ATT&CK Community Workshop

ATT&CK and Deception

Agostino Panico

van1sh@protonmail.com

@Van1sh_BSidesIT

Agenda

- Quick intro to cyber deception
- Common deception issues and risks
- Attacker targeting mindset
- Modern deception key points
- Conclusions
- Q&A

Deception Introduction

“Men are so simple of mind, and so much dominated by their **immediate** needs, that a deceitful man will always find plenty who are ready to be **deceived**.”

Niccolò Machiavelli

What’s Cyber Deception

The goal of cyber deception is to more **effectively** detect attacks that have infiltrated an organization’s network, to confuse and **misdirect** the attacker, and to understand what assets have been **compromised**.

What’s Cyber Deception

Common Deception Focus Point:

- Manipulating the **One Thing** that Cyber Attackers Count On;
- Providing **Instant** Gratification;
- Going **Beyond** Common Security Implementation;
- **Simplifying** the implementation and the maintenance.

Cyber Deception Issues

Manipulating the **One Thing** that Cyber Attackers Count On.

– Relies on the common misconception that the attack is not correctly planned, and the **Offensive Cyber Operation** relies only on information gathered from the attack itself.

– Limited application:

- *Script kiddies*;
- *Hacktivist*(??).

Cyber Deception Issues

Providing **Instant** Gratification.

- Let’s focus on the term **Gratification:**

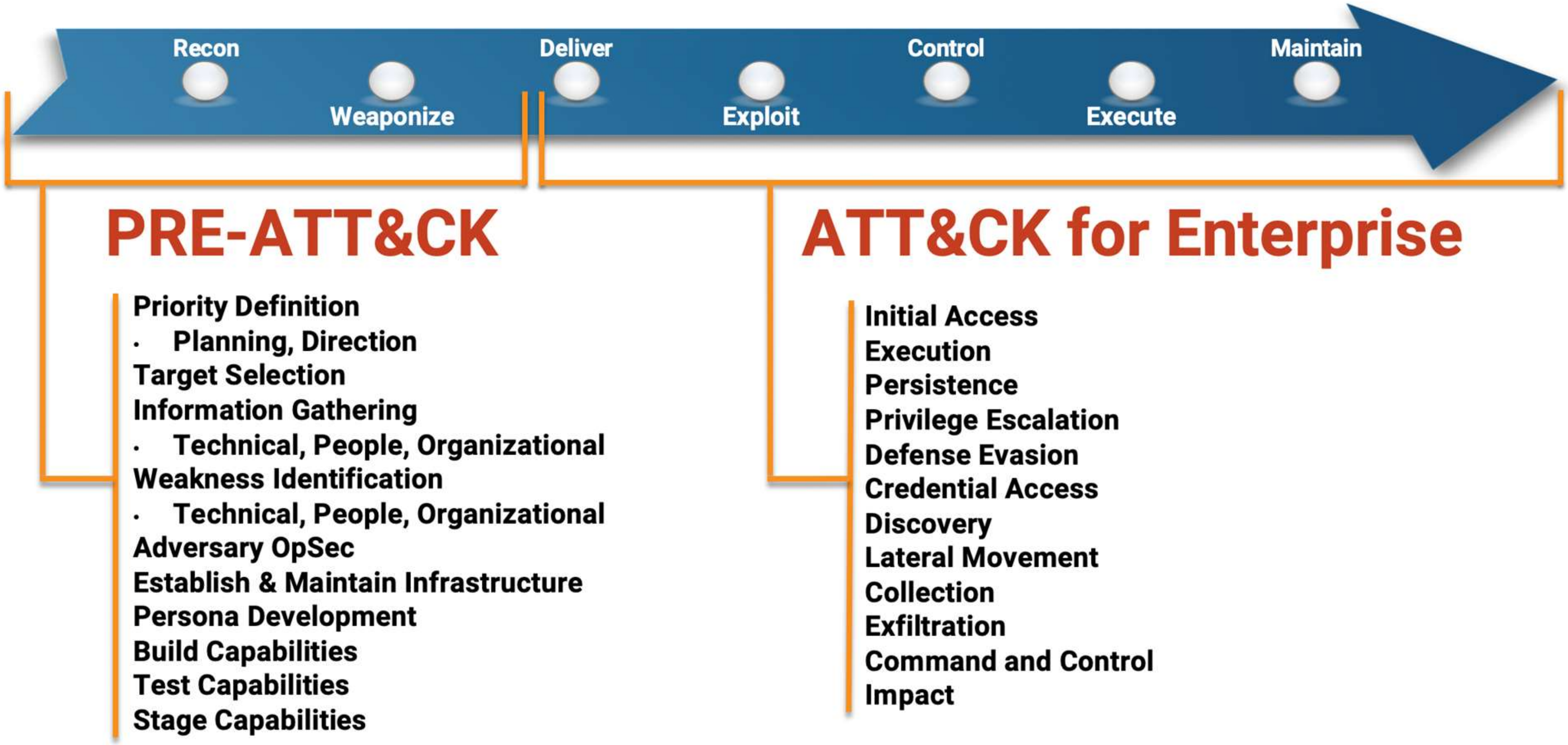
  The definition of gratification is satisfaction or pleasure you feel when you get something you wanted or worked for.

- To correctly evaluate the gratification, we need to know the **target** of a specific **Offensive Cyber Operation**

Advanced Persistent Threat Mindset

- Advanced
  - Logistics, **Planning**, Organization;
- Persistent
  - Focus on the long run goal, and not **immediate** gratification;

MITRE (PRE)-ATT&CK Framework



PRE-ATT&CK

Priority Definition
- Planning, Direction

Target Selection

Information Gathering
- Technical, People, Organizational

Weakness Identification
- Technical, People, Organizational

Adversary OpSec

Establish & Maintain Infrastructure

Persona Development

Build Capabilities

Test Capabilities

Stage Capabilities

ATT&CK for Enterprise

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

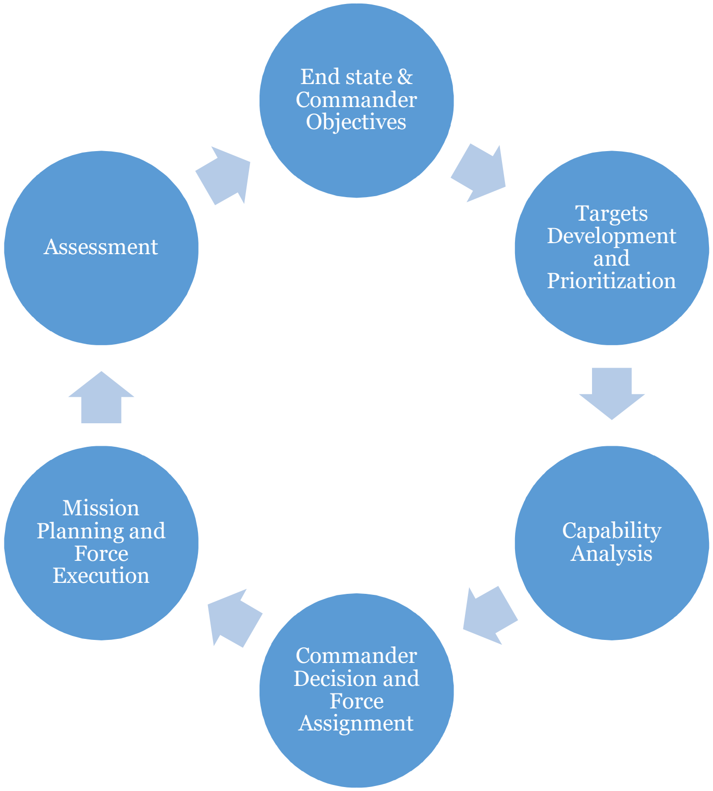
Collection

Exfiltration

Command and Control

Impact

Targeting Cycle


End state & Commander Objectives

Targets Development and Prioritization

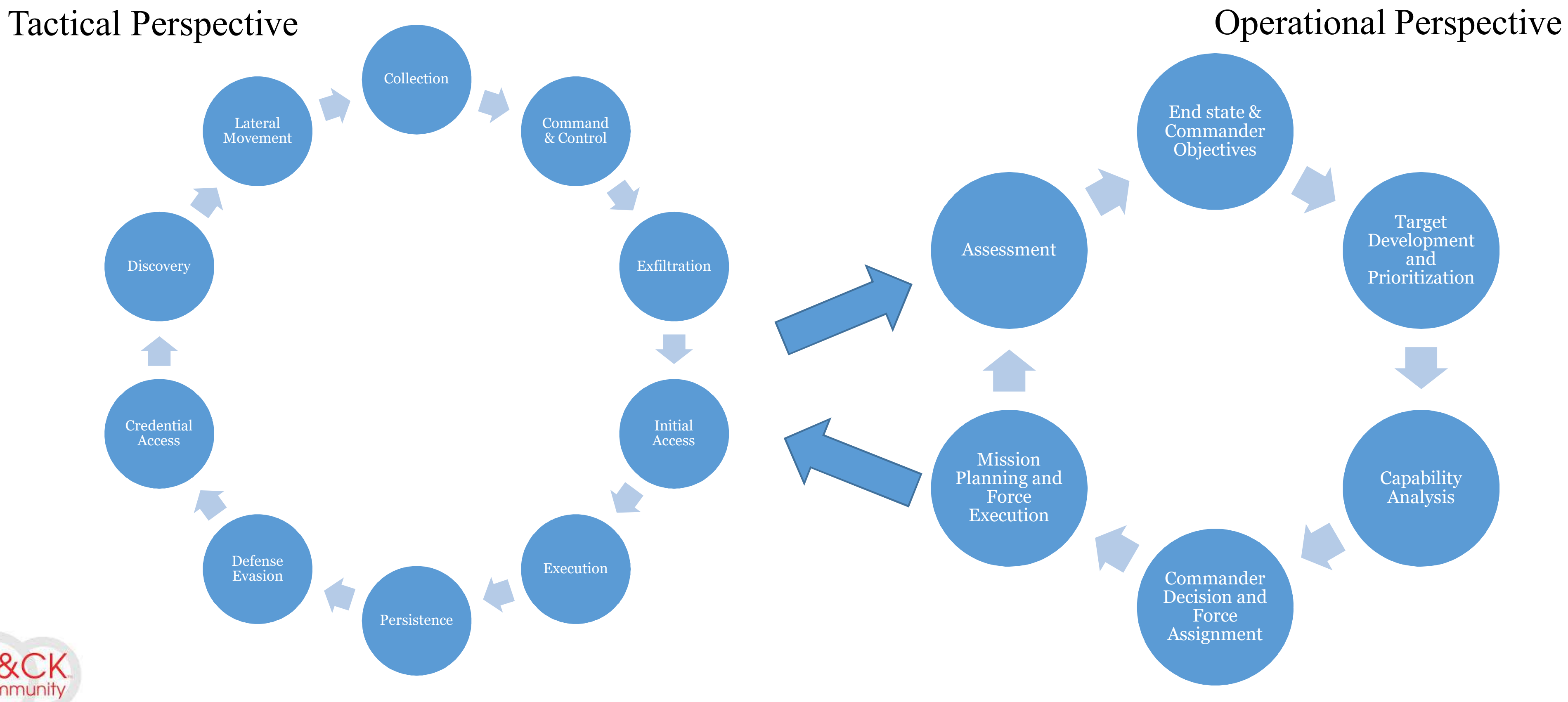
Capability Analysis

Commander Decision and Force Assignment

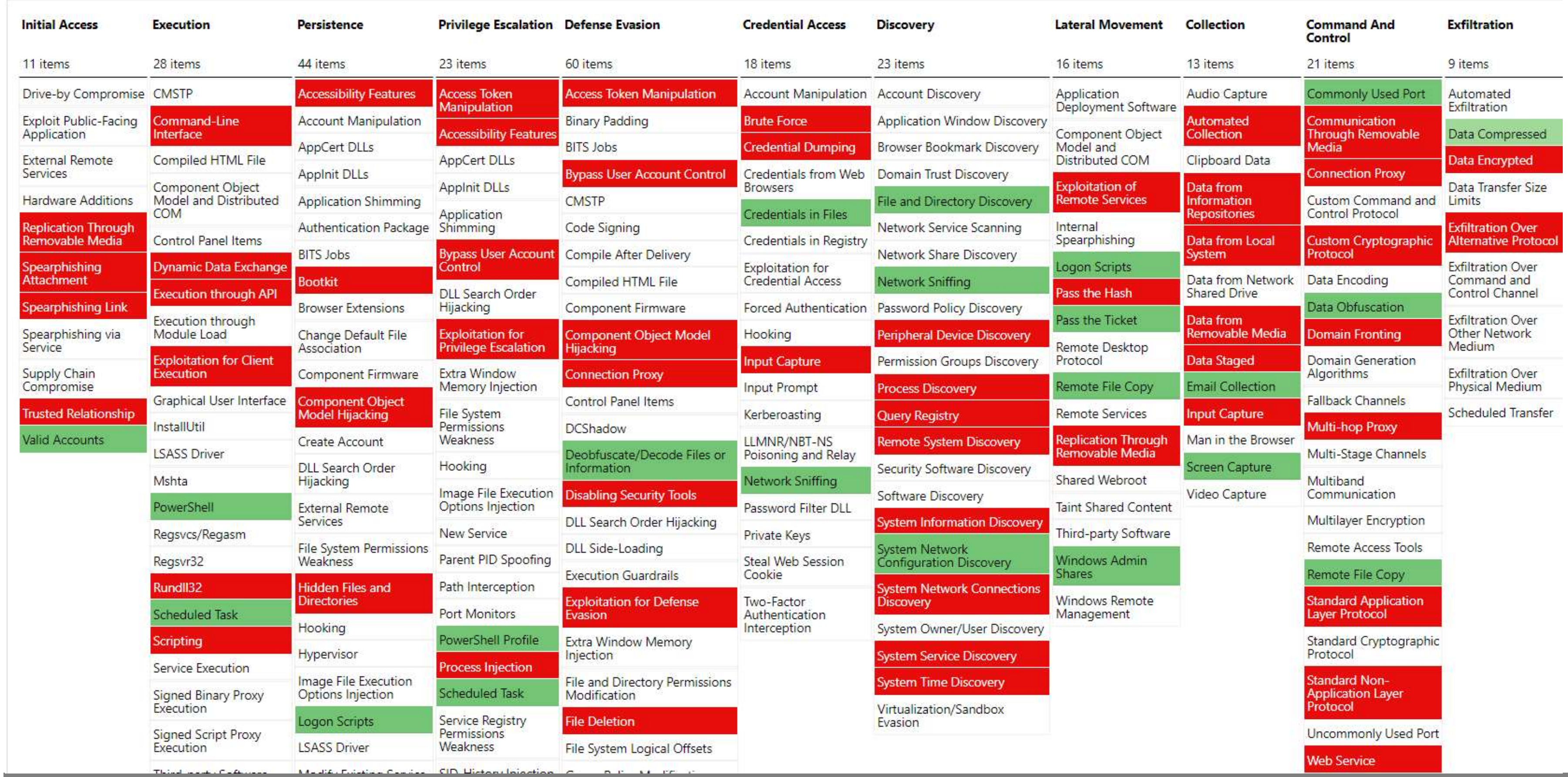
Mission Planning and Force Execution

Assessment

Targeting Cycle with ATT&CK Framework in OODA Loop Style



Threat Model and Deception Path Example



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration
11 items	28 items	44 items	23 items	60 items	18 items	23 items	16 items	13 items	21 items	9 items
Drive-by Compromise	CMSTP	🟥 Accessibility Features	🟥 Access Token Manipulation	🟥 Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	🟩 Commonly Used Port	Automated Exfiltration
Exploit Public-Facing Application	🟥 Command-Line Interface	Account Manipulation	🟥 Accessibility Features	Binary Padding	🟥 Brute Force	Application Window Discovery	Component Object Model and Distributed COM	🟥 Automated Collection	🟥 Communication Through Removable Media	🟩 Data Compressed
External Remote Services	Compiled HTML File	AppCert DLLs	AppCert DLLs	BITS Jobs	🟥 Credential Dumping	Browser Bookmark Discovery	🟥 Exploitation of Remote Services	Clipboard Data	🟥 Connection Proxy	🟥 Data Encrypted
Hardware Additions	Component Object Model and Distributed COM	AppInit DLLs	AppInit DLLs	🟥 Bypass User Account Control	Credentials from Web Browsers	Domain Trust Discovery	Internal Spearphishing	🟥 Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits
🟥 Replication Through Removable Media	Control Panel Items	Application Shimming	Application Shimming	CMSTP	🟩 Credentials in Files	🟩 File and Directory Discovery	🟩 Logon Scripts	🟥 Data from Local System	🟥 Custom Cryptographic Protocol	🟥 Exfiltration Over Alternative Protocol
🟥 Spearphishing Attachment	🟥 Dynamic Data Exchange	Authentication Package	🟥 Bypass User Account Control	Code Signing	Credentials in Registry	Network Service Scanning	🟥 Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel
🟥 Spearphishing Link	🟥 Execution through API	BITS Jobs	DLL Search Order Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Share Discovery	🟩 Pass the Ticket	🟥 Data from Removable Media	🟩 Data Obfuscation	Exfiltration Over Other Network Medium
Spearphishing via Service	Execution through Module Load	🟥 Bootkit	🟥 Exploitation for Privilege Escalation	Compiled HTML File	Forced Authentication	🟩 Network Sniffing	Remote Desktop Protocol	🟥 Data Staged	🟥 Domain Fronting	Exfiltration Over Physical Medium
Supply Chain Compromise	🟥 Exploitation for Client Execution	Browser Extensions	Extra Window Memory Injection	Component Firmware	Hooking	Password Policy Discovery	🟩 Remote File Copy	🟩 Email Collection	Domain Generation Algorithms	Scheduled Transfer
🟥 Trusted Relationship	Graphical User Interface	Change Default File Association	File System Permissions Weakness	🟥 Component Object Model Hijacking	🟥 Input Capture	🟥 Peripheral Device Discovery	Remote Services	🟥 Input Capture	Fallback Channels	
🟩 Valid Accounts	InstallUtil	Component Firmware	Hooking	🟥 Connection Proxy	Input Prompt	Permission Groups Discovery	🟥 Replication Through Removable Media	Man in the Browser	🟥 Multi-hop Proxy	
	LSASS Driver	🟥 Component Object Model Hijacking	Image File Execution Options Injection	Control Panel Items	Kerberoasting	🟥 Process Discovery	Shared Webroot	🟩 Screen Capture	Multi-Stage Channels	
	Mshta	Create Account	New Service	DCShadow	LLMNR/NBT-NS Poisoning and Relay	🟥 Query Registry	Taint Shared Content	Video Capture	Multiband Communication	
	🟩 PowerShell	DLL Search Order Hijacking	Parent PID Spoofing	🟩 Deobfuscate/Decode Files or Information	🟩 Network Sniffing	🟥 Remote System Discovery	Third-party Software		Multilayer Encryption	
	Regsvcs/Regasm	External Remote Services	Path Interception	🟥 Disabling Security Tools	Password Filter DLL	Security Software Discovery	🟩 Windows Admin Shares		Remote Access Tools	
	Regsvr32	File System Permissions Weakness	Port Monitors	DLL Search Order Hijacking	Private Keys	Software Discovery	Windows Remote Management		🟩 Remote File Copy	
	🟥 Rundll32	🟥 Hidden Files and Directories	🟩 PowerShell Profile	DLL Side-Loading	Steal Web Session Cookie	🟥 System Information Discovery			🟥 Standard Application Layer Protocol	
	🟩 Scheduled Task	Hooking	🟥 Process Injection	Execution Guardrails	Two-Factor Authentication Interception	🟩 System Network Configuration Discovery			Standard Cryptographic Protocol	
	🟥 Scripting	Hypervisor	🟩 Scheduled Task	🟥 Exploitation for Defense Evasion		🟥 System Network Connections Discovery			🟥 Standard Non-Application Layer Protocol	
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	Extra Window Memory Injection		System Owner/User Discovery			Uncommonly Used Port	
	Signed Binary Proxy Execution	🟩 Logon Scripts	SID-History Injection	File and Directory Permissions Modification		🟥 System Service Discovery			🟥 Web Service	
	Signed Script Proxy Execution	LSASS Driver		🟥 File Deletion		🟥 System Time Discovery				
	Third-party Software	Modify Existing Service		File System Logical Offsets		Virtualization/Sandbox Evasion				
				Group Policy Modification						

Modern Deception Key Points and Attacker Mindset

- Evaluating **Offensive Cyber Operation** merging **OODA**, **ATT&CK** and **Targeting** we have a clear picture of the key points of a deception system:
  - driving the attacker on a **deceive target**, according to the real target;
  - cannot be general purpose but should be **threat aware;**
  - **integrated** in the production environment, but should represent a preferential path to reach the deceive target;
  - constantly **maintained and updated** to match the threat TTPs and the threat target.

ATT&CK and Deception: Issues and Risks

Deception:

– is based on the **Threat Model**;

– to be effective should be design as **Threat-Aware;**

– relies on common **Security Mechanism**;

– is an extension of the **Attack Surface;**

Conclusion

- **Deception** is a key feature in you arsenal as **Threat Hunter**;
- The **Enterprise Maturity** level should be correctly evaluated, because you need to:
  - **Extend** Attack Surface;
  - **Integrate** in your current Cyber Defense Infrastructure;
  - **Understand** who is the threat you are facing.

Q&A

“Never attempt to win by force what can be won by deception.”

Niccolò Machiavelli

Contact:

email: van1sh@protonmail.com

twitter: @Van1sh_BSidesIT

github: poppopjmp