Proactive Cybersecurity tailoring through deception techniques

Authors: Luís Guerra[1] and Luís Gonçalves[2]

[1]a43755@alunos.isel.pt , [2] luis.goncalves@isel.pt

Instituto Superior de Engenharia de Lisboa - Departamento de Engenharia Eletrónica e Telecomunicações e de Computadores (DEETC)

Abstract

A proactive approach to cybersecurity can supplement a reactive approach by helping businesses to handle security incidents in the early phases of an attack. Organizations can actively protect against the inherent asymmetry of cyber warfare by using proactive techniques such as cyber deception. The intentional deployment of misleading artifacts to construct an infrastructure that allows real-time investigation of an attacker's patterns and approaches without compromising the organization's principal network is what cyber deception entails. This method can reveal previously undiscovered vulnerabilities, referred to as zero-day vulnerabilities, without interfering with routine corporate activities. Furthermore, it enables enterprises to collect vital information about the attacker that would otherwise be difficult to access. However, putting such concepts into practice in real-world circumstances involves major problems. This study proposes an architecture for a deceptive system, culminating in an implementation that deploys and dynamically customizes a deception grid using Software-Defined Networking (SDN) and network virtualization techniques. The deception grid is a network of virtual assets with a topology and specifications that are pre-planned to coincide with a deception strategy. The system can trace and evaluate the attacker's activity by continuously monitoring the artifacts within the deception grid. Real-time refinement of the deception plan may necessitate changes to the grid's topology and artifacts, which can be assisted by software-defined networking's dynamic modification capabilities. Organizations can maximize their deception capabilities by merging these processes with advanced cyber-attack detection and classification components. The effectiveness of the given solution is assessed using two use cases that demonstrate its utility.

Keywords: Cyber Deception; Deception Grid; Proactive Cybersecurity; Software-Defined Networking; Cyber Warfare; Network Virtualization.

Objectives

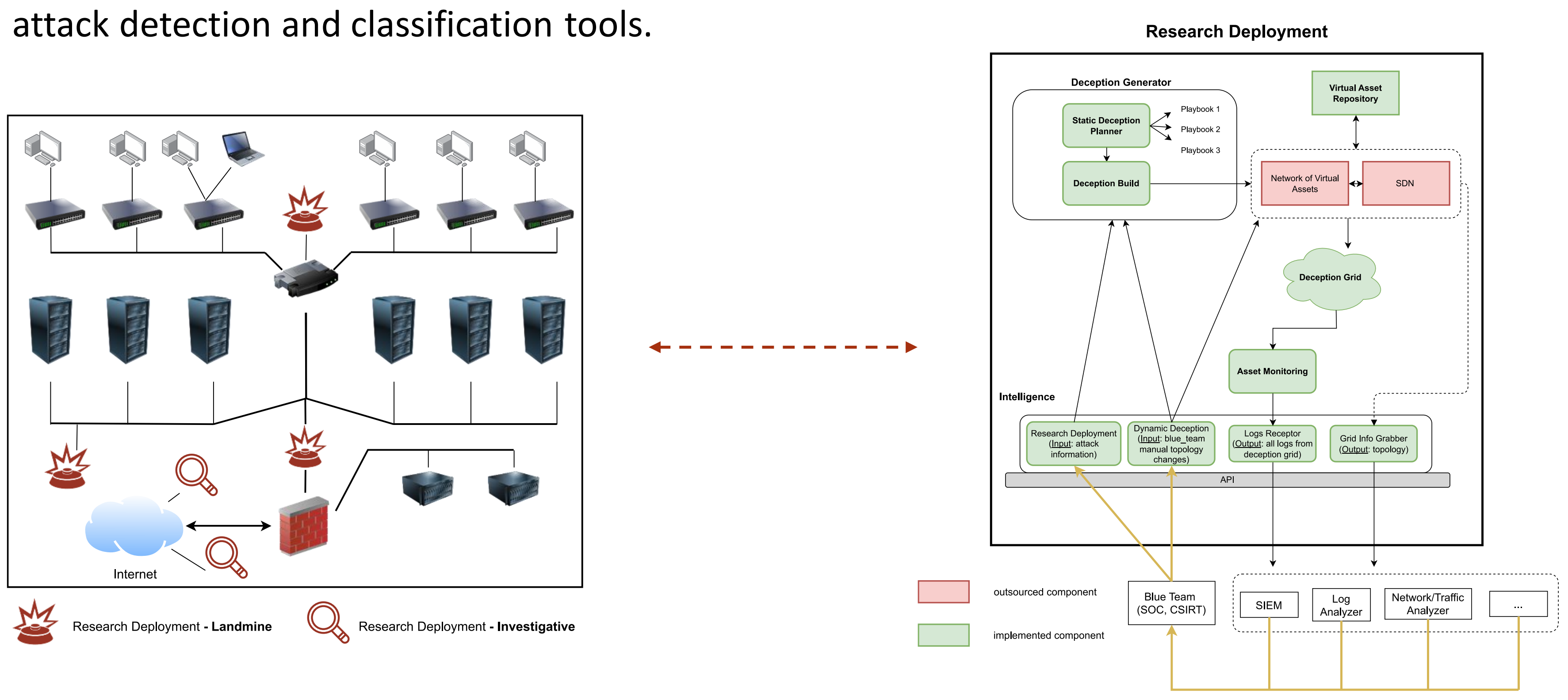
- Conceptual approach to cyber deception and analysis of deception technology.
- **Design a system architecture** with cyber deceptive capabilities:

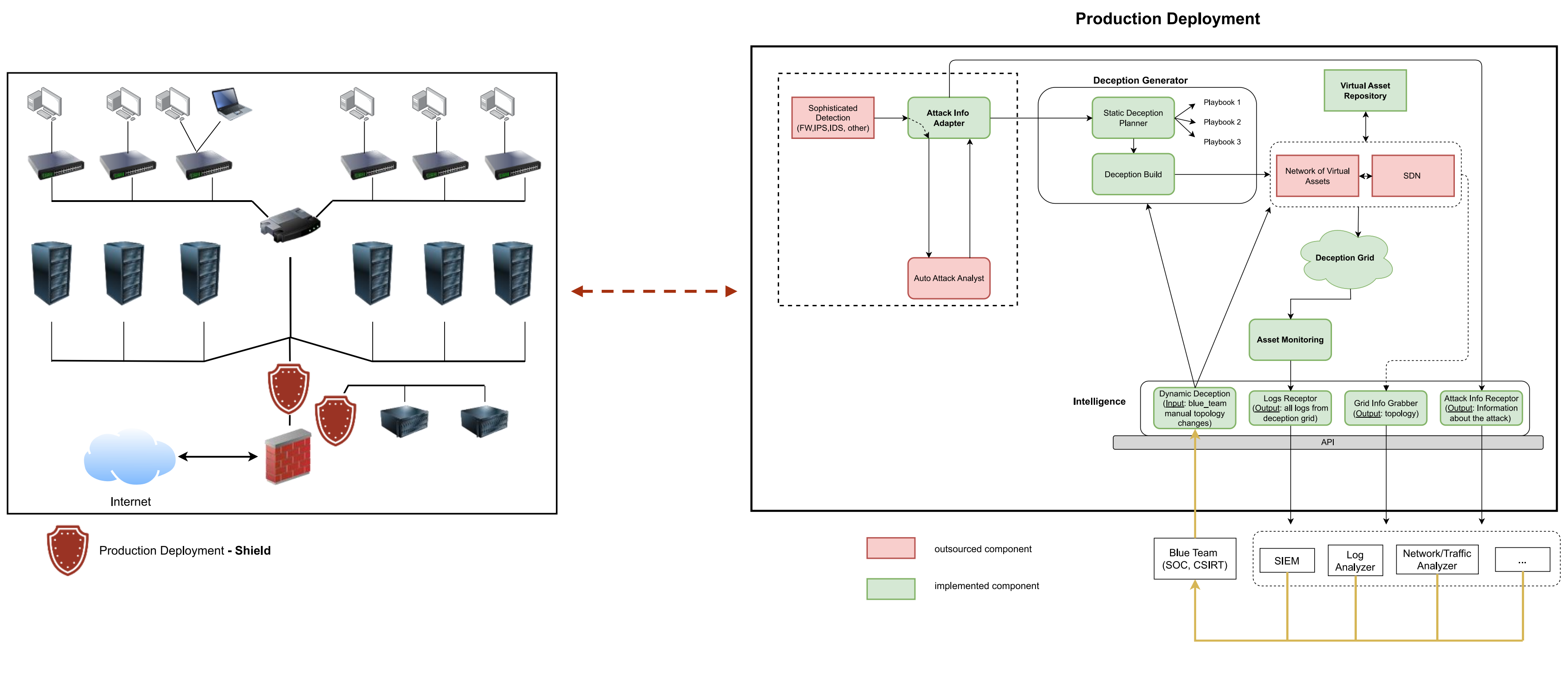
  1. Identify system core components.
  2. Identify external tools that may assist the system's functionalities.
  3. Define and segregate responsibilities between the components.

- **Implementation** of core functionalities.
- **Validate** the correct and advantageous use of the system.

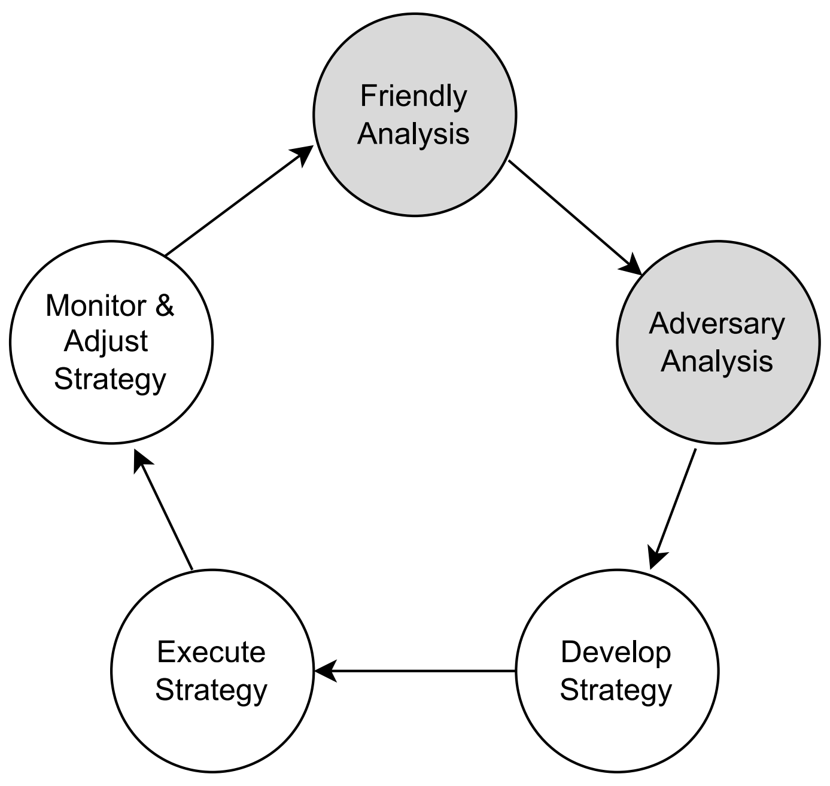
System Architecture

This work proposes **two architectural approaches that should be utilized in a complementary manner** in an organization's cyber deception efforts: **Base Architecture** (for research type of deployments) and its **Extended Architecture** (for production deployments). Research deployment is triggered by the security team and the resulting deception grid can act as a security **alert** (for the security team) and a **trap** (for the attacker) in "landmine" placement (inside infrastructure boundaries). When in "investigative" placement (in direct contact with the Internet), the deception grid can extract **valuable statistical and qualitative information** about possible **organization's adversaries**. Production deployment of the deception grid occurs when an attack is detected and then acts as a "shield", requiring the integration of external cyber-attack detection and classification tools.



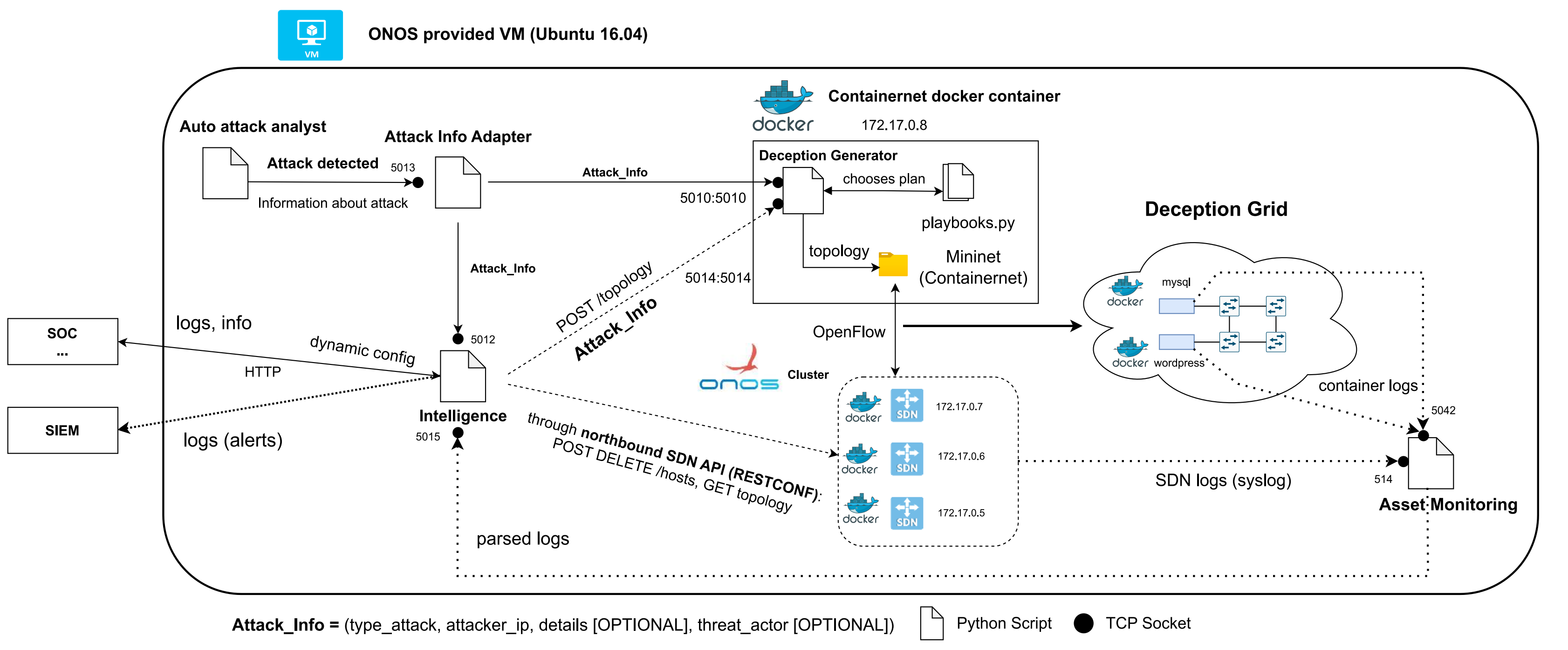


Intelligence component serves as the system gateway enabling communication from the security team to the deceptive system/grid and vice-versa e.g., for research deployment. The security team can additionally dynamically modify the employed deceptive strategy of a deployed deception grid (add and remove hosts) and extract valuable grid-related via this component's API. **Deception Generator** upon receiving a deployment request associated with a set of cyber-attack parameters selects the most suitable deceptive plan according to the received parameters. A deceptive plan is materialized in a deception grid due to the interaction between this component and the triad of **Network of Virtual Assets-SDN-Virtual Asset Repository**. **Network of Virtual Assets** connects the specifically fetched virtual assets (from Virtual Asset Repository) in a network with a planned topology. This network is then managed by SDN (becoming in this context a **Deception Grid**). After its implantation, network and host-centric logs need to be provided to the security team enable real-time visualization of the attacker's footsteps. **Attack Info Adapter** is added on the extended architecture to parse (if needed) proprietary cyber-attack data from external tools to system-acknowledged data on attack classification. **Asset Monitoring** aggregates all deception grid logs and dispatches them to Intelligence which makes them available via **SIEM integration** for the security team to analyze and learn about the attacker's TTP and to evaluate the strategy's effectiveness, which may lead to dynamic modifications. This deceptive operational loop is visible below, adapted from [1]:



System Implementation

The implementation of this system takes advantage of a number of existing technologies and resources, that combined with the development of the depicted components, compose the proposed deceptive system. Python programming language supports the development of the components which communicate via socket connection. Docker containers are used as virtual deceptive assets, Containernet [2] is seized to connect these assets in a realistic virtual network (deception grid) and ONOS [3] SDN controllers are used to manage the grid.



Attack_Info = (type_attack, attacker_ip, details [OPTIONAL], threat_actor [OPTIONAL])

System-acknowledged data for cyber-attack identification is as follows:

Attack_Info (attackType,attackerIp,attackDetails,threatActor)

A set of Playbooks (Python Scripts) contains deceptive strategies for catalogued cyber-attacks. Playbook selection relies on the quantity of information provided. The "attackType" and "attackerIp" parameters are mandatory while others are optional. Specific values of each parameter determines what deceptive strategy is chosen from a certain playbook. A deceptive strategy becomes a deployed deception grid via Python scripting, the use of Containernet's Python packages and the grid's management by ONOS SDN controller.

Conclusions and Future Work

The discussed deceptive system, by leveraging depicted technologies and complementing them with the development of supporting components, enables deception execution versatility, substantial information collection (for attacker's profiling) and ultimately defends the technological infrastructure of an organization diverting the attack through the deception grid. Future work revolves around the clarification of establishing the proposed system in a real technological infrastructure, integration with the referred external tools and the use of attacker redirection enforcing mechanisms.

References

[1] Brown, B.: Deception Strategy Development and Execution, TrapX Security, San Jose, U.S. (2021)

[2] M. Peuster, H. Karl, and S. v. Rossem: MeDICINE: Rapid Prototyping of Production-Ready Network Services in Multi-PoP Environments. IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), Palo Alto, CA, USA, pp. 148-153. doi: 10.1109/NFV-SDN.2016.7919490. (2016)

[3] ONOS(Open Network Operating System), https://opennetworking.org/onos/. Last accessed 14 August 2023