MANUEL KERN[1][2] // manuel.kern@ait.ac.at

1 AIT Austrian Institute of Technology GmbH, Center for Digital Safety & Security, Security & Communication Technology, Giefinggasse 4, 1210 Vienna, Austria.

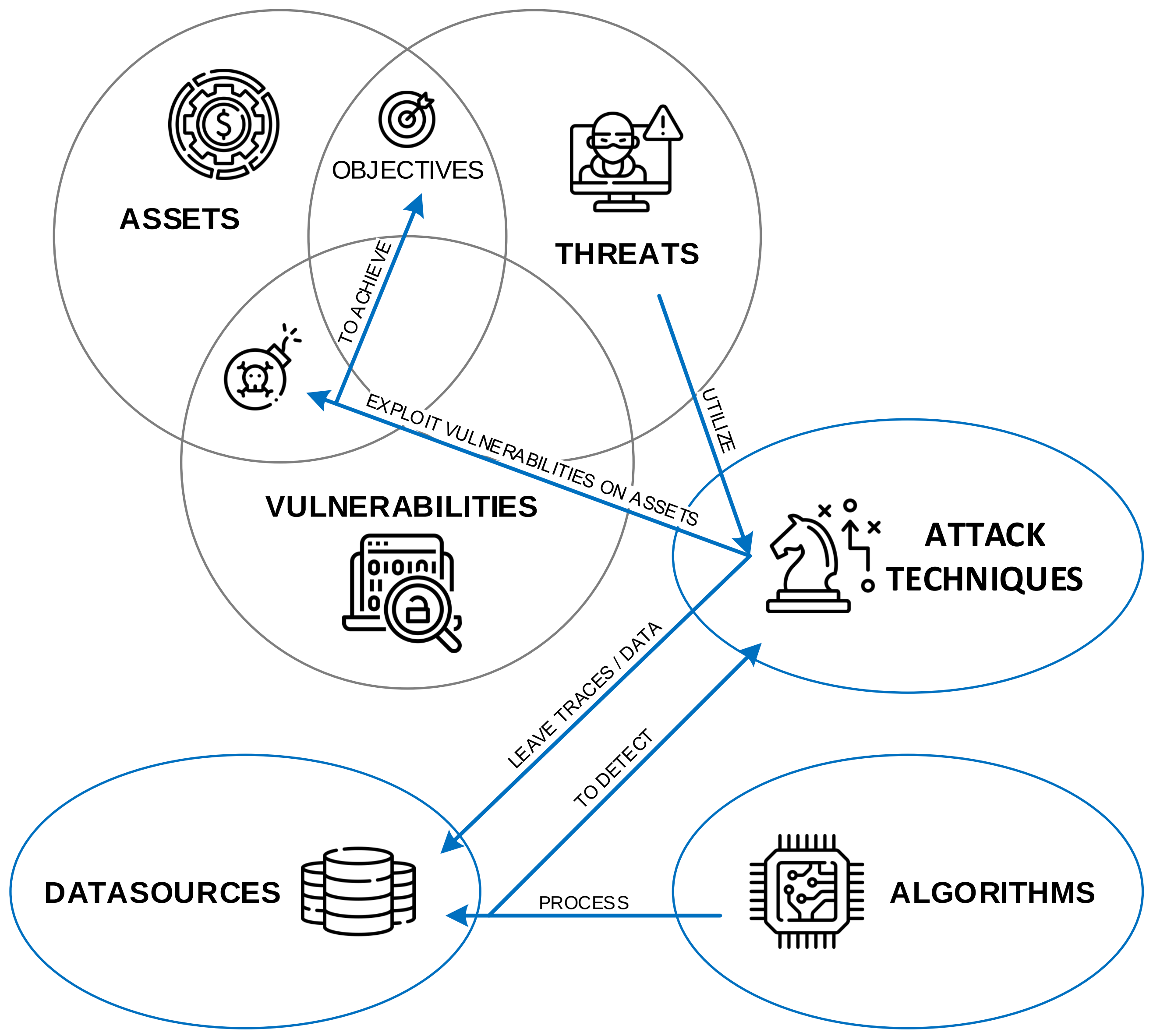
2 Technical University of Vienna, Institute of Information Systems Engineering, Vienna, Austria.

SPOTTED - SYSTEMATIC MAPPING OF DETECTION APPROACHES ON DATA SOURCES FOR ENHANCED CYBER DEFENCE

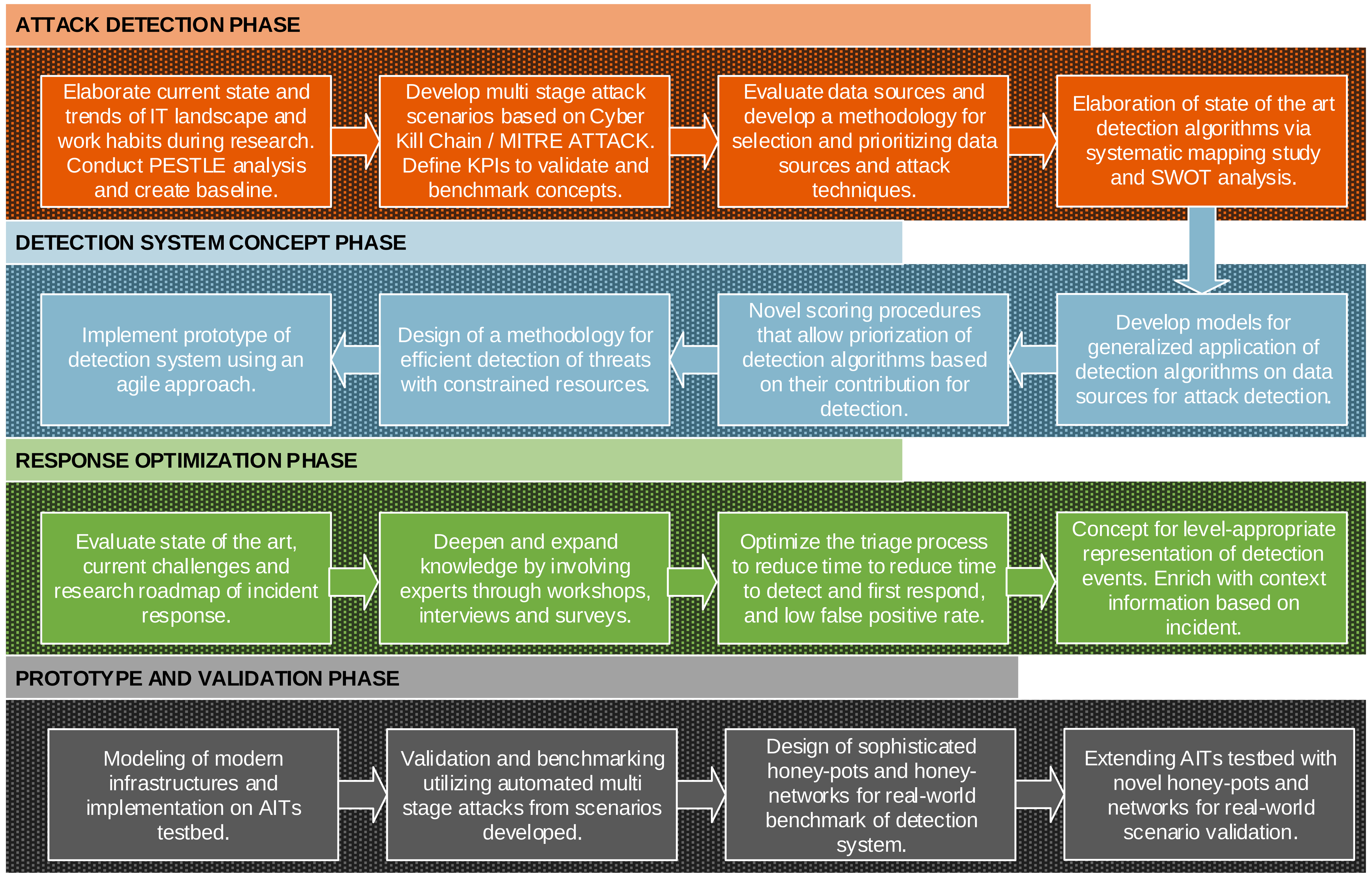
INDUSTRIAL PHD SPOTTED

SPOTTED generates knowledge in the area of usable security. Methods and models in the area of incident detection and response are developed that enable accurate detection and efficient prediction in minimum time. Special focus will be put on the fact that organizations have only limited resources for these processes. Therefore, an optimization problem is the basis of the project. How can the optimal selection of data sources and detection algorithms be found with limited resources in order to detect as many cyber attacks as possible, the most frequent ones or those that are particularly dangerous (in terms of damage), and to react to them in an appropriate time frame.

Project duration: 01.10.2021 – 30.09.2024
Support: Edgar Weippl (TU-Wien), Florian Skopik (AIT)



Project Phases



ATTACK DETECTION PHASE

Elaborate current state and trends of IT landscape and work habits during research. Conduct PESTLE analysis and create baseline.

Develop multi stage attack scenarios based on Cyber Kill Chain / MITRE ATTACK. Define KPIs to validate and benchmark concepts.

Evaluate data sources and develop a methodology for selection and prioritizing data sources and attack techniques.

Elaboration of state of the art detection algorithms via systematic mapping study and SWOT analysis.

DETECTION SYSTEM CONCEPT PHASE

Develop models for generalized application of detection algorithms on data sources for attack detection.

Novel scoring procedures that allow priorization of detection algorithms based on their contribution for detection.

Design of a methodology for efficient detection of threats with constrained resources.

Implement prototype of detection system using an agile approach.

RESPONSE OPTIMIZATION PHASE

Evaluate state of the art, current challenges and research roadmap of incident response.

Deepen and expand knowledge by involving experts through workshops, interviews and surveys.

Optimize the triage process to reduce time to reduce time to detect and first respond, and low false positive rate.

Concept for level-appropriate representation of detection events. Enrich with context information based on incident.

PROTOTYPE AND VALIDATION PHASE

Modeling of modern infrastructures and implementation on AITs testbed.

Validation and benchmarking utilizing automated multi stage attacks from scenarios developed.

Design of sophisticated honey-pots and honey-networks for real-world benchmark of detection system.

Extending AITs testbed with novel honey-pots and networks for real-world scenario validation.

STRATEGIC SELECTION OF DATA SOURCES

Cyber attacks leave traces in data sources, such as in log files, memory or data-streams. Detection systems utilize these data sources to detect the application of specific attack techniques. Attack techniques vary considerably in terms of their effectiveness, potential impact and application by threat actors. Data sources, on the other side, may contain traces of one or several attack techniques, and the effort to process their output may differ heavily. Therefore, it is obvious that not all data sources are of equal value for detection and organizations must carefully survey which sources shall be analyzed and what attack techniques need to be found.

D3TECT, a process model that describes a procedure for dynamically ranking and selecting data sources suitable for detection is introduced.

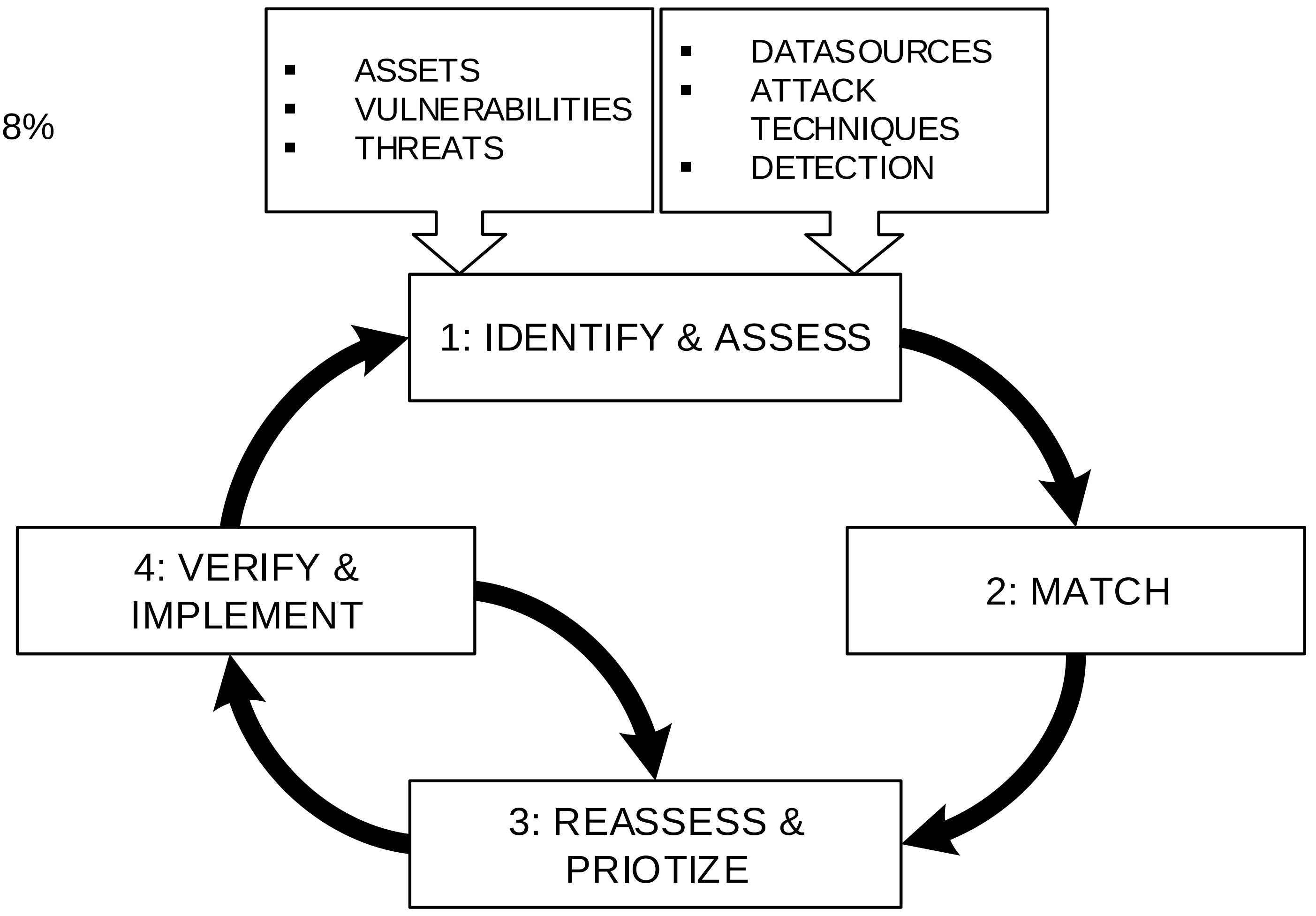
OPTIMAL RANKED SET OF DATA SOURCES FOR DETECTION BASED ON MITRE ATT&CK DATA

1. Command: Command Execution 51.27% (of detected techniques with perfect detection on this data source)
2. Network Traffic: Network Traffic Content 66.31%
3. Process: Process Creation 71.82%
4. File: File Metadata 74.58%
5. User Account: User Account Authentication 77.75%
6. Process: OS API Execution 81.99%
7. Network Traffic: Network Traffic Flow 84.96%
8. File: File Creation 86.86%
9. Application Log: Application Log Content 89.19%
10. Driver: Driver Load 89.41%
11. Drive: Drive Modification 89.83%
12. Active Directory: Active Directory Credential Request 90.68%
13. File: File Content 91.1%
14. Logon Session: Logon Session Creation 92.16%
15. User Account: User Account Modification 93.22%
16. Firmware: Firmware Modification 94.07%
17. File: File Access 94.28%
18. Drive: Drive Access 94.49%
19. Cloud Storage: Cloud Storage Access 94.7%
20. File: File Modification 97.03%
21. Logon Session: Logon Session Metadata 97.25%
22. Instance: Instance Creation 97.88%
23. Snapshot: Snapshot Creation 98.31%
24. Cloud Service: Cloud Service Disable 98.52%
25. Cloud Service: Cloud Service Enumeration 98.73%
26. Cloud Storage: Cloud Storage Enumeration 98.94%
27. Firewall: Firewall Disable 99.15%
28. Image: Image Creation 99.36%
29. Instance: Instance Deletion 99.58%
30. Instance: Instance Modification 99.79%
31. User Account: User Account Creation 100.0%

D3TECT METHODOLOGY

The novelty is that D3TECT accounts for constraints in the selection process so that even if a certain data source cannot be utilized in a specific setting, e.g., due to data privacy constraints, the discovery of the most important attack techniques are still ensured by the remaining data sources.

The model is tested with real data, utilizing the MITRE ATT&CK framework.


ASSETS
VULNERABILITIES
THREATS
DATASOURCES
ATTACK TECHNIQUES
DETECTION
1: IDENTIFY & ASSESS
2: MATCH
3: REASSESS & PRIOTIZE
4: VERIFY & IMPLEMENT