A Proactive Cyber Threat Response Framework Integrating Real-Time CTI with MITRE ATT&CK and D3FEND Mapping*

Rino-Jo[1]
and Han-Bin Lee[1], Jihun Han[1], Woong-Kyo Jung[1], Jun-Yong Lee[2], Tae-Young Kang[2], Byung-Il Kwak[3]†, Mee Lan Han[3]‡, and Jungmin Kang[3]§

Korea University, Sejong, South Korea
jolino@korea.ac.kr, 2019270119@korea.ac.kr, smallstone00@korea.ac.kr,
zzang98gu@korea.ac.kr, jjanggoo@korea.ac.kr, kkttyy324@korea.ac.kr,
kwacka12@korea.ac.kr, blosst@korea.ac.kr, jmkang@korea.ac.kr

Abstract

The modern cyber threat environment is increasingly diversified, creating a persistent gap between threat awareness and operational response. This study proposes a framework to bridge this gap by leveraging the latest CTI together with the MITRE ATT&CK and D3FEND knowledge bases. The framework maps threat information collected from OpenCTI to the MITRE ATT&CK tactics and techniques taxonomy and leverages LLMs to generate diverse TI-based variant scenarios. These scenarios are organized along tactic sequences, each technique mapped to MITRE D3FEND defensive technique groups by combining official MITRE mappings with LLM-assisted inference, and delivered as a Defense Description. The framework rapidly links the latest TI to scenarios and defensive options and systematizes response decision-making through risk-based prioritization, thereby enabling proactive defense against diverse, evolving attacks.

1 Introduction

Recent patterns of cyberattacks are becoming increasingly sophisticated and diverse. Recent cases further underscore the necessity of this approach. In May 2021, the Colonial Pipeline ransomware incident, which began with the compromise of a single account, resulted in the complete shutdown for several days of a 5,500-mile pipeline supplying fuel to the U.S. East Coast. This highlighted how a single breach can exert massive influence over critical infrastructure operations[1]. Similarly, in early 2024, a deepfake based phishing scam at a Hong Kong company involved an AI-generated fraudulent video call impersonating executives, deceiving an employee into transferring approximately 25 million dollars. This incident demonstrated the real-world convergence of social engineering with advanced deepfake technology[2]. Such examples show that systematic analysis and preparation based on up to date threat intelligence are indispensable for responding effectively to increasingly sophisticated threats.

*Proceedings of the 9th International Conference on Mobile Internet Security (MobiSec'25), Article No. P-30, December 16-18, 2025, Sapporo, Japan.

†Corresponding author: jmkang@korea.ac.kr

‡Corresponding author: blosst@korea.ac.kr

§Corresponding author: kwacka12@korea.ac.kr

2 Methodology

This study proposes a framework for responding to emerging threats that comprises CTI collection and preprocessing, MITRE ATT&CK–based threat scenario generation, D3FEND based defensive technique mapping, and the production of a Defense Description. In Figure 1, In the preprocessing stage of the framework, objects are collected from OpenCTI. The resulting Fragmented TI Dataset is combined with the latest ATT&CK data to compose the data required for scenario training and inference. This data is injected as LLM based context to generate, for the input TI bundle T_I, a threat scenario in the form of a technique sequence with a tactical order, $T_{i1} \to T_{i2} \to \cdots$. The generated scenarios are mapped to D3FEND techniques via MITRE's official mappings through mitigation associations and via LLM-assisted inference. The outputs are produced as a Defense Description in a report format that includes the TID, recommended D3FEND techniques, supporting rationale, and preconditions, and, when necessary, are integrated with ASM(Attack Surface Management).

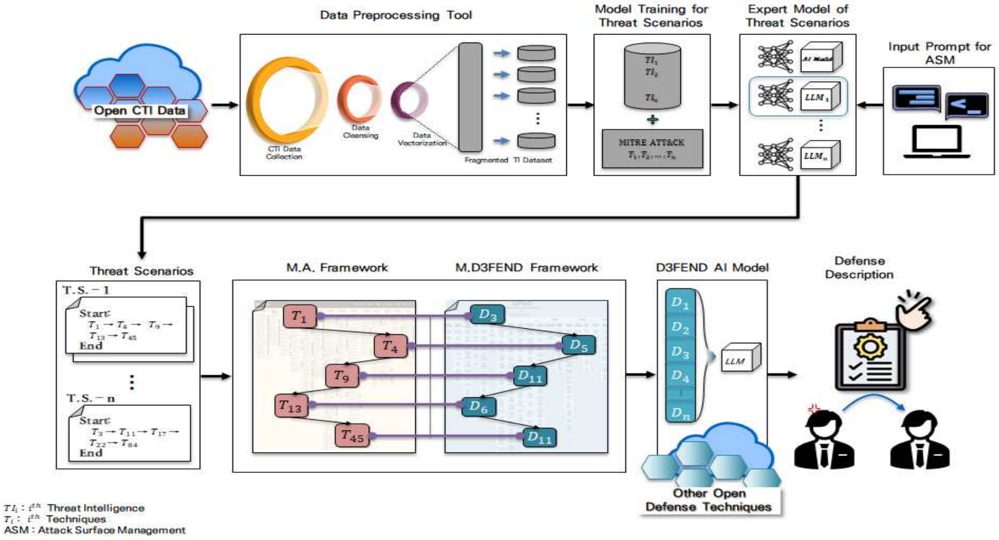
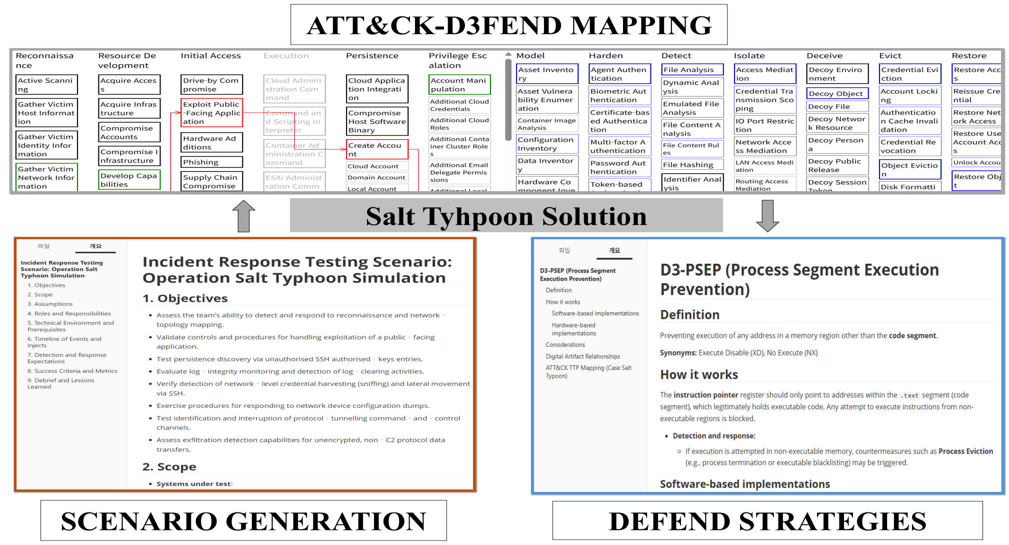

Data Preprocessing Tool
Model Training for Threat Scenarios
Expert Model of Threat Scenarios
Input Prompt for ASM
Open CTI Data
CTI Data Collection
Data Cleansing
Data Vectorization
Fragmented TI Dataset
TI_1 TI_2 TI_n
+
MITRE ATT&CK
$T_1, T_2, \dots, T_n$
AI Model
LLM_1
LLM_n
Threat Scenarios
T.S. − 1
Start
$T_1 \to T_4 \to T_9 \to T_{13} \to T_{45}$
End
T.S. − n
Start
$T_3 \to T_{11} \to T_{17} \to T_{22} \to T_{84}$
End
M.A. Framework
M.D3FEND Framework
T_1 T_4 T_9 T_{13} T_{45}
D_3 D_5 D_{11} D_6 D_{11}
D3FEND AI Model
D_1 D_2 D_3 D_4 D_n
LLM
Other Open Defense Techniques
Defense Description
TI_i : i^{th} Threat Intelligence
T_i : i^{th} Techniques
ASM : Attack Surface Management

Figure 1: Overview of the proposed Framework

3 Experiments

This section presents the procedure for extracting ATT&CK-based TTPs from the Salt Typhoon Group incidents and mapping them to D3FEND countermeasures to derive scenario-specific defensive strategies. Salt Typhoon is a threat actor supported by the PRC (People's Republic of China) government that has been active since at least 2019 and is known to be responsible for multiple intrusions into the network infrastructure of major telecommunications companies and ISPs (internet service providers) in the United States. Figure 2 is an example of a variant scenario generated based on the TIDs of the Salt Typhoon group. Corresponding countermeasures were mapped according to D3FEND tactics for the identified TIDs. The final report outputs include a list of actions related to the TIDs, together with each technique's D3FEND techniques. However, because CVE based vulnerability exploitation was not observed for the Salt Typhoon group, risk based mapping was not performed, and thus content related to CVSS and EPSS is not included.



Incident Response Testing Scenario: Operation Salt Typhoon Simulation

1. Objectives
2. Scope
3. Assumptions
4. Roles and Responsibilities
5. Technical Environment and Prerequisites
6. Timeline of Events and Injects
7. Detection and Response Expectations
8. Success Criteria and Metrics
9. Debrief and Lessons Learned

Incident Response Testing Scenario: Operation Salt Typhoon Simulation

1. Objectives

- Assess the team's ability to detect and respond to reconnaissance and network - topology mapping.
- Validate controls and procedures for handling exploitation of a public - facing application.
- Test persistence discovery via unauthorised SSH authorised - keys entries.
- Evaluate log - integrity monitoring and detection of log - clearing activities.
- Verify detection of network - level credential harvesting (sniffing) and lateral movement via SSH.
- Exercise procedures for responding to network device configuration dumps.
- Test identification and interruption of protocol - tunnelling command - and - control channels.
- Assess exfiltration detection capabilities for unencrypted, non - C2 protocol data transfers.

2. Scope

- **Systems under test:**

D3-PSEP (Process Segment Execution Prevention)
Definition
How it works
Software-based implementations
Hardware-based implementations
Considerations
Digital Artifact Relationships
ATT&CK TTP Mapping (Case Salt Typoon)

D3-PSEP (Process Segment Execution Prevention)

Definition

Preventing execution of any address in a memory region other than the **code segment**.

Synonyms: Execute Disable (XD), No Execute (NX)

How it works

The **instruction pointer** register should only point to addresses within the `.text` segment (code segment), which legitimately holds executable code. Any attempt to execute instructions from non-executable regions is blocked.

- **Detection and response:**
  - If execution is attempted in non-executable memory, countermeasures such as **Process Eviction** (e.g., process termination or executable blacklisting) may be triggered.

Software-based implementations

Figure 2: ATT&CK–D3FEND Mapping based Framework for Salt Typhoon

4 Conclusion

Consequently, using MITRE ATT&CK and D3FEND as axes, a practical procedure was established that systematically analyzes recent cyberattack cases and converts that analysis into an operational defensive summary report. By mapping the latest CTI to immediately actionable scenarios and response options, the proposed framework provides concise and reproducible grounds for proactive actions. At present, the framework is only partially automated, and full automation across all stages is in progress. A limitation is that scenario validation relies on a single LLM (GPT-4.5), so testing with diverse alternative models is required. In addition, because some TIDs lack associated CVEs and multiple defensive techniques are mapped to a single TID, we plan as future work to provide LLM-based summaries that condense numerous defensive actions into key actions.

Acknowledgement: This study was conducted as a research project commissioned by the Korean Association of Cybersecurity Studies(Project title : 'A Study on MITRE ATT&CK-Based Threat Analysis and D3FEND-Based Defense Strategies', Project period : 2025.04∼2025.11), his work was supported by the IITP(Institute of Information & Coummunications Technology Planning & Evaluation)-ITRC(Information Technology Research Center) grant funded by the Korea government(Ministry of Science and ICT) (IITP-2025-RS-2022-00164800), this work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. RS-2025-00252157, "Contrastive Learning-based Dark Web Criminal Profiling Research").

References

[1] Bloomberg News. Colonial pipeline paid hackers nearly $5 million in ransom. https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom, 2021. Accessed: 2025-09-02.

[2] Yuning Jiang et al. Mitre att&ck applications in cybersecurity and the way forward. *arXiv preprint*, 2025.

A Proactive Cyber Threat Response Framework Integrating Real-Time CTI with MITRE ATT&CK and D3FEND Mapping

Rino − Jo, Han − Bin Lee, Jihun Han, Woong − Kyo Jung, Jun − Yong Lee, Tae − Young Kang,
Byung − Il Kwak, Mee Lan Han, Jungmin Kang

Dept. of Cyber Security, Korea University

Abstract

- Proposes a framework that combines up-to-date CTI with MITRE ATT&CK and D3FEND to close the gap between threat awareness and operational response in real time
- Maps intelligence collected from OpenCTI to ATT&CK tactics and techniques, uses LLMs to generate tactic-sequenced variant scenarios, maps each technique to D3FEND, and delivers the results as a Defense Description

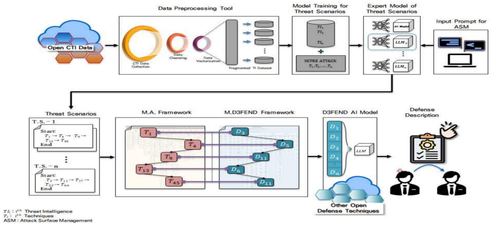
Introduction

- Recent attacks are growing more sophisticated and diverse, exemplified by the 2021 Colonial Pipeline ransomware shutdown and a 2024 deepfake-enabled phishing heist
- These cases necessitate swift, proactive countermeasures against the same or similar attacks

Methodology

Framework

- The proposed framework comprises CTI collection and preprocessing, MITRE ATT&CK based threat scenario generation, D3FEND-based defensive technique mapping, and the production of a Defense Description
- Collect objects from OpenCTI, build a Fragmented TI Dataset, and combine it with the latest ATT&CK to prepare data for scenario training and inference
- This data is injected as LLM based context to generate, for the input TI bundle T_I, a threat scenario in the form of a technique sequence with a tactical order $T_{i1} \rightarrow T_{i2} \rightarrow \cdots$
- Link each technique to D3FEND via MITRE's official mitigation associations and LLM-assisted inference
- Produce a Defense Description report including TIDs, recommended D3FEND techniques, supporting rationale, and preconditions, integrating with ASM when necessary

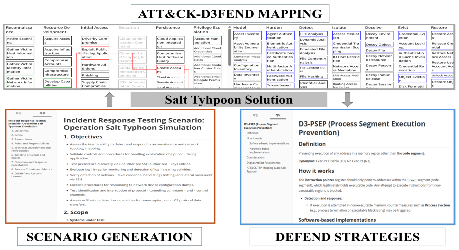


< Overview of the proposed Framework >

Experiments

Salt Typhoon Solution

- Extract ATT&CK based TTPs from the Salt Typhoon incidents, generate variant scenarios based on the identified TIDs, map them to D3FEND countermeasures, and derive scenario-specific defensive strategies
- Defense Description report includes a list of actions for each TID and the corresponding D3FEND techniques



Incident Response Testing Scenario: Operation Salt Typhoon Simulation

1. Objectives
2. Scope
3. Assumptions
4. Roles and Responsibilities
5. Technical Environment and Prerequisites
6. Timeline of Events and Injects
7. Detection and Response Expectations
8. Success Criteria and Metrics
9. Debrief and Lessons Learned

Incident Response Testing Scenario: Operation Salt Typhoon Simulation

1. Objectives

- Assess the team's ability to detect and respond to reconnaissance and network - topology mapping.
- Validate controls and procedures for handling exploitation of a public - facing application.
- Test persistence discovery via unauthorised SSH authorised - keys entries.
- Evaluate log - integrity monitoring and detection of log - clearing activities.
- Verify detection of network - level credential harvesting (sniffing) and lateral movement via SSH.
- Exercise procedures for responding to network device configuration dumps.
- Test identification and interruption of protocol - tunnelling command - and - control channels.
- Assess exfiltration detection capabilities for unencrypted, non - C2 protocol data transfers.

2. Scope

- **Systems under test:**

D3-PSEP (Process Segment Execution Prevention)

Definition
How it works
Software-based implementations
Hardware-based implementations
Considerations
Digital Artifact Relationships
ATT&CK TTP Mapping (Case Salt Typhoon)

D3-PSEP (Process Segment Execution Prevention)

Definition

Preventing execution of any address in a memory region other than the **code segment**.

Synonyms: Execute Disable (XD), No Execute (NX)

How it works

The **instruction pointer** register should only point to addresses within the `.text` segment (code segment), which legitimately holds executable code. Any attempt to execute instructions from non-executable regions is blocked.

- **Detection and response:**
  - If execution is attempted in non-executable memory, countermeasures such as **Process Eviction** (e.g., process termination or executable blacklisting) may be triggered.

Software-based implementations

< ATT&CK–D3FEND Mapping based Framework for Salt Typhoon >

Conclusion

- This study establishes a procedure that derives variant threat scenarios from recent cyberattack cases and translates them into an operations-ready defensive summary report
- The proposed framework provides concise, reproducible rationale for proactive action

Acknowledgements
This study was conducted as a research project commissioned by the Korean Association of Cybersecurity Studies(Project title : 'A Study on MITRE ATT\&CK-Based Threat Analysis and D3FEND-Based Defense Strategies', Project period : 2025.04~2025.11), his work was supported by the IITP(Institute of Information & Coummunications Technology Planning & Evaluation)-ITRC(Information Technology Research Center) grant funded by the Korea government(Ministry of Science and ICT) (IITP-2025-RS-2022-00164800), this work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. RS-2025-00252157, "Contrastive Learning-based Dark Web Criminal Profiling Research").