

Cyber Threat Intelligence and Critical National Infrastructure: Effective Cyber Threat Intelligence and its impact on reducing security risk

BSc (Hons) Computing (Computer Networks and Cybersecurity) Carys Newing

1. Introduction

Critical National Infrastructure (CNI) organisations face persistent and evolving cyber threats that can impact service availability, safety and public trust.

Cyber Threat Intelligence (CTI) provides awareness of vulnerabilities, threat actors, and emerging attack techniques. However, manual intelligence consumption limits time and scalability within an organisation.

There is limited applied research evaluating whether automated CTI alerting systems directly contribute to a measurable security risk reduction within CNI environments and this project addresses the gap.

2. Aim and Objectives

Aim:

To evaluate whether an automated Cyber Threat Intelligence alerting system can reduce cyber security risk within a Critical National Infrastructure environment.

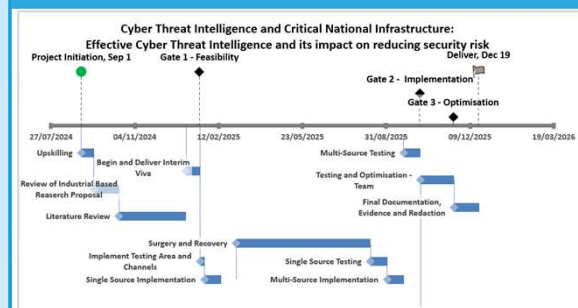
Objectives:

1. Research and Literature review to perform Gap analysis and understand requirements
2. Design and develop alerting system based on requirements
3. Produce documentation outlining the system architecture, key components and data flows along with implementation
4. Conduct comprehensive testing and evaluate effectiveness

3. Lit Review

CTI in Security Operations	CNI Risk Characteristics	Automation in CTI
• Enables intelligence-led defence • Supports proactive vulnerability management • Improves detection and response capabilities	• High availability requirements • IT/OT convergence • Regulatory and resilience obligation	• Increase threat volume requires automation • Continuous monitoring enhances situational awareness • Intelligence must be operationalised not just collected

4. Project Timeline



Followed a waterfall model. Actual project included delays due to medical leave.

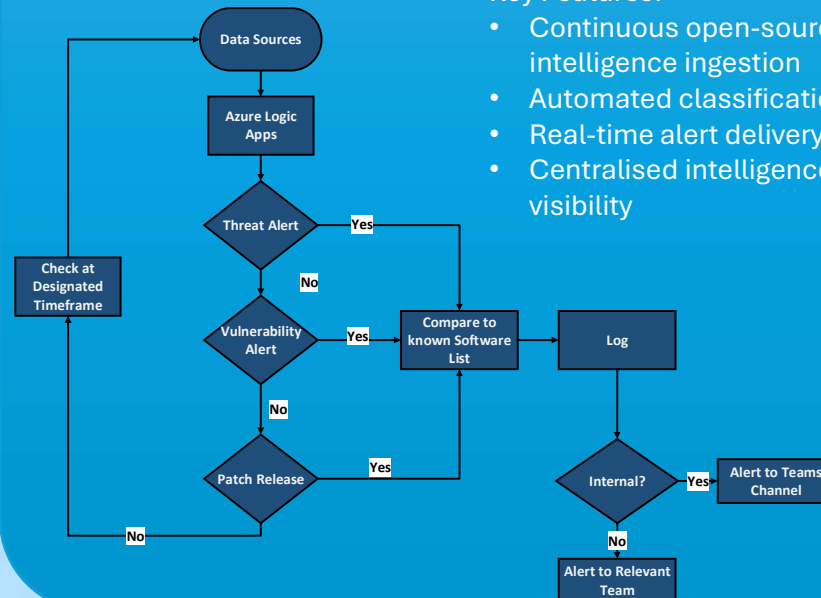
Set timescales for implementation and testing at each phase.

5. Design & Implementation

Due to being CNI this project had to be implemented externally and assessed by Dwr Cymru Welsh Water for system compatibility.

Key Features:

- Continuous open-source intelligence ingestion
- Automated classification
- Real-time alert delivery
- Centralised intelligence visibility



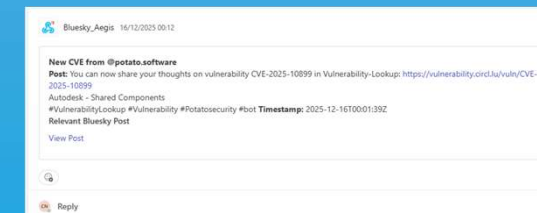
8. References

- [1] R. M. Lee, "2020 SANS Cyber Threat Intelligence (CTI) Survey," SANS Institute, 2020. <https://www.sans.org/white-papers/39395/> (accessed Dec. 14, 2025).
- [2] NIST, "The NIST cybersecurity framework (CSF) 2.0," The NIST Cybersecurity Framework (CSF) 2.0, vol. 2.0, no. 29, Feb. 2024, doi: <https://doi.org/10.6028/nist.cswp.29>.
- [3] NCSC, "Cyber Assessment Framework," www.ncsc.gov.uk, Apr. 18, 2024. <https://www.ncsc.gov.uk/collection/cyber-assessment-framework>
- [4] K. Baker, "What Is Cyber Threat Intelligence? [Beginner's Guide] | CrowdStrike," CrowdStrike.com, Mar. 04, 2025. <https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/>
- [5] H. Kure and S. Islam, "Cyber Threat Intelligence for Improving Cybersecurity and Risk Management in Critical Infrastructure," Journal of Universal Computer Science, vol. 25, no. 11, pp. 1478–1502, Nov. 2019, Available: <https://repository.uel.ac.uk/item/877y3>

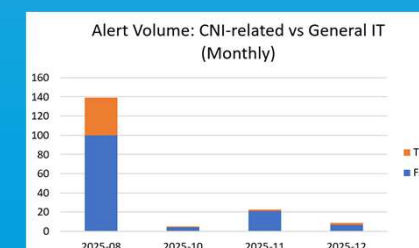
6. Testing

Dataset:

- 176 CTI events generated
- Real-world operational intelligence



Framework Alignment

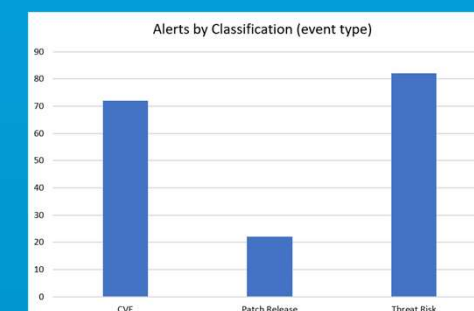


NIST Cybersecurity Framework

- Identify (ID.RA) – Early vulnerability awareness
- Detect (DE.CM) – Continuous Monitoring Support
- Respond (RS.MI) – Risk-based remediation prioritisation

UK NCSC Cyber Assessment Framework

- Objective A3 – Understanding Security Risk
- Partial Support for protective decision-making



7. Conclusion

The automated CTI alerting system demonstrates measurable support for cyber security risk reduction within a CNI environment.

The system aligns strongly with recognised framework functions related to risk identification and situational awareness.

It functions as an enabling capability within a defence-in-depth strategy rather than a standalone security control.

Operational feedback from Dwr Cymru Welsh Water confirmed the system met organisational requirements and provided practical value.