MUNI
FI

Cyber Threat Management

PA211 Advanced Topics of Cyber Security

October 4, 2022

Lukáš Sadlek, Jan Vykopal, and Pavel Čeleda

Exit tickets from last week – I

- **Q:** What is this “measure” part of vulnerability management lifecycle in example Tenable?
- **A:** *It measures the **success** of lifecycle, e.g., using **risk** computed from*
  - ***threats** caused by vulnerabilities,*
  - *probability of **vulnerability exploit,***
  - ***asset** criticality,*
  - *possible **impact.***

  *It allows tracking and **comparing risk** (between business units and organizations) and making **strategic decisions**.*

Exit tickets from last week – II

- **Q:** What exactly is QoD ?
- **A:** *It is the **reliability** of the vulnerability detection method. For example, the **exploit** has 100% QoD, and **remote banner** containing the patch level has 80% QoD. See [1].*

- **Q:** As for the generating PDF reports, Is there any way to customize content of the report?
- **A:** *Yes, see [2]. You can specify, e.g., that you want only **HIGH severity** vulnerabilities or **QoD** >= 90%.*

Exit tickets from last week – III

- **Q:** What is the best SW/way how to check vulnerabilities in our computer? SW that we used today seemed not working 100% and too heavy for local computers.
- **A:** *I would perform some **stress tests** on the computer or use utilities that check **system health**. We used a network vulnerability scanner, which reveals a **different type** of vulnerabilities.*

Exit tickets from last week – IV

Greenbone's management daemon was constantly crashing, which prevented me from finishing some tasks.

A: *Environments consisting of docker containers showed to be very* ***fragile****. It is not possible to* ***manually*** *test every computer when shortly after* `vagrant up` *everything seems OK.*

We ask you to change seats today to test whether the problems are associated with particular machines in this room.

Goals of this lecture

- Become **acquainted** with:
  - **cyber threat intelligence** and related terminology,
  - cyber **threat hunting**,
  - cyber threat intelligence **sharing** and threat **intelligence platforms**,
  - standards, **knowledge bases**, and **data sources**.

Essential terminology

Cyber threat

- **Circumstance or event with** the potential adversarial **impact**
- Impacts **operations**, **assets**, individuals, or organizations
- **Threat actor** – a **source** of malicious activity
- **Examples:**
  - SQL injection
  - Denial of service
  - Elevation of privileges
  - Unauthorized access
  - Disclosure or modification of information

Cyber threat management

- A process that **manages** cyber threats
- It **detects** threats and **prevents** attacks
  - Uses **different data** sources that provide **evidence**
  - **Internal data** – packets, logs, IP flows, scans
  - **External data** – cyber threat intelligence, knowledge bases, databases
- Requires to discover **vulnerabilities** and **vulnerable assets**
  - Coupled with **vulnerability** and **asset** managements

Cyber threat intelligence

Cyber threat intelligence

- **Evidence-based knowledge** about an existing hazard to assets
- **Common content**
  - Context
  - Mechanisms
  - Indicators
  - Implications for the decision regarding the response

Cyber threat intelligence sources

- **Open-source** intelligence
  - **Example:** threat intelligence platforms
- Device **log files**
- Network **traffic**
- **Human intelligence** from incident resolution
  - Alerts
  - Warnings
  - Security advisories

Indicators of Compromise (IoCs)

- Piece of information that objectively **describes an intrusion**
- **Atomic**
  - **Cannot be broken** down into smaller parts
  - **Examples**: IP addresses, email addresses, and vulnerability identifiers
- **Computed**
  - **Derived** from data involved in an incident
  - **Examples**: file hash values and regular expressions
- **Behavioral**
  - **Collection of** computed and atomic **indicators,** which is often quantified
  - **Examples**: unusual outbound network traffic and user activity anomalies

Tactics, Techniques, and Procedures (TTPs)

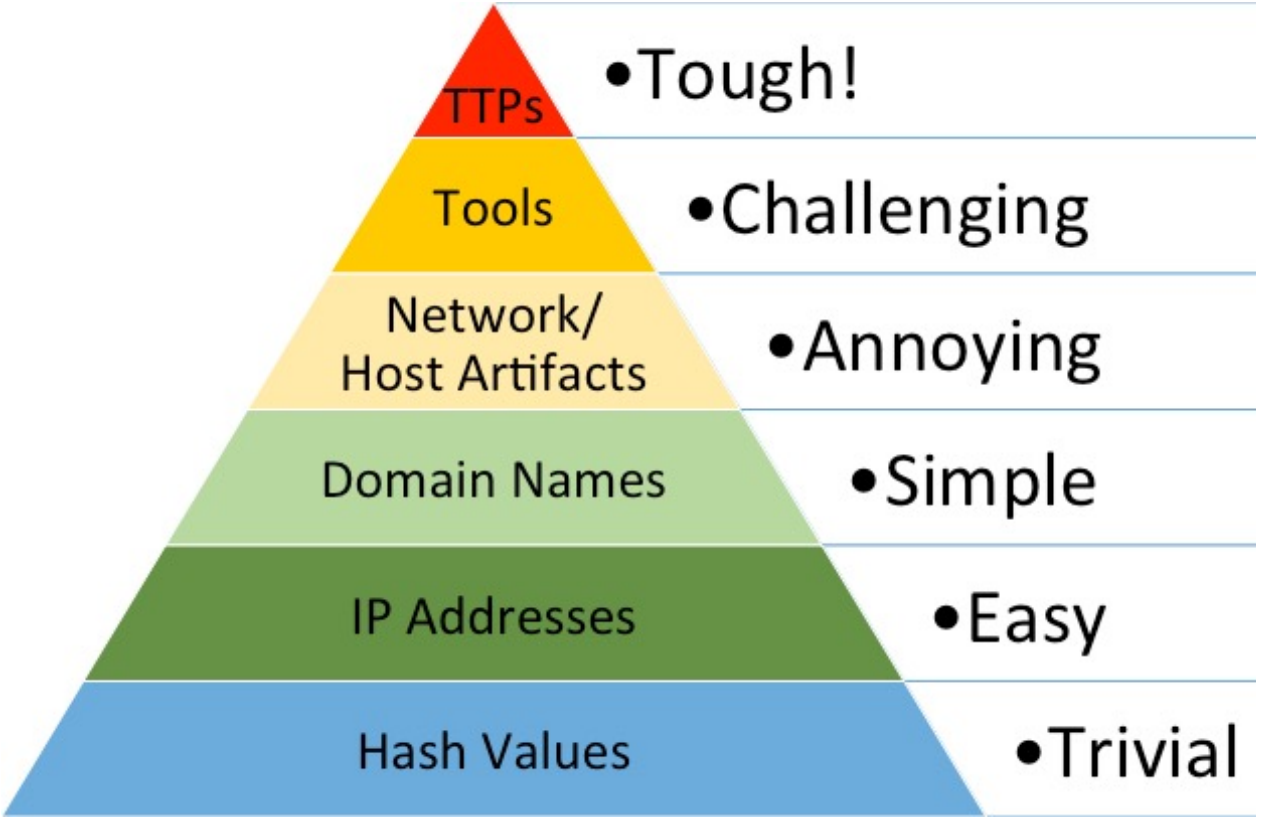
- Describe the **behavior of an actor**
- **Tactic**
  - The **highest-level** description of the behavior
- **Technique**
  - A **more detailed** description of behavior in the context of a **tactic**
- **Procedure**
  - **Highly detailed** description in the context of a **technique**
- **Sources:**
  - MITRE ATT&CK,
  - Possibly CAPEC

Examples of TTPs

- **Privilege escalation** example
  - **Tactic:** privilege escalation
  - **Technique:** vulnerability exploitation
  - **Procedure:** submit specially crafted input to a vulnerable application
- **Network scanning** example
  - **Tactic:** reconnaissance
  - **Technique:** network scanning
  - **Procedure:** run command `nmap -sP <ip_address>/<mask>`

Pyramid of Pain

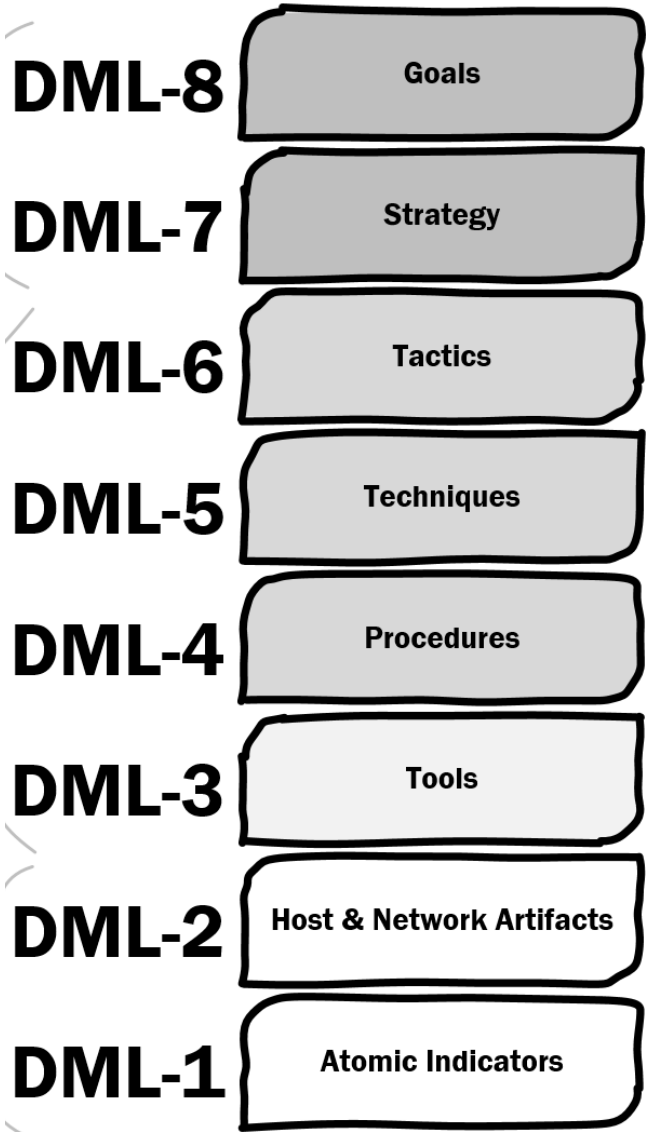
- **Not** all indicators are **equal**
- Attack **complexity** based on **detected** artifacts
- The **lowest** level
  - **Precise** but the **easiest** to change
- The **highest** level
  - **Abstract** but the **hardest** to change
- **Example**:
  - **IP addresses** not valid IOCs after **a day**



MUNI FI

Detection Maturity Level model

- **Detection Maturity Level** (DML) model
  - The **lowest** levels are the most **technically specific**
  - The **highest** levels the most **technically abstract**
- **Comparison with Pyramid of Pain:**
  - The **same ordering** of indicators



MUNI FI

Threat intelligence platforms

- Platforms that **aggregate and organize** threat intelligence
- **Open-source**
  - Collaborative Research Into Threats (CRITs) by MITRE
  - GOSINT by CISCO
- **Commercial**
  - ThreatConnect
  - ThreatStream
- **Community**
  - Open Threat Exchange (**OTX**)
  - Malware Information Sharing Platform (**MISP**)

MUNI FI

Challenges of CTI sharing

- **Trust**
  - **Anyone** can produce cyber threat intelligence
  - Sharing **participants** do not want **negative publicity –** anonymization
- **Quality**
  - information may **not** be **complete** or may be **wrong**
- **Volume of data**
  - Threat **intelligence platforms** contain a lot of **IOCs**
- **Privacy and legal rules**
  - GDPR
- **Changing nature of cyber attacks**
  - CTI may not be usable for the **next attack**
- **Diverse data models and formats**

Standards and enumerations

Standards and enumerations

- Common Attack Pattern Enumeration and Classification (**CAPEC**)
- **MITRE ATT&CK**
- The Structured Threat Information eXpression (**STIX**)
- Trusted Automated Exchange of Intelligence Information (**TAXII**)

MUNI FI

Common Attack Pattern Enumeration and Classification (CAPEC)

- Enumeration of known **attack categories** (attack patterns)
- **Hierarchical** organization
- Example **use cases**:
  - Threat modeling
  - Incident response
- **Example entries**:
  - CAPEC-125 (Flooding) [1]
  - CAPEC-482 (TCP Flood)
  - CAPEC-486 (UDP Flood)

MITRE ATT&CK

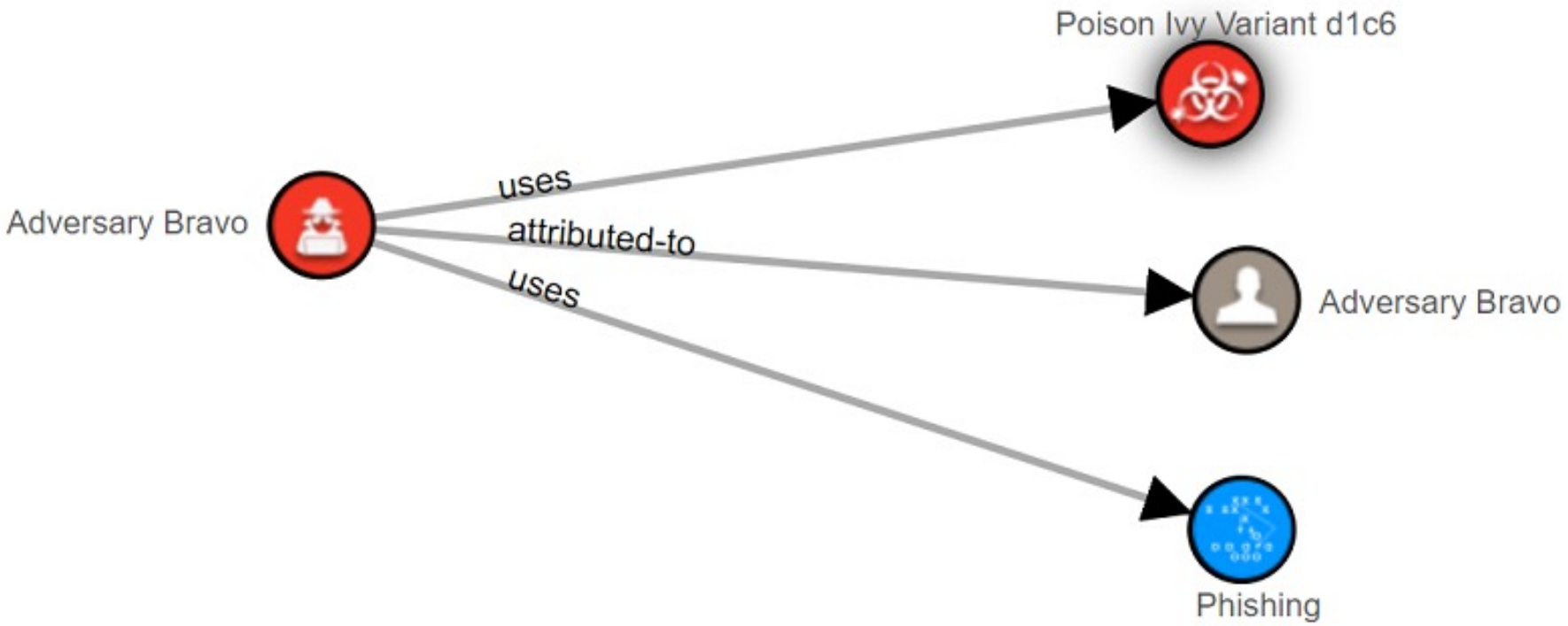
- **A**dversarial **T**actics, **T**echniques **and C**ommon **K**nowledge [1]
- **A knowledge base** of adversarial tactics and techniques created from **real-world** observations
- **A set of matrices** consisting of
  - Tactics (columns)
  - Techniques (rows)
- **Example:** TA0001 – **Initial Access** tactic
  - T1190 – Exploit Public-Facing Application [2]
  - T1566.001 - Phishing: Spearphishing Attachment

The Structured Threat Information eXpression (STIX)

- **A format** for expressing and serialization of **CTI**
- Structured as a **graph** with objects and relationships
- **Objects**:
  - Attack pattern
  - Campaign
  - Malware
  - Vulnerability
  - Other

STIX example

- **Threat actor**
  - Adversary Bravo
- **Identity**
  - Adversary Bravo
- **Attack pattern**
  - Phishing
- **Malware**
  - Poison Ivy
- **Relationships**



MUNI FI

Trusted Automated Exchange of Intelligence Information (TAXII)

- **Protocol** designed to support the exchange of CTI **over HTTPS**
- Any implementation of a server that uses this protocol must **support the STIX format**
- STIX and TAXII should allow **automated processing of CTI**
- Some threat intelligence **platforms provide** data in **STIX**
- MITRE ATT&CK is also **expressed** in STIX

Cyber threat identification and threat management tools

Cyber threat hunting

- **Proactive** security search that
  - Reveals malicious and suspicious **activities that** have **evaded detection** by existing tools
  - Identifies and categorizes potential threats **in advance of** an **attack**
  - Uses **new threat intelligence** on previously collected data
- Threat actors are often **Advanced Persistent Threats** (APTs)
- **Example**:
  - Hunting for **internal reconnaissance**
  - Search **through logs** to find the use of **commands** *whoami, hostname, ipconfig*

Threat hunting and other approaches

- **Threat hunting**
  - Reveals malicious activities that **evaded** detection by **existing tools**
- **Bug bounty** program
  - Uses **existing tools** to discover security vulnerabilities
- **Asset discovery**
  - Uses **existing tools** to discover assets
- **Penetration testing**
  - Uses **existing tools** to test applications

SIEM

- Security **information** and **event** management
- Threat **detection** and security **incident management**
- Collection and analysis of **security events**
  - Near **real-time** and **historical**
- **Core capabilities**
  - **Log event** collection and management
  - Analyze data from **various sources**
  - **Operational capabilities** – dashboards, reporting, and other

SIEM tools

- **Commercial:**
  - **SolarWinds** Security Event Manager (SEM)
  - **AT&T Cybersecurity** (AlienVault) Unified Security Management (USM)
  - **IBM Security** QRadar SIEM
  - **Splunk** Enterprise Security
- **Open-source**:
  - **Elastic** Security
  - **AlienVault** OSSIM (leverages OTX platform),
  - **Apache** Metron,
  - SIEMonster
  - Security Onion

MUNI FI

SOAR

- **S**ecurity **O**rchestration, **A**utomation, and **R**esponse
- Related to **playbooks**
- Streamlines security operations in **three key areas**:
  1. **Threat** and **vulnerability** management
  2. Incident **response**
  3. Security operations **automation**

Questions?

Supplementary materials

- David Bianco. 2013. *The Pyramid of Pain*. http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html
- Ryan Stillions. 2014. *The DML model*. http://ryanstillions.blogspot.com/2014/04/the-dml-model_21.html

Before the seminar

- Those sitting in the 1st row, please switch your seats with other sitting in other rows.
- We would like to test whether problems with VMs are associated with particular machines in this room.

MUNI FI