Section A: Survey Information & Consent

Study Title:

Evaluation of an AI-Enabled Cyber Threat Intelligence (CTI) Framework for Industrial and Critical Infrastructure Environments Research

Purpose:

This survey is part of a PhD research study conducted at Cranfield University.

The aim of the study is to evaluate a proposed Cyber Threat Intelligence framework that employs Natural Language Processing (NLP) and Large Language Models (LLMs) to support threat detection and analysis in Industrial Control Systems (ICS) and Industry 4.0 environments.

Why You Have Been Invited:

You are invited to participate because of your professional experience in cybersecurity, CTI, SOC operations, incident response, ICS/OT security, or related domains. Your expertise is valuable in assessing the practical relevance and feasibility of the proposed framework. Voluntary Participation: Participation is entirely voluntary. You may decline to answer any question or withdraw at any time before submitting the survey. There are no penalties or disadvantages for choosing not to participate.

Confidentiality & Data Handling:

• No personally identifying information is required.
• Responses will be stored securely and used only for academic research purposes.
• Data will be reported in aggregate form so that individuals cannot be identified.
• Optional contact information (if provided) will be stored separately

and will not be linked to survey responses.

Risks & Benefits:

There are no known risks associated with participating in this survey.

While there may be no direct personal benefit, your input will contribute to research that may support the development of more effective cyber defence methodologies for industrial environments.

Time Commitment:

The survey is expected to take approximately 10–15 minutes to complete.

Ethics Approval:

This research has been reviewed and approved by the Cranfield University Research Ethics System (CURES), Reference Number: CURES/26101/2025.

Contact for Questions:

If you have questions about this study, please contact: Cranfield University Email: majed.albarrak.592@cranfield.ac.uk

Consent Statement By proceeding with this survey, I confirm that:

- I am 18 years of age or older,
- I have read and understood the information provided above,
- I understand that participation is voluntary and anonymous, and
- I agree to participate in this research study.

Participation is voluntary and anonymous.
Participation is voluntary and anonymous.

Please indicate your consent below:

- ◯ Yes, I consent to participate
- ◯ No, I do not consent

I confirm I am a cybersecurity / CTI / SOC / ICS security professional and consent to participate.

- ◯ Yes
- ◯ No

Section B: Introduction

Expert Survey for Evaluating the NLP-Based CTI Framework for Industrial Cybersecurity

This survey is part of a research study evaluating an AI-enabled Cyber Threat Intelligence (CTI) framework that integrates Natural Language Processing (NLP) and Large Language Models (LLMs) to support proactive cyber defense for Industrial Control Systems (ICS) and Industry 4.0 environments.
The framework is depicted in these two main diagrams:

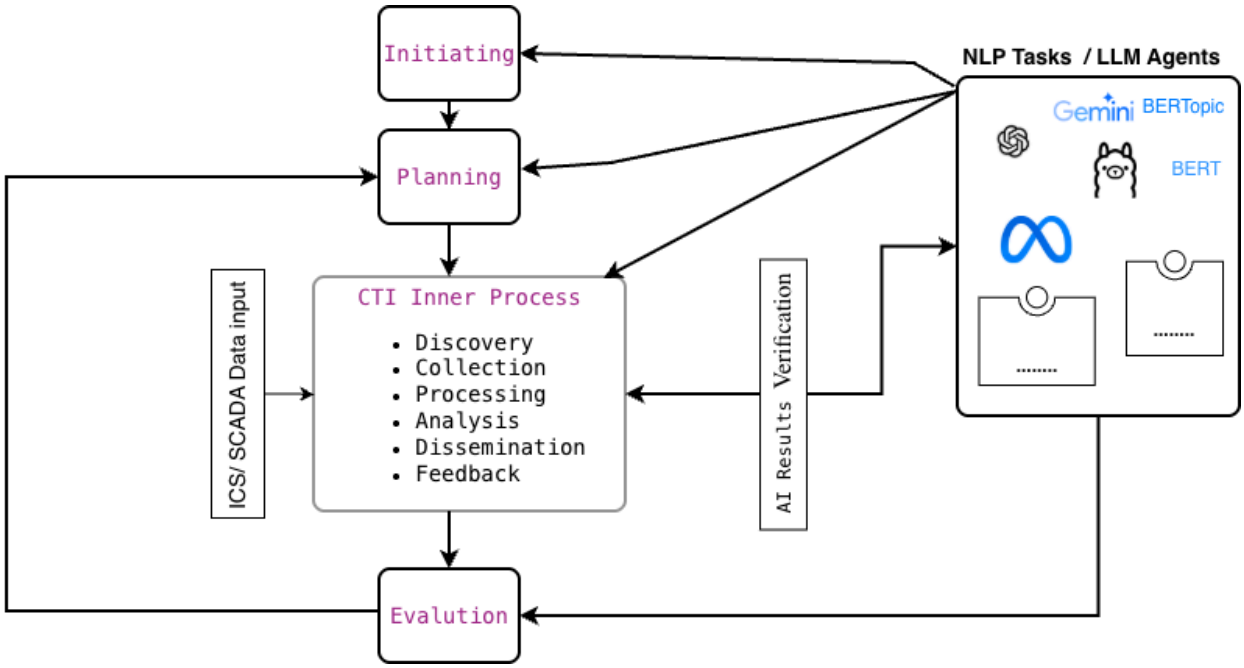

Figure 1. High-Level Framework Overview

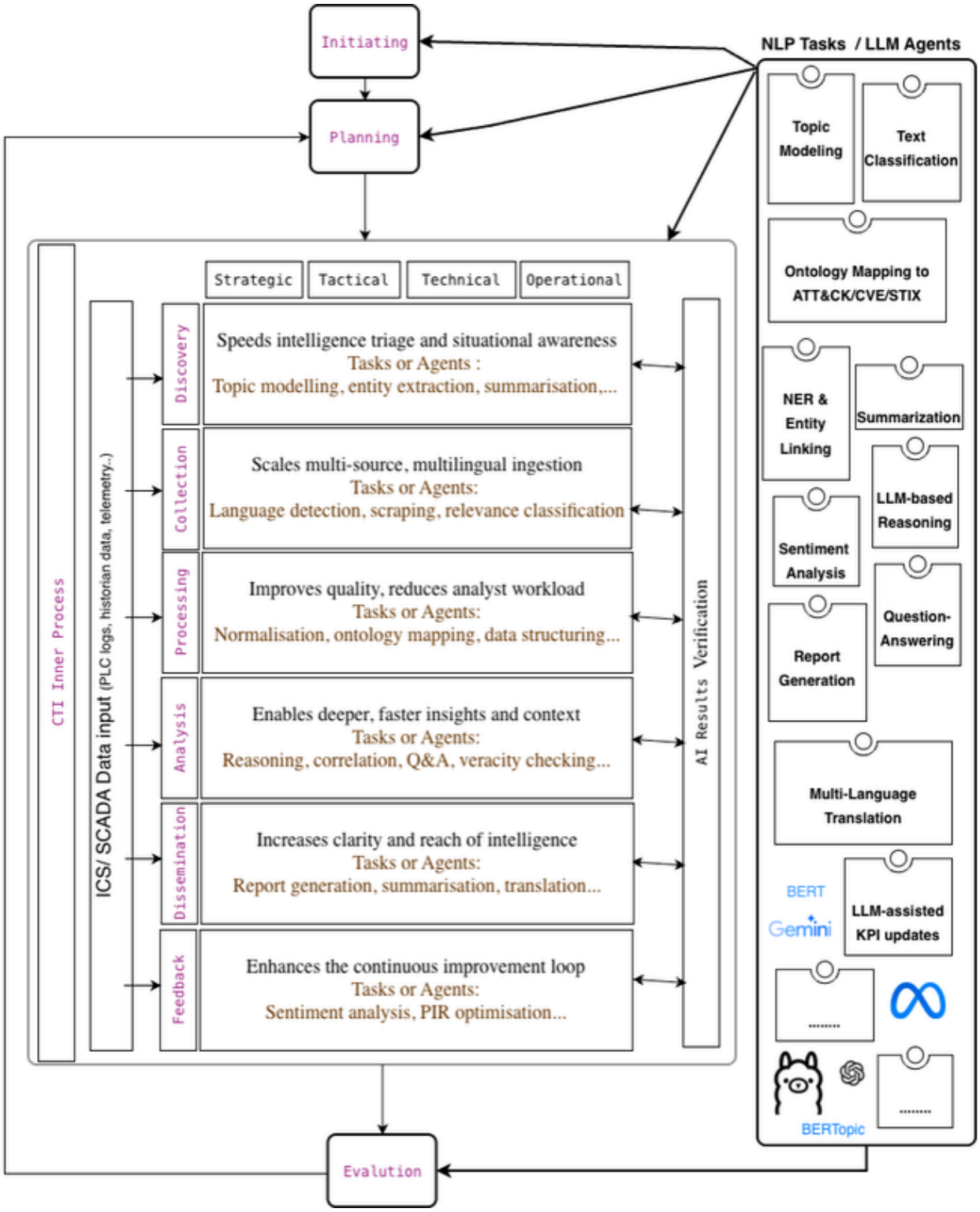

Figure 2. Detailed NLP-based CTI Framework

The framework integrates the best AI-based practices, and two AI contributions, papers, have been made:

- U-BERTopic: A domain-adapted topic modelling method that prioritises emerging and high-urgency cyber discussions to support early threat detection.
- AC_MAPPER: A Large Language Model fine-tuned to map unstructured threat intelligence text to MITRE ATT&CK (including ICS

techniques), improving semantic alignment and traceability of threat behaviours.
Your feedback will help assess the relevance, interpretability, and practical deployability of the framework.

Section C : Participant Profile

Current job role:

- ◯ SOC Analyst
- ◯ CTI Analyst
- ◯ ICS
- ◯ OT Engineer
- ◯ Incident Responder
- ◯ Researcher
- ◯ Management
- ◯ AI/ Data Engineer
- ◯ Other

Years of professional experience

- ◯ Less than 2 years
- ◯ 2-5 years
- ◯ 6-10 years
- ◯ More than 10 years

Primary work domain?

- ◯ Critical Infrastructure
- ◯ Industrial Automation
- ◯ Defense
- ◯ Goverment
- ◯ Companies (Private Sector)
- ◯ Academia / Research centers

Familiarity with MITRE ATT&CK

- ◯ Low
- ◯ Moderate
- ◯ High
- ◯ Expert

Experience using AI/ML in cyber analysis

- ◯ No
- ◯ Yes

Section D : Framework Evaluation

Conceptual Completeness

(1 = Strongly Disagree → 5 = Strongly Agree)

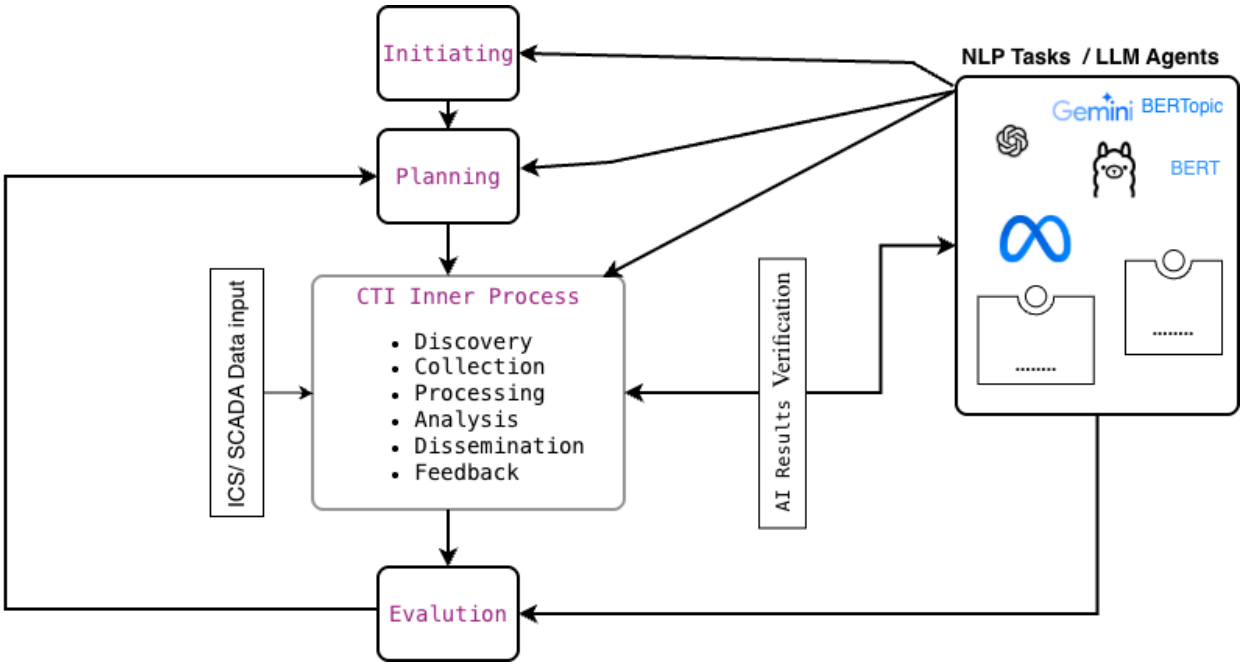

Figure 1. High-Level Framework Overview

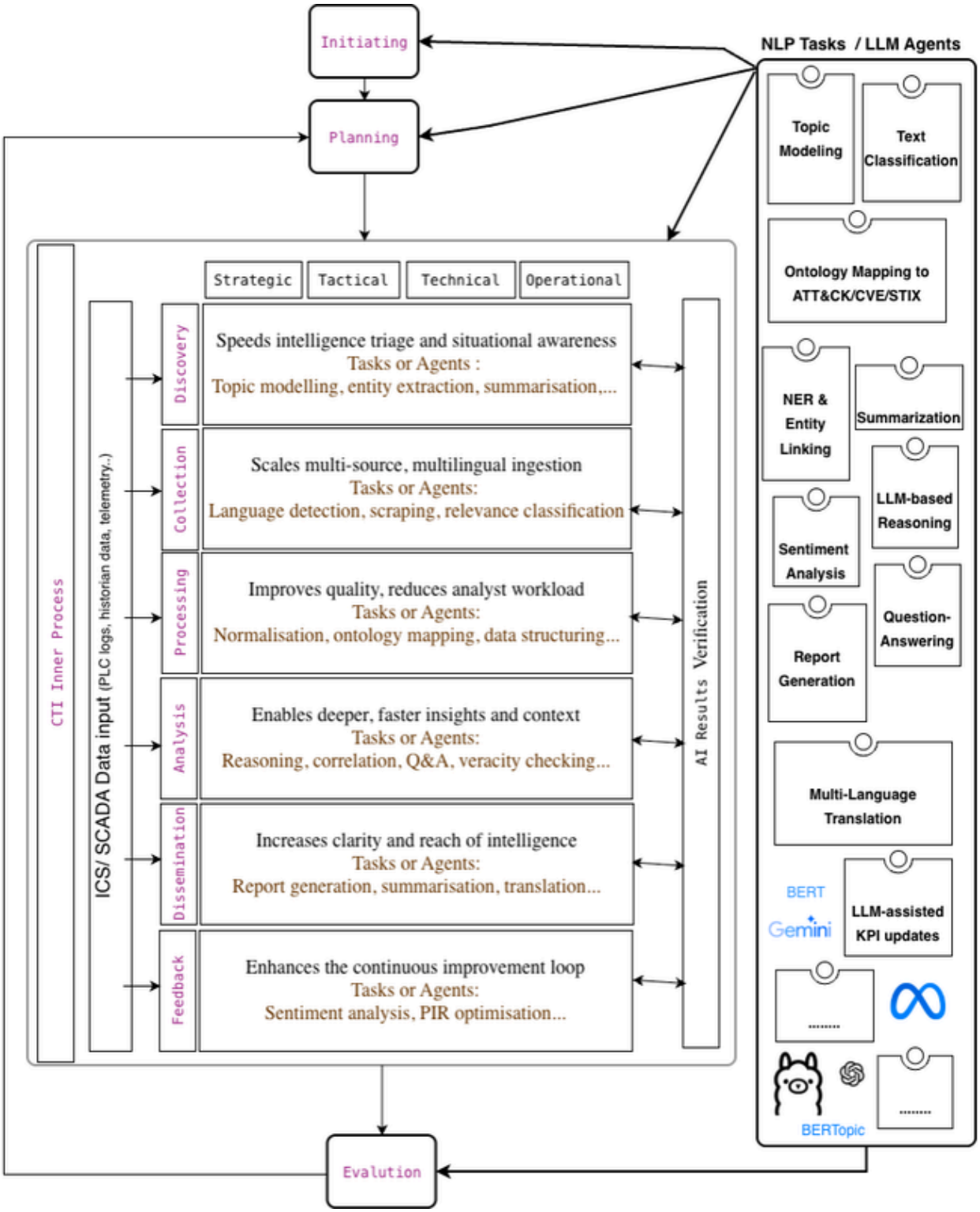

Figure 2. Detailed NLP-based CTI Framework

	1	2	3	4	5
The CTI workflow in Figure 2 reflects real intelligence processes.	○	○	○	○	○

The inclusion of ICS/SCADA data sources makes the framework applicable to industrial environments.	○	○	○	○	○
The framework aligns with operational needs in Industry 4.0 and Critical Infrastructure security.	○	○	○	○	○
U-BERTopic or other cybersecurity Topic Modelling supports early threat discovery from public and intelligence sources.	○	○	○	○	○
AC_MAPPER or Other Mapper models improve the precision and traceability of MITRE ATT&CK (including ATT&CK for ICS) mapping.	○	○	○	○	○
NLP/LLM components reduce analyst workload while preserving contextual accuracy.	○	○	○	○	○
The AI Results Verification loop	○	○	○	○	○

provides adequate human oversight.	○	○	○	○	○
Analysts would understand and trust the outputs of the framework.	○	○	○	○	○
Automation is balanced appropriately with human judgment.	○	○	○	○	○
The framework could integrate with SOC or OT monitoring systems.	○	○	○	○	○
Deployment is feasible given real-world ICS constraints (safety, latency, reliability).	○	○	○	○	○
It would likely improve industrial cyber resilience.	○	○	○	○	○

Section E : Scenario-Based Assessment

(1 = Strongly Disagree → 5 = Strongly Agree)

(Each case describes a realistic industrial cyber incident)

Scenario 1 : Power Grid Ransomware “VoltShade” targets SCADA workstations in a national electrical utility. Early warnings appear on security communities and social media.

	1	2	3	4	5
The framework could detect early threat signals using NLP triage.	○	○	○	○	○
ATT&CK for ICS mapping would help identify affected TTPs.	○	○	○	○	○
The analyst + AI verification loop would prevent incorrect risk escalation.	○	○	○	○	○

Scenario 2 : Water Treatment PLC Firmware Manipulation A compromised vendor update modifies chlorine dosing logic in a water treatment facility.

	1	2	3	4	5
The framework can combine CTI + historian/PLC telemetry for detection.	○	○	○	○	○
The AI reasoning layer would support root-cause clarification.	○	○	○	○	○
The framework output would be understandable to OT engineers.	○	○	○	○	○

Scenario 3 : Smart Factory Insider Data Exfiltration An engineer uses IoT sensors to exfiltrate proprietary models.

	1	2	3	4	5
NLP could detect early insider threat signals in discussions/logs.	○	○	○	○	○
LLM correlation could link suspicious behaviors to known ICS tactics.	○	○	○	○	○
The continuous feedback loop would improve insider threat awareness.	○	○	○	○	○

Section F : Open Feedback

Please answer in few words to these questions.

Most valuable strength of the framework:

Most significant limitation or risk:

Recommendations for improvement:

We thank you for your time spent taking this survey.
Your response has been recorded.