Enhancing Organisational Cyber Resilience with a Machine-Readable Knowledge Base of Cyber Incident Response Communications and Response Activities

Haula Sani Galadima
ADAPT & CCI, School of Computer Science
University College Dublin
Dublin, Ireland
haula.galadima@ucdconnect.ie

Cormac Doherty
CCI, School of Computer Science
University College Dublin
Dublin, Ireland
cormac.doherty@ucd.ie

Rob Brennan
ADAPT & CCI, School of Computer Science
University College Dublin
Dublin, Ireland
rob.brennan@ucd.ie

INTRODUCTION

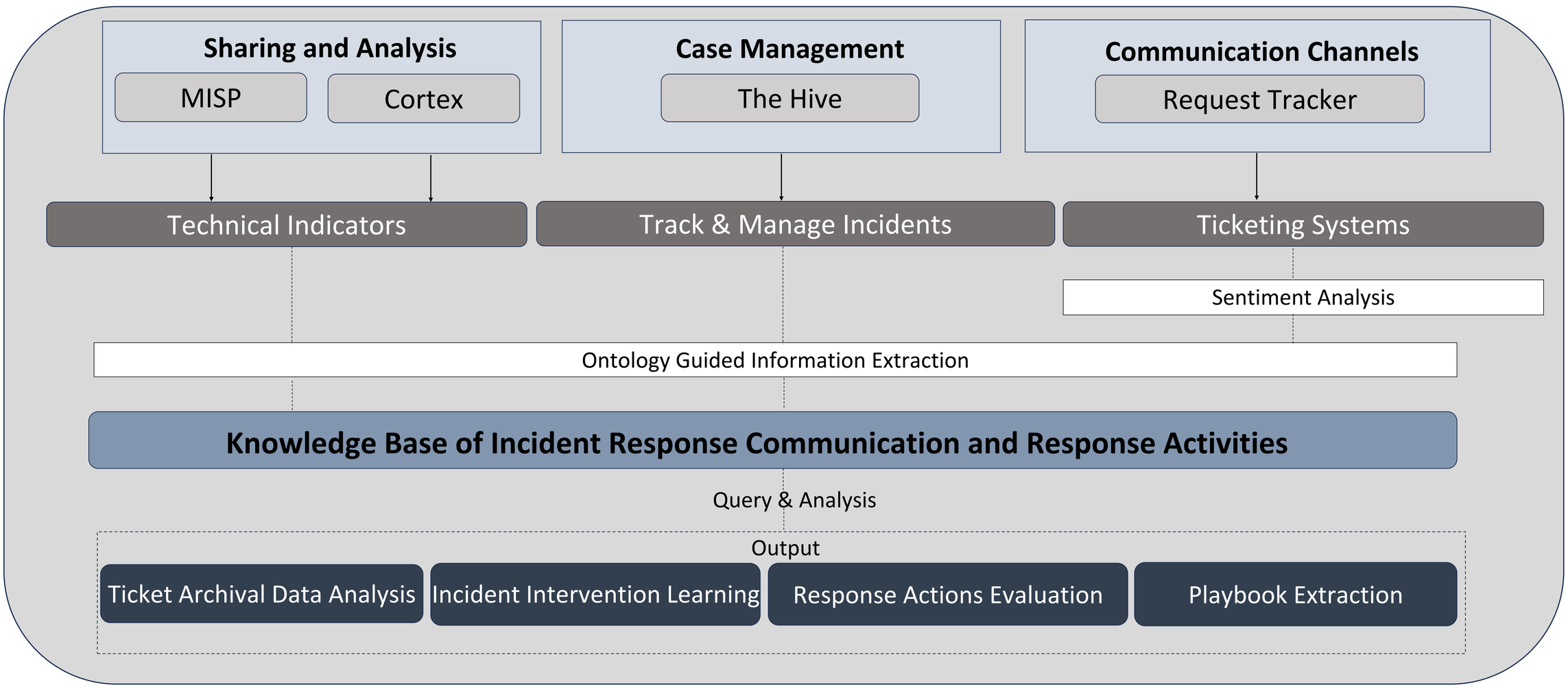
Problem statement:

- The learning components of incident response and post-incident activities frequently receive insufficient attention [1].
- To be able to achieve cyber resiliency, there is a need to establish mechanisms that can learn and reuse the knowledge of how an incident was resolved.

Aim:

- This research aims to enhance learning and continuous improvement in incident response, with a specific focus on effective communication and response activities to enhance organisational resilience.
- Evaluation of corrective measures and root cause analysis from past incidents enables defense systems modification and adaptation to proactively react to emerging security threats, risks and attacks [2].

SYSTEM ARCHITECTURE



SIGNIFICANCE

- This proposed framework addresses the lack of an evidence-driven approach to incident intervention learning [1] and addresses the absence of a common format for analyzing diverse process data in incident response.

METHODOLOGY

The development of a machine-readable knowledge base using and extending existing cybersecurity ontologies such as Unified Cyber Ontology (UCO) [3], and Cyber-investigation Analysis Standard Expression (CASE) [4] ontology for IR-specific elements. The knowledge base will serve as a repository that stores a structured collection of incident response communication and strategies for response actions, utilizing Natural Language Processing (NLP) models for automated extraction, assessment, and categorization.

DATA SOURCES TO ENRICH THE KNOWLEDGE BASE

The following sources will be used to enrich the knowledge base:

Technical:

- External resources, such as the Malware Information Sharing Platform (MISP) and The Hive, will be leveraged to extract incident and threat intelligence-related data.

Social:

- This research identifies the vital role of ticketing systems and communication channels within Computer Security Incident Response Team (CSIRT) operations as repositories of unstructured institutional knowledge about incident response.
- The social dynamics of analyst activities will be analysed using methods such as sentiment analysis.

REFERENCES

1. Ahmad, A., Hadgkiss, J. and Ruighaver, A.B., 2012. Incident response teams–Challenges in supporting the organisational security function. Computers & Security, 31(5), pp.643-652.
2. Ahmad, A., Desouza, K.C., Maynard, S.B., Naseer, H. and Baskerville, R.L., 2020. How integration of cyber security management and incident response enables organizational learning. Journal of the Association for Information Science and Technology, 71(8), pp.939-953.
3. Syed, Z., Padia, A., Finin, T., Mathews, L. and Joshi, A., 2016. UCO: A unified cybersecurity ontology. UMBC Student Collection.
4. Casey, E., Barnum, S., Griffith, R., Snyder, J., van Beek, H. and Nelson, A., 2018. The evolution of expressing and exchanging cyber-investigation information in a standardized form. Handling and Exchanging Electronic Evidence Across Europe, pp.43-58..

This research was conducted with the financial support of Science Foundation Ireland at ADAPT, the SFI Research Centre for AI-Driven Digital Content Technology at UCD [13/RC/2106_P2].