Halle 10.0
Stand: 216

CYBER DEFENSE MATURITY ASSESSMENT

Cyber Defense gemessen, bewertet, verbessert und endlich wieder ruhig schlafen

Computacenter – Making Digital Work

Dr. Sebastian Schmerl – Solution Manager Cyber Defense

AGENDA

Cyber Defense

-

high level goal

Measure Cyber Defense

-

assess the technical security level

Defense Optimization

-

strategic investments

GENERAL CYBER DEFENSE STRATEGY

DETECTION, REACTION, RESILIENCE

DIGITAL Trust
Mastering business security

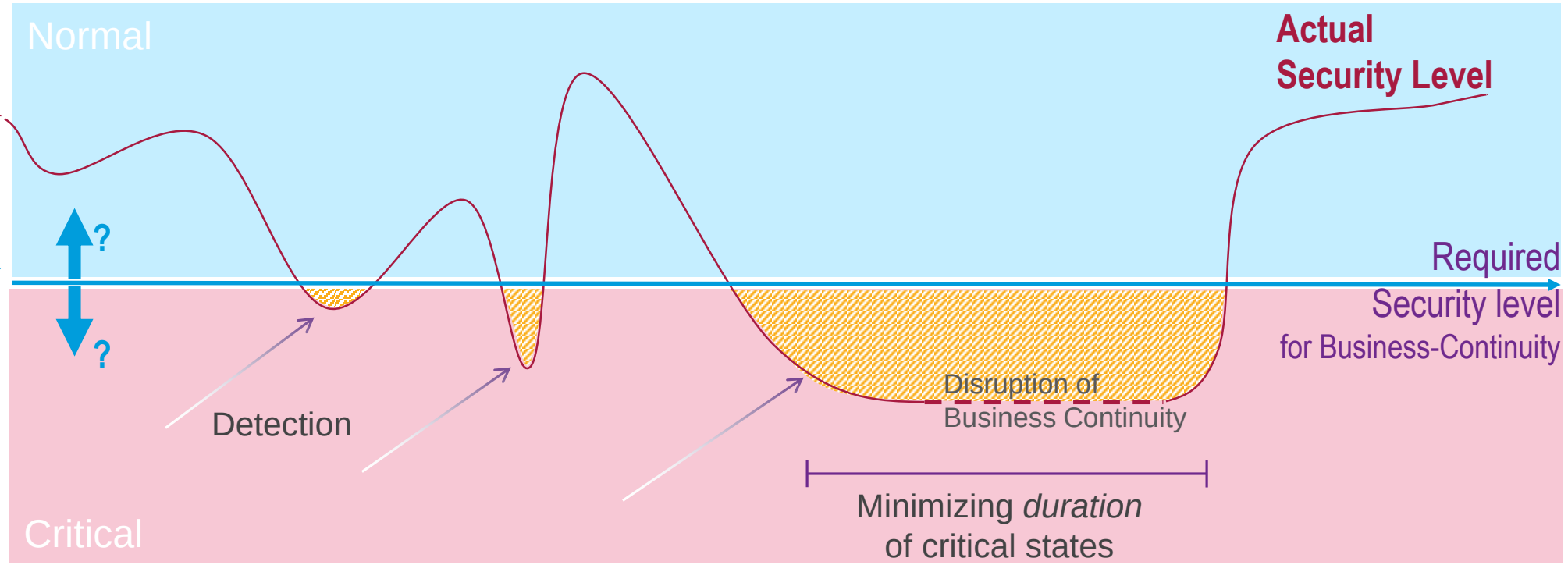
Risk based Protection

Real-time Monitoring & Triage

Incident Management

Situation awareness picture

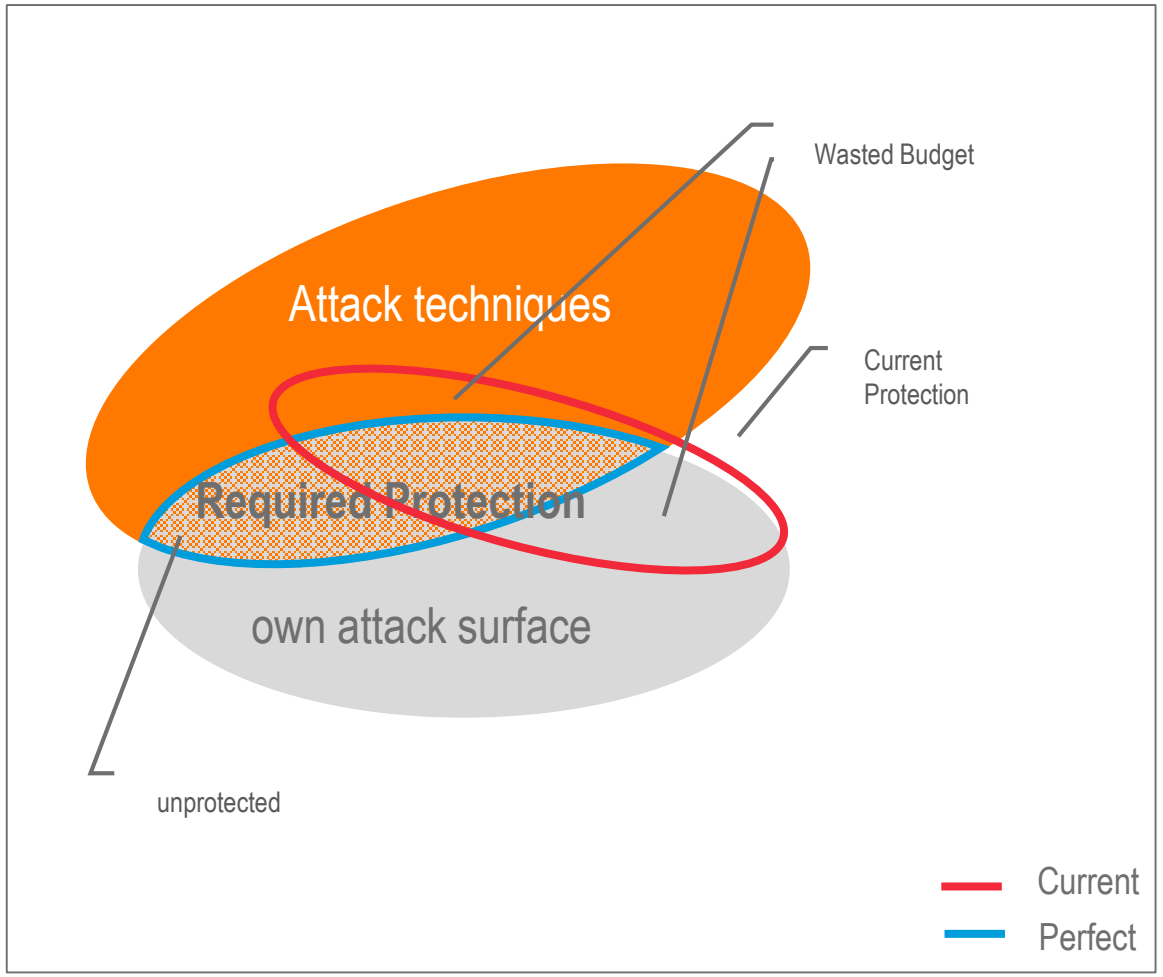
Intelligence



Reducing **amount** of critical states

CYBER DEFENSE MATURITY

ADAPTING SECURITY TO THE REQUIRED SCOPE



- If you know
  - the threats,
  - the attacker,
  - used techniques and
  - the own attack surface.

→ You can adjust the cyber protection perfectly

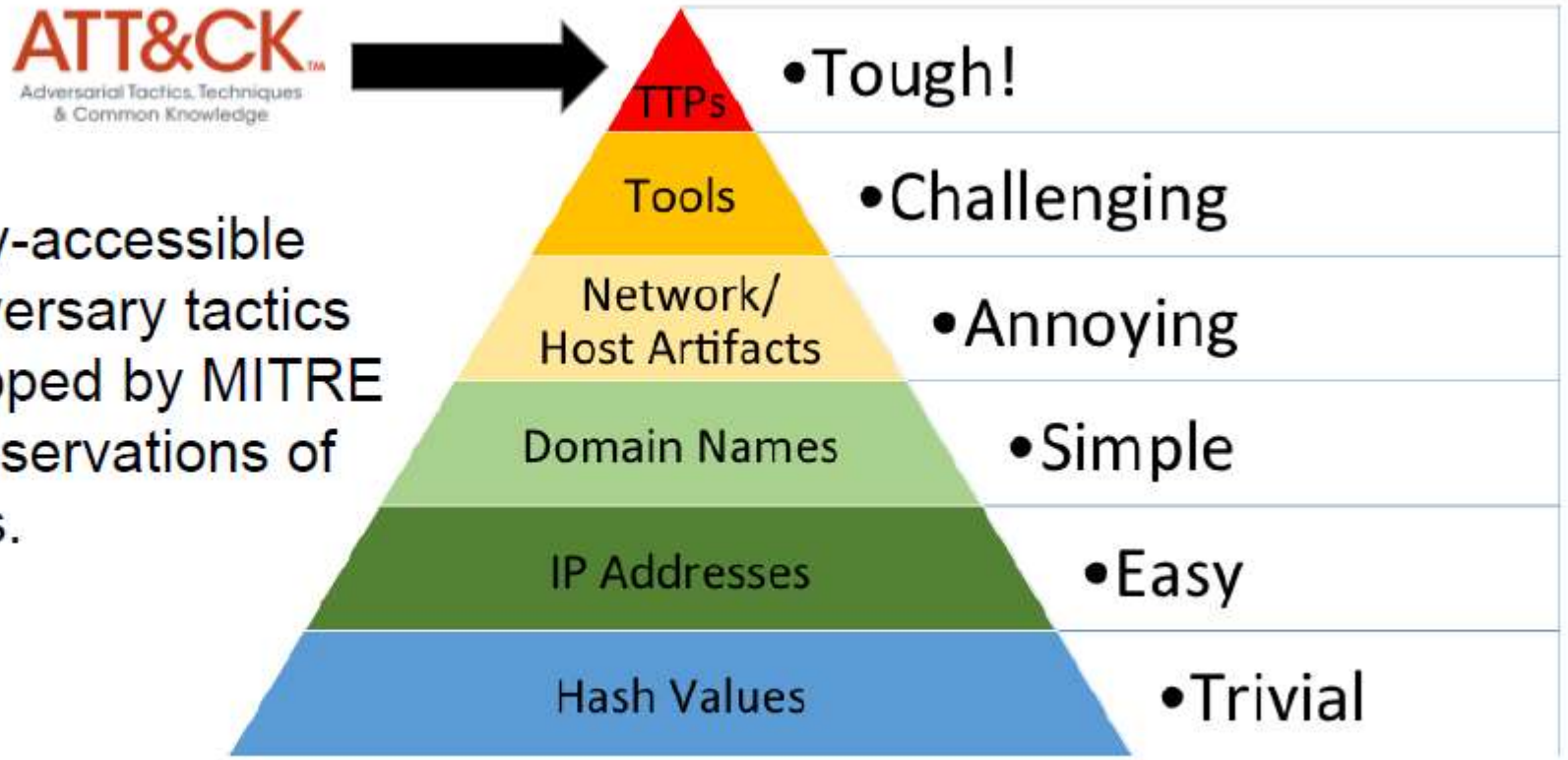
MITRE ATT&CK

OVERVIEW ON ATTACKER TECHNIQUES AND ATTACK PHASES

DIGITAL Trust. Mastering business security

attack.mitre.org

ATT&CK™ is a globally-accessible knowledge base of adversary tactics and techniques, developed by MITRE based on real-world observations of adversaries' operations.



Source: David Bianco

https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

TTPs = Tactics, Techniques, and Procedures

 |

A. Appelbaum: Attack by numbers

ATT&CK FOR ENTERPRISE

DIGITAL Trust. Mastering business security

attack.mitre.org

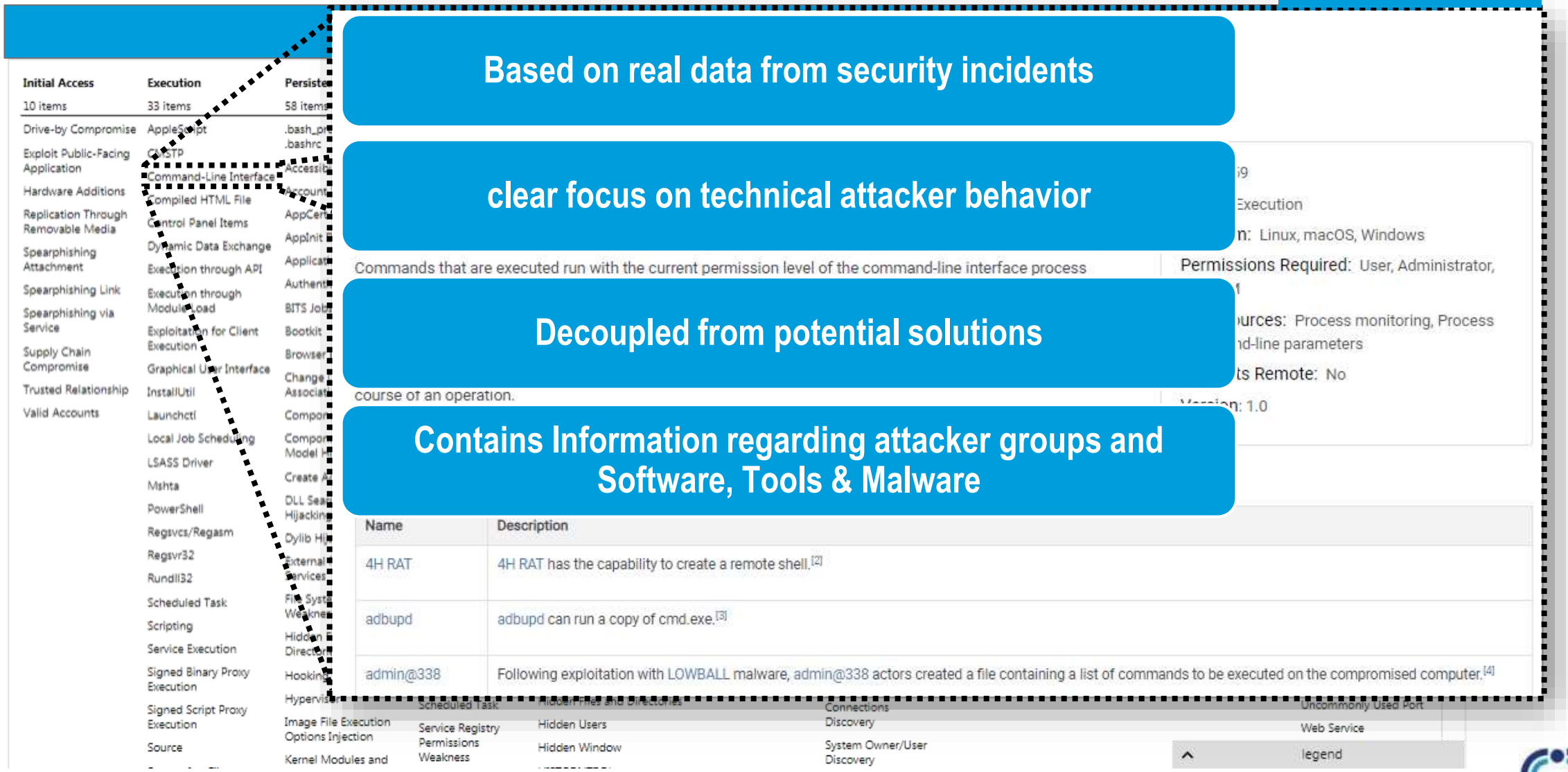
Attacker Techniques – how a goal is achieved

Based on real data from security incidents

clear focus on technical attacker behavior

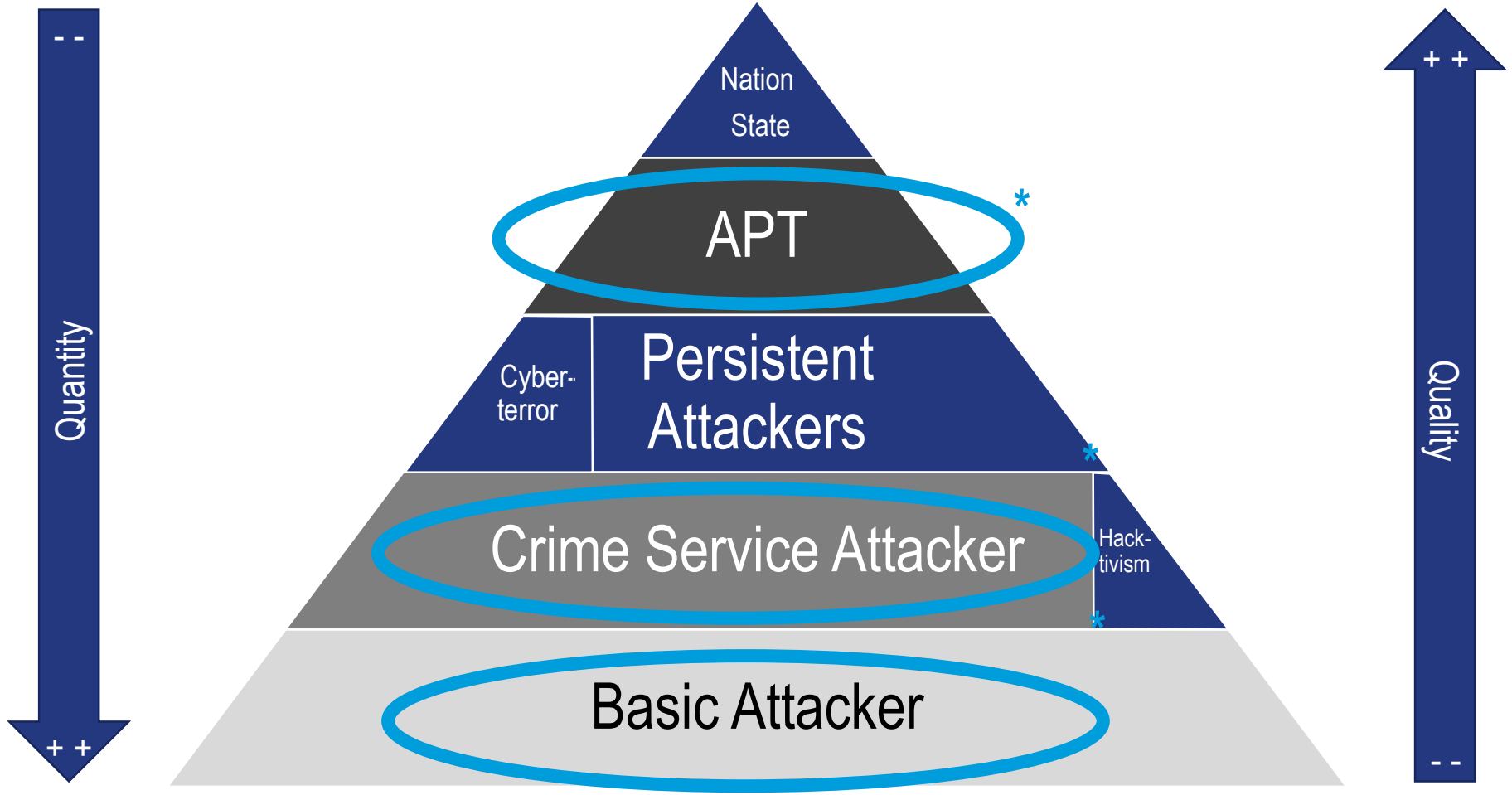
Decoupled from potential solutions

Contains Information regarding attacker groups and Software, Tools & Malware



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

ATTACKER CLASSES



* We tailor attacker classes specific to industry domains

FROM ATTACKER CLASSES TO TECHNIQUES

WHICH ATTACKER CLASS USES WHICH TECHNIQUES

APT

APT Reports

Crime Service Attacker

Techniques used by Exploit-Kits

Techniques used by Loads

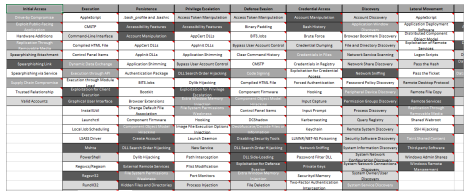
Techniques used by Infostealer

Basic Attacker

Techniques used by Groups

Techniques used by Software

Number of references by technique



Target Scope

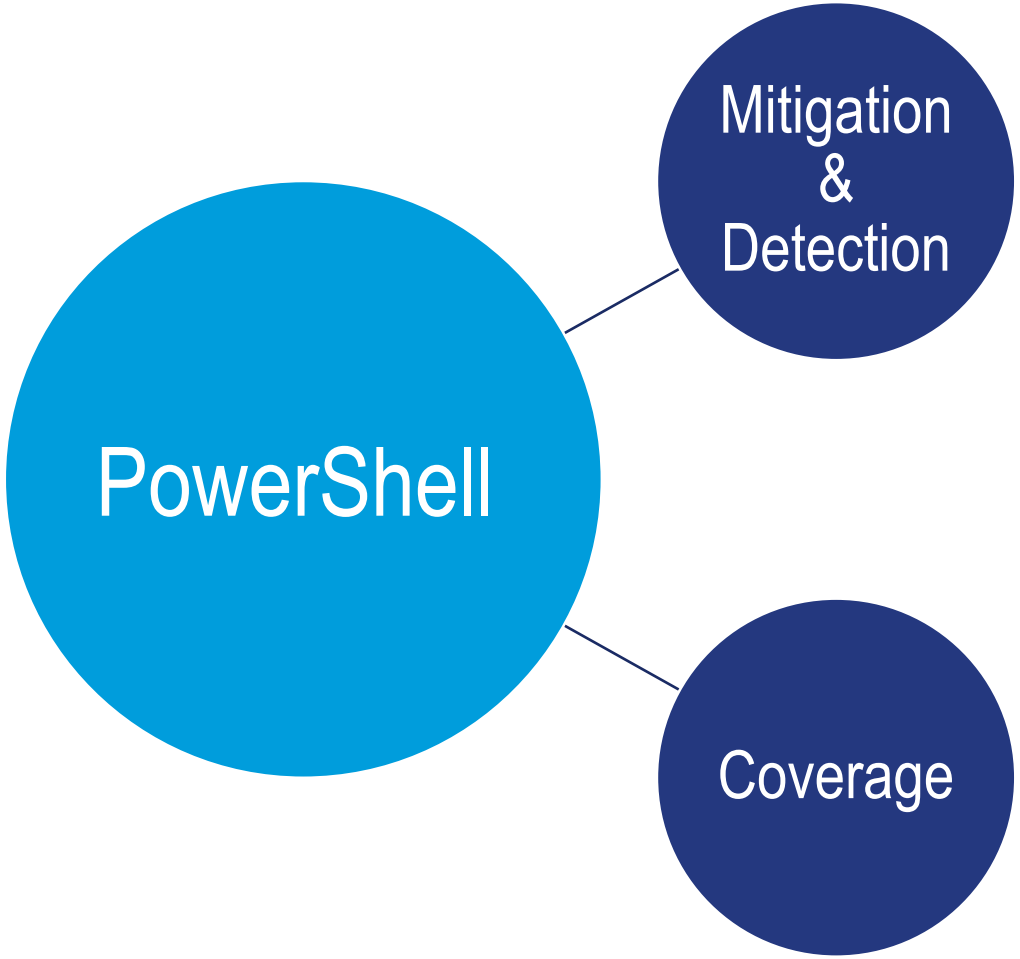
COMBINED VIEW ON ALL ATTACKER CLASSES

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model
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
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	Network Service Scanning	Logon Scripts
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Share Discovery	Pass the Hash
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services
	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items	Input Prompt	Process Discovery	Replication Through Removable Media
	Launchctl	Component Firmware	Hooking	DCShadow	Kerberoasting	Query Registry	Shared Webroot
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	Keychain	Remote System Discovery	SSH Hijacking
	LSASS Driver	Create Account	Launch Daemon	Disabling Security Tools	LLMNR/NBT-NS Poisoning	Security Software Discovery	Taint Shared Content
	Mshta	DLL Search Order Hijacking	New Service	DLL Search Order Hijacking	Network Sniffing	System Information Discovery	Third-party Software
	PowerShell	Dylib Hijacking	Path Interception	DLL Side-Loading	Password Filter DLL	System Network Configuration Discovery	Windows Admin Shares
	Regsvcs/Regasm	External Remote Services	Plist Modification	Exploitation for Defense Evasion	Private Keys	System Network Connections Discovery	Windows Remote
		File System Permissions		Extra Window Memory			

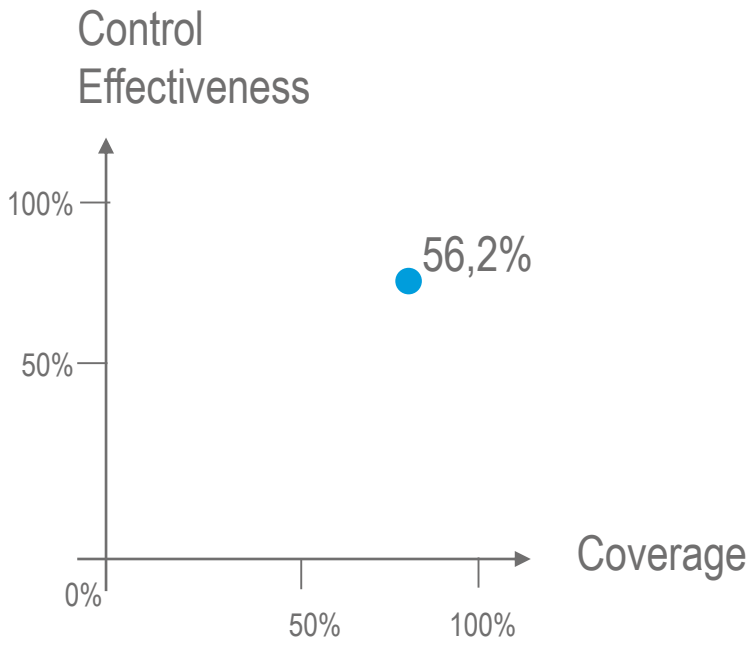
used attack techniques by three different attacker classes
light grey (basic attacker), grey (crime service attacker), dark grey (APT)

ASSESSMENT VIA EFFECTIVENESS & COVERAGE

ONE EXAMPLE - POWERSHELL



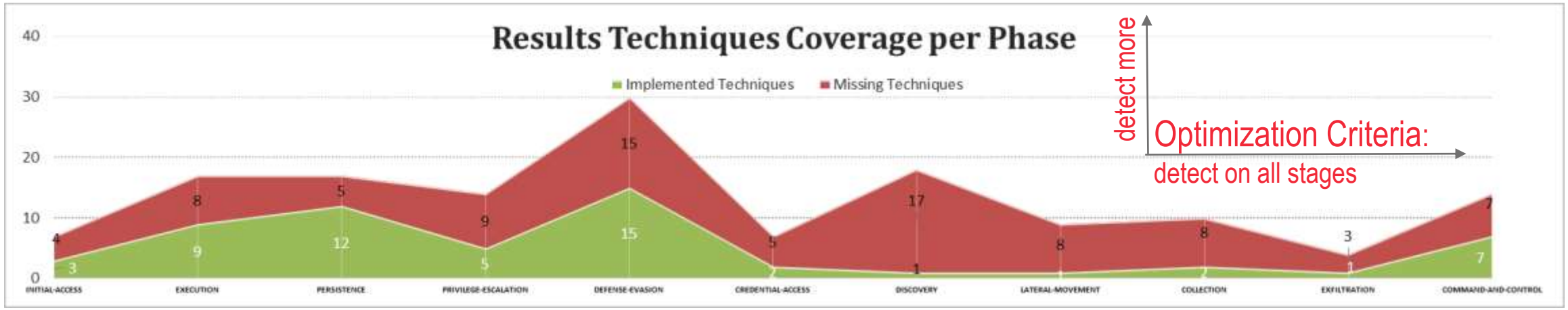
- **Mitigation**
  - least privilege,
  - admin-only,
  - Signed scripts only,
  - pslockdown,
  - constrained-language-mode policies
  - disable WinRM service
- **Detection**
  - Windows Event PowerShell Analysis
  - SIEM-Correlation
- Implementation on
  - Clients
  - Server
  - Cloud Systems
  - VMs
  - ….



 |

RESULTS - CYBER DEFENSE PERFORMANCE

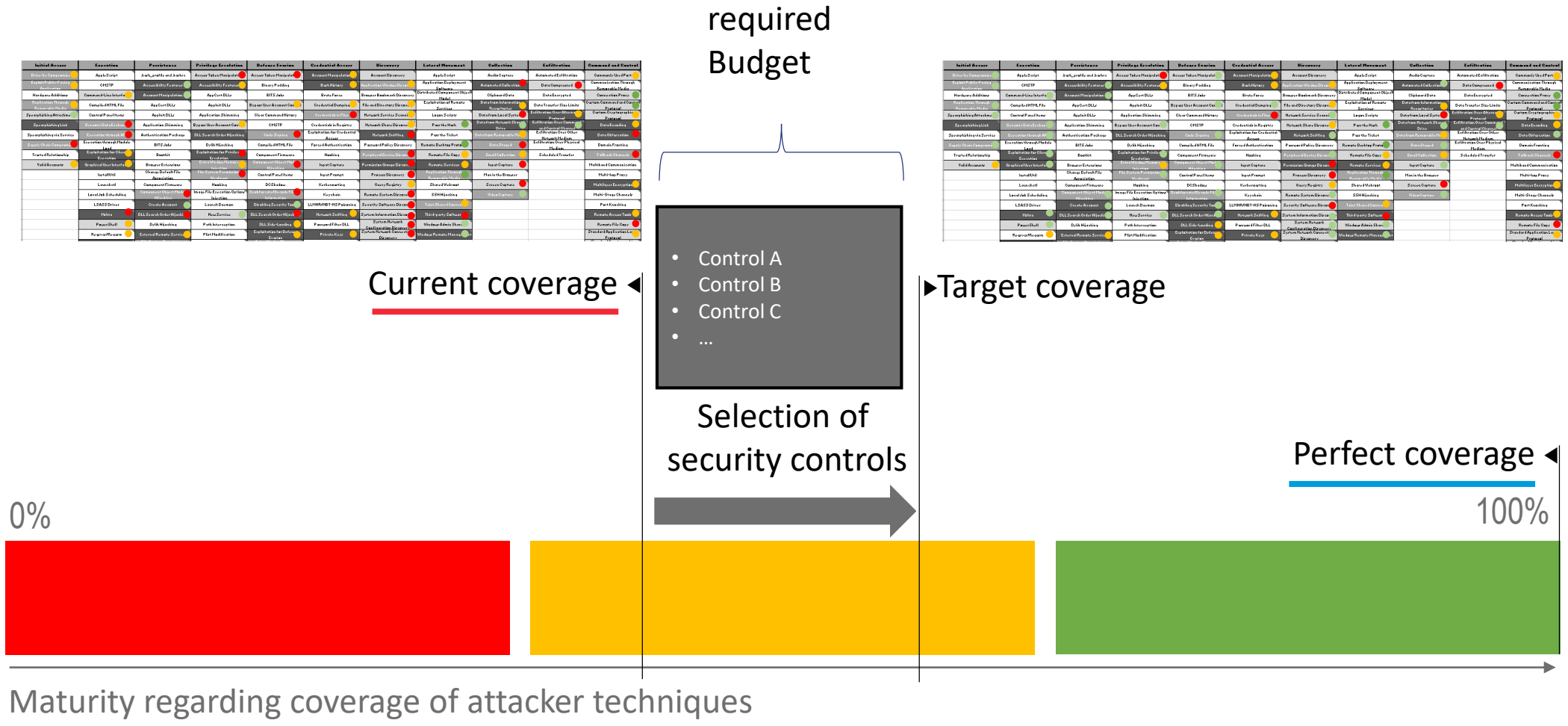
KILL CHAIN & ATT&CK TO MEASURE SUCCESS



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
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		Multiband Communication
	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-hop Proxy
	Launchctl	Component Firmware	Hooking	DCShadow	Kerberoasting	Query Registry	Shared Webroot	Screen Capture		Multilayer Encryption
	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		Multi-Stage Channels
	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

CYBER DEFENSE MATURITY

CYBER DEFENSE OPTIMIZATION



SUMMARY
STRATEGIC INVESTMENTS IN CYBER-SECURITY

Advantages of our Cyber Defense Maturity Assessments:

- It is fast.
- It generates a technical verifiable overview
- It abstracts from many infrastructure details and all the „If‘s und but‘s“
- It allows a technical security control optimization based on techncial facts
- Reality Check can be done by „automatic Red Team Tests“

By purpose, we don't want:

- Consider all awareness, management, process based security matures
- Time consuming collection of the current state

THANK YOU

DIGITAL Trust
Mastering business security

**SECURITY IS NOT LUXURY,
IT IS A NECESSITY.**

**Computacenter
Halle 10.0
Stand: 216**

 |