

Agile use case development with **MITRE ATT&CK**

Bern, 25.10.2022



Speaker



Bruno Blumenthal

Dipl. Ing. FH in Computer Science, CISM, CISA,
CISSP
Managing Security Consultant, Member of the Board
TEMET AG

Main Topics:

- Information Security Management
- Cybersecurity
- Security Architecture and Strategy

Contact:

Mobile: +41 78 859 57 15

E-Mail: bruno.blumenthal@temet.ch


Use case development

The process of

- identifying undesirable behavior or system activities,
- establishing indicators to spot them,
- implementing the technology to detect them,
- and preparing to respond to those detections.

The challenges

- Finding use cases
- Too many use cases
- Not enough resources
- Missing technology
- Changing threat landscape
- Changing technology or business environment
- New risk mitigation requirements



It's about Prioritization and Adaption



It's about
being **agile**



The Agile Manifesto

the use case development version

We value more

Individuals and interactions over processes and tools

Working detections over comprehensive documentation

Many detections over a perfect detection

Responding to change over following a plan



The Five Principles

Our highest priority is to **address real threats** through early and continuous delivery of **effective detections**.

Welcome the changing **threat landscape**. Agile processes harness change for the **organization's advantage over the adversaries**.

Deliver **working detections** frequently, from a couple of weeks to a couple of months, with a preference to the shorter timescale.

Working **detections** are the **primary** measure of progress.

Continuous attention to **technical excellence** and **good design** enhances agility.



If the agile manifesto fits our needs,
tools and methods might as well

Agile methods

- Work with a backlog
- Re-evaluate priorities
- Work on a cadence
- Focus on digestible portions
- Update detection capabilities frequently
- Test and evaluate value constantly



MITRE ATT&CK

ATT&CK Matrix for Enterprise

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 16 techniques	Discovery 30 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (3)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (6)	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Credentials from Password Stores (5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (3)	Browser Extensions	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Services (6)	Browser Session Hijacking	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deploy Container	Forge Web Credentials (2)	Cloud Storage Object Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (5)	Trusted Relationship	Scheduled Task/Job (5)	Create Account (3)	Execution Guardrails (1)	Direct Volume Access	Input Capture (4)	Container and Resource Discovery	Software Deployment Tools	Data from Cloud Storage Object	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)	Valid Accounts (4)	Valid Accounts (4)	Shared Modules	Create or Modify System Process (4)	Escape to Host	Domain Policy Modification (2)	Modify Authentication Process (5)	Debugger Evasion	Taint Shared Content	Data from Configuration Repository (2)	Ingress Tool Transfer	Exfiltration Over Web Service (2)	Firmware Corruption
Search Open Websites/Domains (2)			Software Deployment Tools	Event Triggered Execution (15)	Event Triggered Execution (15)	Exploitation for Defense Evasion	Multi-Factor Authentication Interception	Domain Trust Discovery	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Multi-Stage Channels	Scheduled Transfer	Inhibit System Recovery
Search Victim-Owned Websites			System Services (2)	External Remote Services	Exploitation for Privilege Escalation	File and Directory Permissions Modification (2)	Multi-Factor Authentication Request Generation	File and Directory Discovery	Group Policy Discovery	Data from Local System	Non-Application Layer Protocol	Transfer Data to Cloud Account	Resource Hijacking
			User Execution (3)	Hijack Execution Flow (12)	Hijack Execution Flow (12)	Hide Artifacts (10)	Network Sniffing	Group Policy Discovery	Network Service Discovery	Data from Network Shared Drive	Non-Standard Port		Service Stop
			Windows Management Instrumentation	Implant Internal Image	Process Injection (12)	Hijack Execution Flow (12)	OS Credential Dumping (8)	Network Share Discovery	Network Sniffing	Data from Removable Media	Protocol Tunneling		System Shutdown/Reboot
				Modify Authentication Process (5)	Scheduled Task/Job (5)	Impair Defenses (9)	Steal Application Access Token	Network Sniffing	Password Policy Discovery	Data from Removable Media	Proxy (4)		
				Indicator Removal on Host (6)	Valid Accounts (4)	Indicator Removal on Host (6)	Steal or Forge Kerberos Tickets (4)	OS Credential Dumping (8)	Peripheral Device Discovery	Data Staged (2)	Remote Access Software		
				Indirect Command Execution		Masquerading (7)	Steal Web Session Cookie	Steal Application Access Token	Permission Groups Discovery (3)	Email Collection (3)	Traffic Signaling (1)		
				Pre-OS Boot (5)		Modify Authentication Process (5)	Unsecured Credentials (7)	Steal or Forge Kerberos Tickets (4)	Process Discovery	Input Capture (4)	Web Service (3)		
				Scheduled Task/Job (5)		Modify Cloud Compute Infrastructure (4)	Modify Registry	Unsecured Credentials (7)	Query Registry	Screen Capture			
				Server Software Component (5)		Modify System Image (2)	Network Boundary Bridging (1)	System Information Discovery	Remote System Discovery	Video Capture			
				Traffic Signaling (1)		Obfuscated Files or	Obfuscated Files or	System Location Discovery (1)	System Network Configuration Discovery (1)				
				Valid Accounts (4)				System Network Configuration Discovery (1)					

More than Tactics and Techniques

- 14 Tactics
- 191 Techniques
 - 385 Sub-techniques
- 133 Groups
- 680 Software
- 43 Mitigations
- 39 Data Sources

Prioritize use cases with ATT&CK

- Filter and rank techniques
- Assess the inherent value
- Consider time criticality
- Evaluate implementation complexity
- Score use cases relative to each other

Filter and rank techniques

- Filter for applicability
 - Based on your environment and platforms in use
- Remove preventable techniques
 - Use the mitigation information from ATT&CK
- Count # of group using the technique
 - You may also filter for relevant groups

Assess the value

- Rank of addressed techniques
- Position of tactic in the matrix
- Coverage of your environment
 - Exposure of covered systems

Consider time criticality

- Does it mitigate a known vulnerability?
- Do we have specific threat intel
 - Running campaign
 - Relevant incidents
 - Other indicators

Evaluate implementation complexity

- Existence of needed data sources
- Specific tooling
- Distinguishability
 - Definable IoCs
 - # of Expected false positives

Bring it all together

Again borrowing from agile software development methods we calculate:

$$Priority = \frac{Value + TimeCriticality}{Complexity}$$

This is an adaption of WSJF (Weighted Shortest Job First)

Where we do not need absolute numbers, but relative weights between the use cases to prioritize

Conclusion

- The world changes constantly
- We need to be agile
- Agile means prioritize and adapt
- ATT&CK provides information to assess use case value
- Consider value and complexity
- Focus on deliver value early and often

Questions?



Thank you