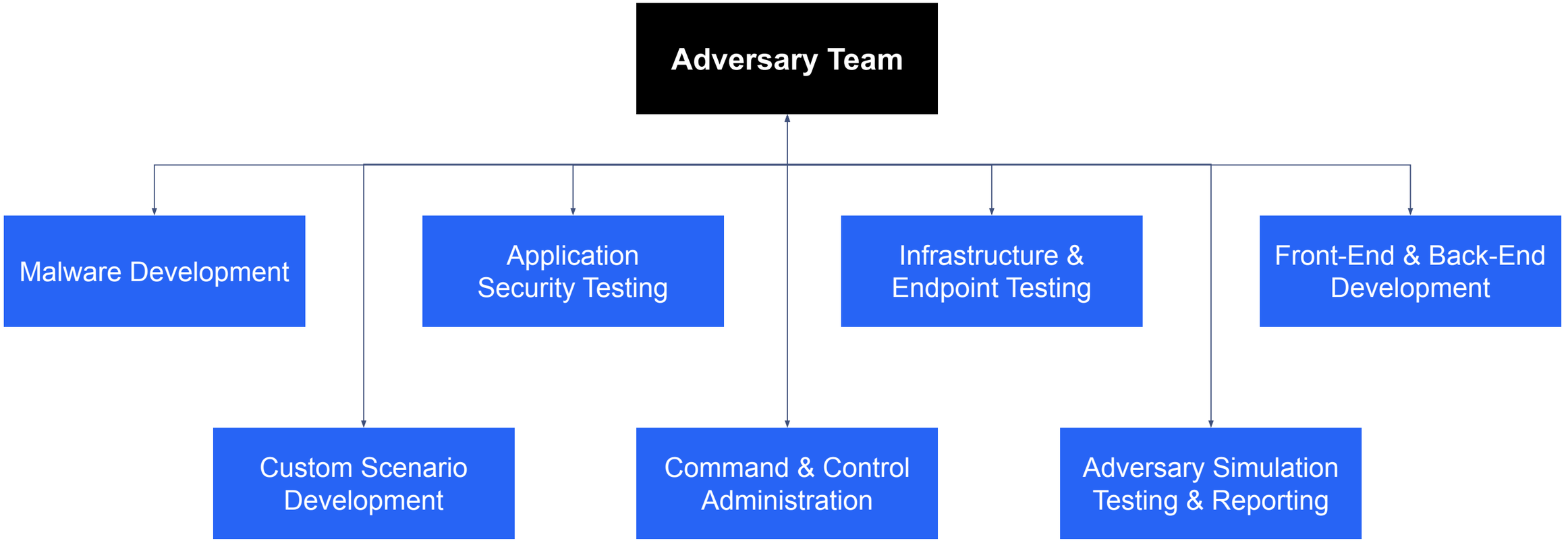
ASSESSMENT CHAIN



1	2	3	4	5
Assessing external network regarding security controls of delivery channels, web assets and 3rd parties' integrations.	Assessing Network Protection blocks and overall security architecture with topology, device positioning and system management.	Assessing incident handling and response processes of company with deep analysis of SIEM technology and its capabilities.	Assessing data security technologies, identity management approach regarding MS systems and Privileged (Service, Admin) accounts.	Assessing overall security staff capabilities, risk awareness and end-point (Laptop, Mobile) management technologies.

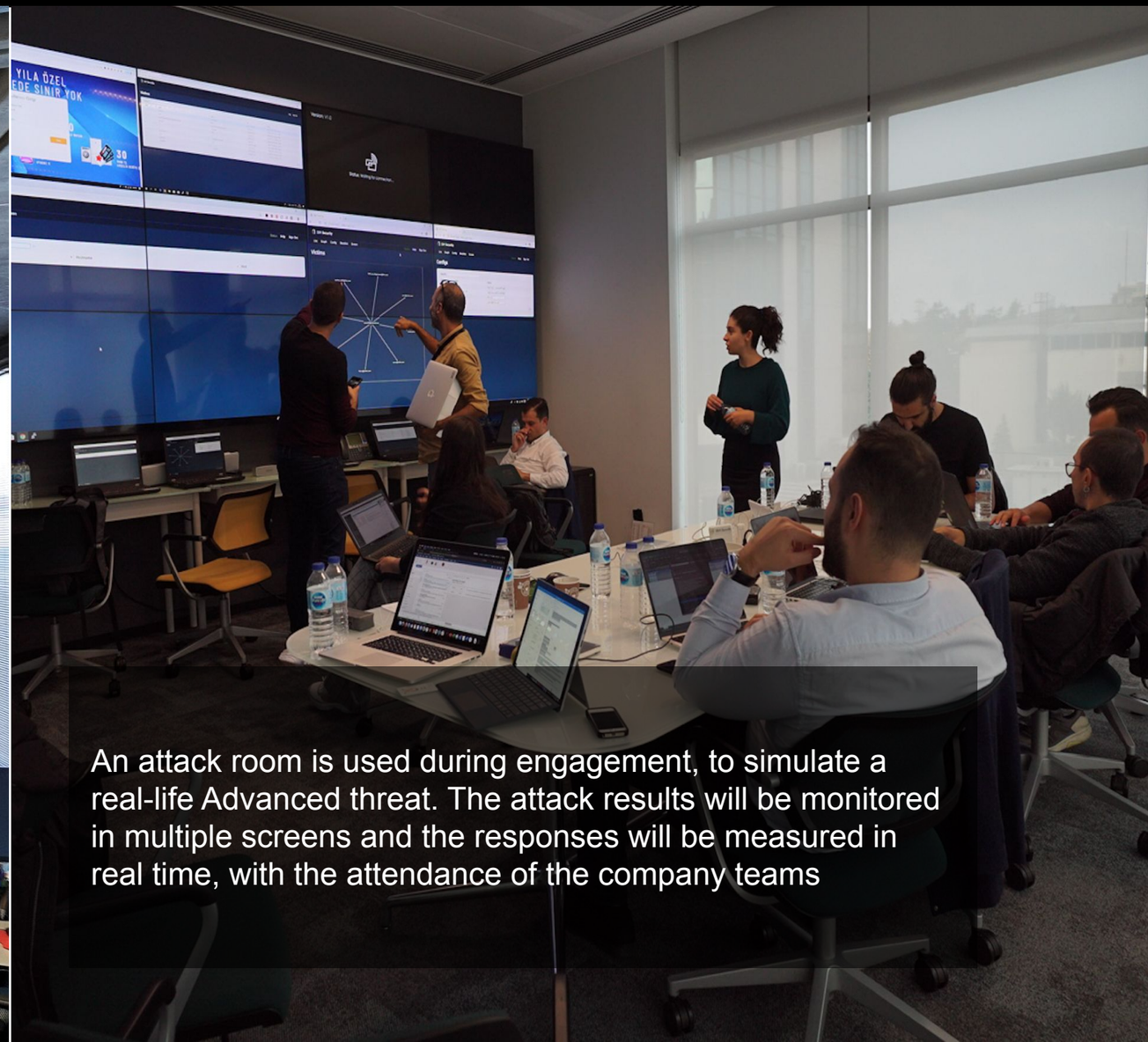
The functions of project must be distributed to expertise

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

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

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

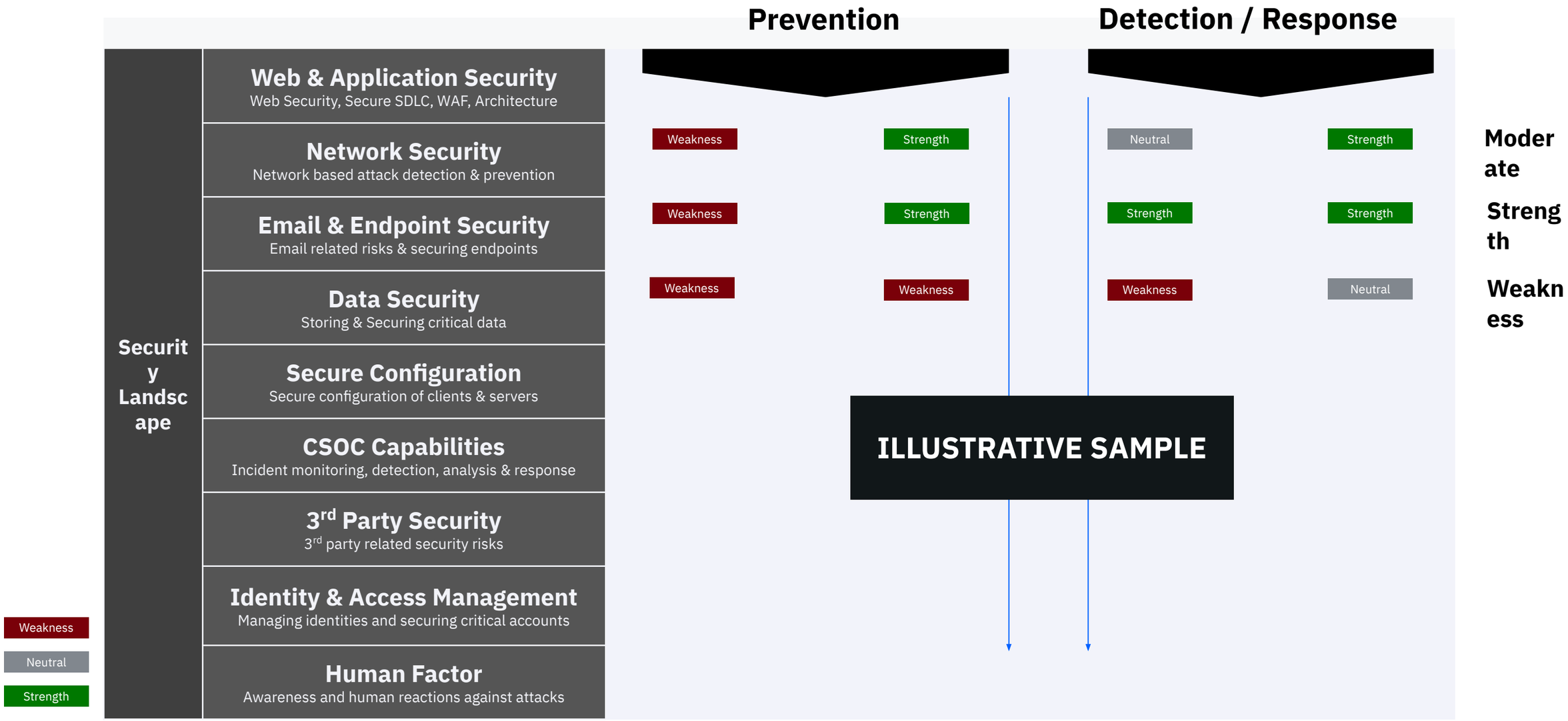
- Analyze how your action was prevented (if)
- Analyze if the environment has related logs
- Analyze if the logs are correlated correctly
- Analyze if the alarms are generated in correct manner
- Analyze if the alarms are handled by SOC teams
- Analyze Playbooks & Response Procedures

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

Security Landscape		Prevention		Detection / Response		
	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 min weaknesses	h visibility on clients and stom 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 s to detect inte 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	olicies have some restriction opportunities om 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 cased 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

YapıKredi Teknoloji
IBM

Reporting all “Good & Bad”

Findings

Finding 1

Detecting CVE-2020-0688 Remote Code Execution Vulnerability

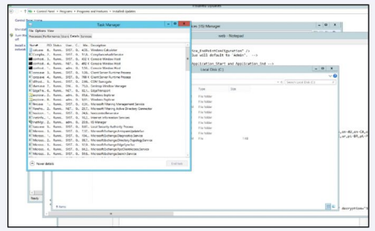
Description

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	➢ Gain Access ➢ Availability Loss



Initiatives

Initiative 3

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

Description

Threat Modelling is an effective way to pinpoint weaknesses in a kill-chain rather than conducting full-scale pentests. It’s result driven and original, adds value not only to technical security but also demonstrates which parts of business might be affected too. It’s considered useful to add threat modelling to the SDLC phases of the development teams both inhouse and 3rd parties.

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.

Risk & Dependency

Threat 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.

Parties Involved

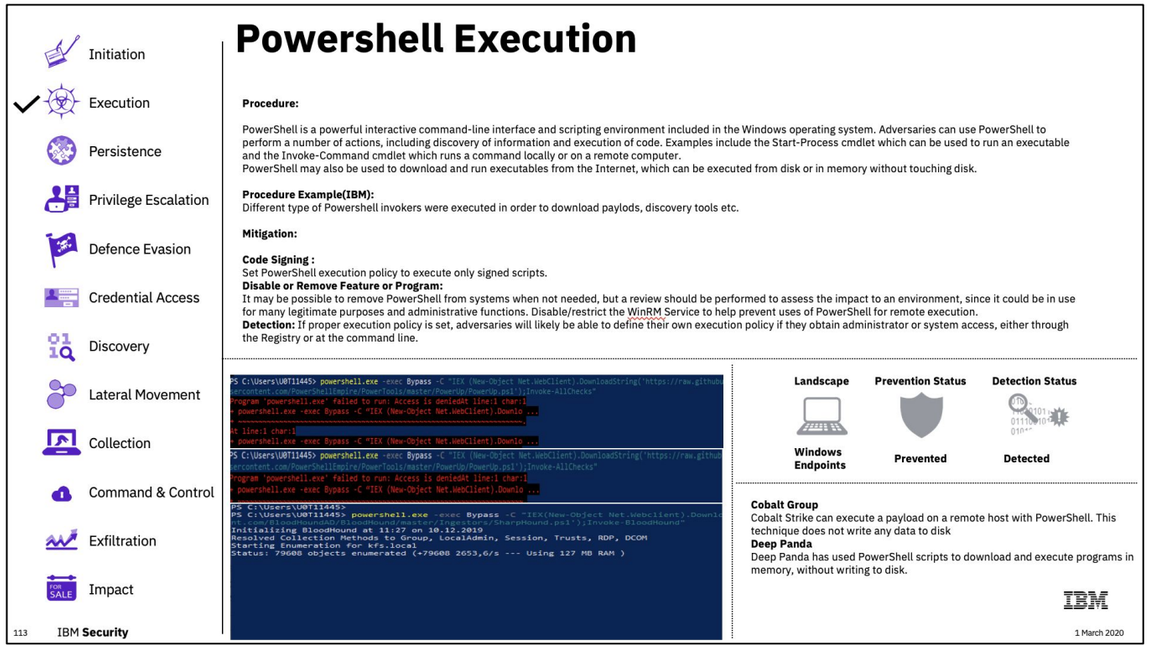
Information Security Teams, SOC Teams, Application Teams, Analyst Teams

Risk Category

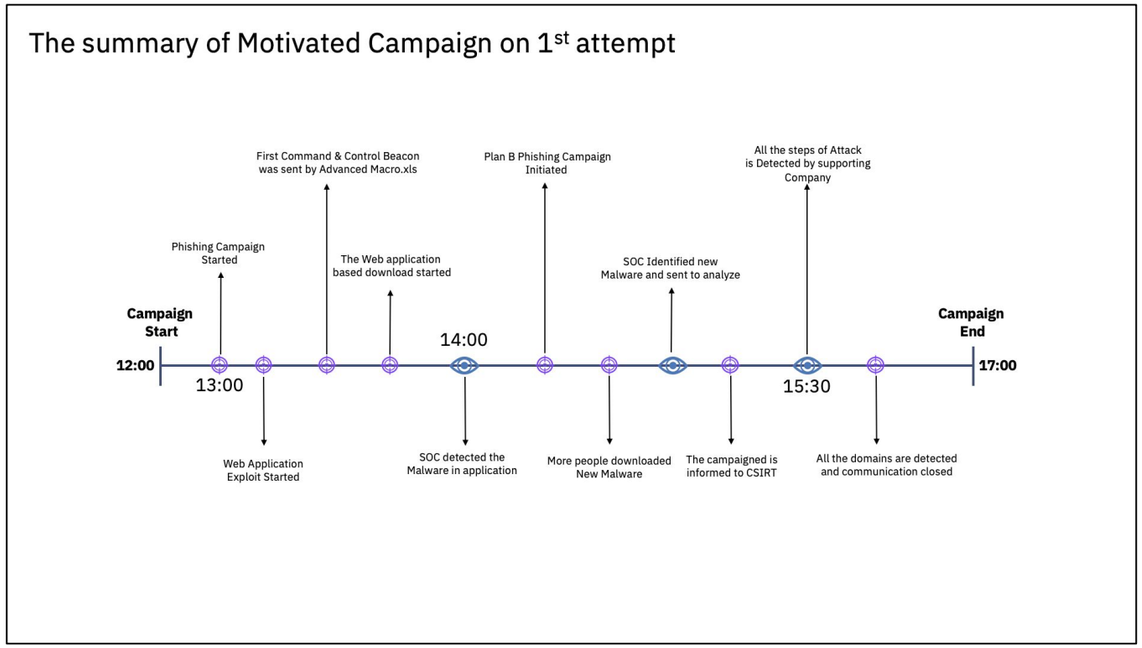
Gain Access , Data Loss, Reputation Loss, Financial Impact, Availability Risks

Reporting all “Good & Bad”

Techniques



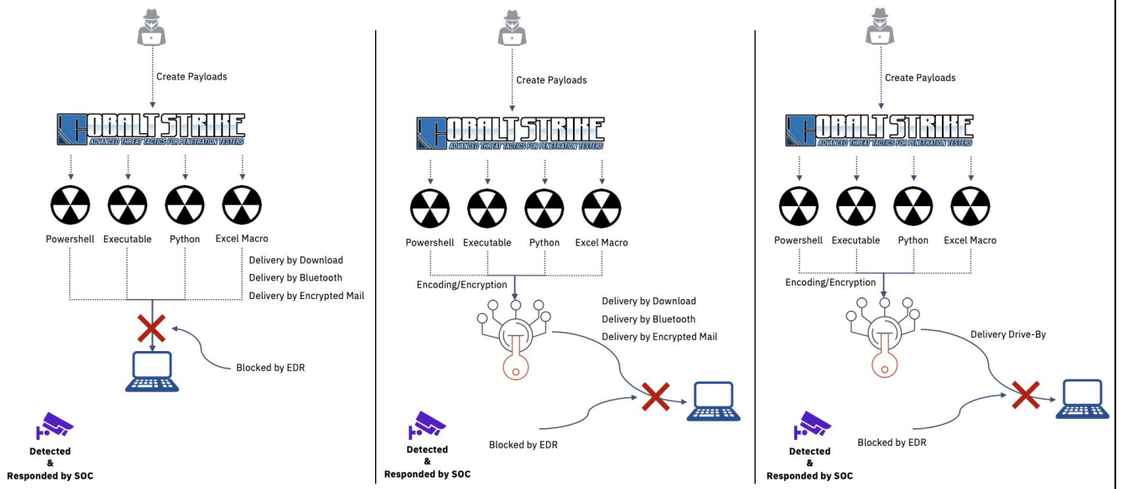
Summary of Campaigns



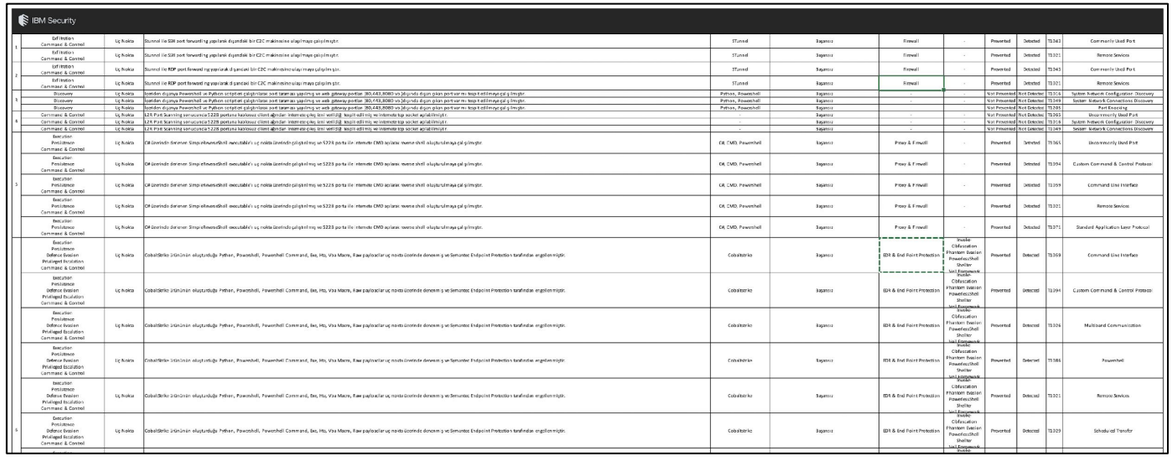
Reporting all “Good & Bad”

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