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.

TEMET
end-to-end IT security

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

TEMET
end-to-end IT security

It's about
Prioritization and Adaption

It's about
being **agile**

TEMET
end-to-end IT security

The Agile Manifesto

the use case development version

TEMET
end-to-end IT security

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

TEMET
end-to-end IT security

The Five Principles

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

TEMET
end-to-end IT security

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.

TEMET
end-to-end IT security

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

TEMET
end-to-end IT security

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

TEMET
end-to-end IT security

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

TEMET
end-to-end IT security

MITRE ATT&CK

ATT&CK Matrix for Enterprise

Reconnaissance — 10 techniques
- Active Scanning (3)
- Gather Victim Host Information (4)
- Gather Victim Identity Information (3)
- Gather Victim Network Information (6)
- Gather Victim Org Information (4)
- Phishing for Information (3)
- Search Closed Sources (2)
- Search Open Technical Databases (5)
- Search Open Websites/Domains (2)
- Search Victim-Owned Websites

Resource Development — 7 techniques
- Acquire Infrastructure (6)
- Compromise Accounts (2)
- Compromise Infrastructure (6)
- Develop Capabilities (4)
- Establish Accounts (2)
- Obtain Capabilities (6)
- Stage Capabilities (5)

Initial Access — 9 techniques
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (3)
- Replication Through Removable Media
- Supply Chain Compromise (3)
- Trusted Relationship
- Valid Accounts (4)

Execution — 12 techniques
- Command and Scripting Interpreter (8)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (3)
- Native API
- Scheduled Task/Job (5)
- Shared Modules
- Software Deployment Tools
- System Services (2)
- User Execution (3)
- Windows Management Instrumentation

Persistence — 19 techniques
- Account Manipulation (5)
- BITS Jobs
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (3)
- Create or Modify System Process (4)
- Event Triggered Execution (15)
- External Remote Services
- Hijack Execution Flow (12)
- Implant Internal Image
- Modify Authentication Process (5)
- Office Application Startup (6)
- Pre-OS Boot (5)
- Scheduled Task/Job (5)
- Server Software Component (5)
- Traffic Signaling (1)
- Valid Accounts (4)

Privilege Escalation — 13 techniques
- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Create or Modify System Process (4)
- Domain Policy Modification (2)
- Escape to Host
- Event Triggered Execution (15)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (12)
- Process Injection (12)
- Scheduled Task/Job (5)
- Valid Accounts (4)

Defense Evasion — 42 techniques
- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (2)
- Execution Guardrails (1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (2)
- Hide Artifacts (10)
- Hijack Execution Flow (12)
- Impair Defenses (9)
- Indicator Removal on Host (6)
- Indirect Command Execution
- Masquerading (7)
- Modify Authentication Process (5)
- Modify Cloud Compute Infrastructure (4)
- Modify Registry
- Modify System Image (2)
- Network Boundary Bridging (1)
- Obfuscated Files or Information …

Credential Access — 16 techniques
- Adversary-in-the-Middle (3)
- Brute Force (4)
- Credentials from Password Stores (5)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (2)
- Input Capture (4)
- Modify Authentication Process (5)
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- Network Sniffing
- OS Credential Dumping (8)
- Steal Application Access Token
- Steal or Forge Kerberos Tickets (4)
- Steal Web Session Cookie
- Unsecured Credentials (7)

Discovery — 30 techniques
- Account Discovery (4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (1)
- System Information Discovery
- System Location Discovery (1)
- System Network Configuration Discovery (1)

Lateral Movement — 9 techniques
- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (2)
- Remote Services (6)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (4)

Collection — 17 techniques
- Adversary-in-the-Middle (3)
- Archive Collected Data (3)
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage Object
- Data from Configuration Repository (2)
- Data from Information Repositories (3)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (2)
- Email Collection (3)
- Input Capture (4)
- Screen Capture
- Video Capture

Command and Control — 16 techniques
- Application Layer Protocol (4)
- Communication Through Removable Media
- Data Encoding (2)
- Data Obfuscation (3)
- Dynamic Resolution (3)
- Encrypted Channel (2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (4)
- Remote Access Software
- Traffic Signaling (1)
- Web Service (3)

Exfiltration — 9 techniques
- Automated Exfiltration (1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (1)
- Exfiltration Over Physical Medium (1)
- Exfiltration Over Web Service (2)
- Scheduled Transfer
- Transfer Data to Cloud Account

Impact — 13 techniques
- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation (3)
- Defacement (2)
- Disk Wipe (2)
- Endpoint Denial of Service (4)
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service (2)
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

TEMET
end-to-end IT security

More than Tactics and Techniques

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

TEMET
end-to-end IT security

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

TEMET
end-to-end IT security

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

TEMET
end-to-end IT security

Assess the value

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

TEMET
end-to-end IT security

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

TEMET
end-to-end IT security

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

TEMET
end-to-end IT security

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

TEMET
end-to-end IT security

Questions?

Thank you