Paper Summary

<!--META_START-->

Title: TriCTI: an actionable cyber threat intelligence discovery system via trigger-enhanced neural networ

Authors: Jian Liu, Junjie Yan, Jun Jiang, Yitong He, Xuren Wang, Zhengwei Jiang, Peian Yang, Ning Li

DOI: https://doi.org/10.1186/s42400-022-00110-3

Year: 2022

Publication Type: Journal

Discipline/Domain: Cybersecurity

Subdomain/Topic: Cyber threat intelligence, NLP, threat detection

Eligibility: Eligible

Overall Relevance Score: 95

Operationalization Score: 92

Contains Definition of Actionability: Yes

Contains Systematic Features/Dimensions: Yes

Contains Explainability: Yes

Contains Interpretability: Yes

Contains Framework/Model: Yes

Operationalization Present: Yes

Primary Methodology: Mixed Methods (conceptual + experimental model implementation)

Study Context: Automated extraction of actionable CTI from unstructured cybersecurity reports using NLP

Geographic/Institutional Context: Chinese Academy of Sciences; Capital Normal University

Target Users/Stakeholders: Security operations centers (SOC), cybersecurity analysts, threat intelligence

Primary Contribution Type: Methodological framework and system development (TriCTI)

CL: Yes – clarity of campaign stage and IOC association explicitly tied to actionability (p.2)

CR: Yes – contextual relevance via mapping IOCs to campaign stages (p.2)

FE: Yes – feasibility demonstrated by operational system tested on 29k reports (p.1, p.12)

TI: Partial – system processes historical and near-real-time data, but not explicitly constrained by latency

EX: Yes – interpretability through “campaign triggers” enhancing classification explainability (p.2, p.6)

GA: Yes – goal alignment through prioritizing defense actions based on campaign stage severity (p.8–9)

Reason if Not Eligible: N/A

<!--META_END-->

Title:

TriCTI: an actionable cyber threat intelligence discovery system via trigger-enhanced neural network

Authors:

Jian Liu, Junjie Yan, Jun Jiang, Yitong He, Xuren Wang, Zhengwei Jiang, Peian Yang, Ning Li

DOI:

https://doi.org/10.1186/s42400-022-00110-3

Year:

2022

Publication Type:

Journal

Discipline/Domain:

Cybersecurity

Subdomain/Topic:

Cyber threat intelligence, NLP, threat detection

Contextual Background:

The paper addresses the challenge of extracting actionable cyber threat intelligence (CTI) from the vast a

Geographic/Institutional Context:

Institute of Information Engineering, Chinese Academy of Sciences; University of Chinese Academy of Sc

Target Users/Stakeholders:

Security operations centers (SOC), incident response teams, cybersecurity researchers.

Primary Methodology:

Mixed methods: conceptual framework design, NLP-based system architecture, experimental validation c

Primary Contribution Type:

Novel system (TriCTI) and methodology for discovering actionable CTI with enhanced interpretability.

General Summary of the Paper

The authors propose TriCTI, a trigger-enhanced neural network system for discovering actionable cyber t

---

Eligibility

Eligible for inclusion: **Yes**

How Actionability is Understood

Actionable CTI is defined as CTI that “conveys a richer context of IOCs by revealing their campaign stage

> “Actionable CTI can provide incident response teams with actionable insights and recommendations to

> “If actionable CTI is integrated into intrusion detection systems, SOC teams can take appropriate mitiga

---

What Makes Something Actionable

- Coupling IOCs with campaign stages for context.
- Providing interpretability for prioritization of threats.
- Supporting direct mitigation decisions aligned with attack phase.
- Being complete across all stages of the attack lifecycle.
- Accurate extraction to avoid false positives.

How Actionability is Achieved / Operationalized

- **Framework/Approach Name(s):** TriCTI (Trigger-enhanced Cyber Threat Intelligence discovery syste
- **Methods/Levers:** Campaign trigger annotation, IOC detection and filtering, BERT-based trigger vecto
- **Operational Steps / Workflow:** Data crawling → preprocessing (purification, segmentation, IOC fangi
- **Data & Measures:** 29,686 cybersecurity reports; annotated datasets DS-1 and DS-2; evaluation met
- **Implementation Context:** Applied to unstructured vendor reports spanning 2000–2021; verified using

> “The sooner the detection is done, the less loss the organization under attack will suffer” (p.8)

> “Applying actionable CTI to intrusion detection systems can guide security operators to make faster, be

---

Dimensions and Attributes of Actionability (Authors’ Perspective)

- **CL (Clarity):** Yes – clear association of IOCs to campaign stages is essential (p.2).
- **CR (Contextual Relevance):** Yes – mapping to campaign stages ensures relevance to defense conte
- **FE (Feasibility):** Yes – operationalized on large dataset with automation (p.1, p.12).
- **TI (Timeliness):** Partial – while timely response is stressed, the system is not explicitly real-time.
- **EX (Explainability):** Yes – campaign triggers improve interpretability (p.2, p.6).
- **GA (Goal Alignment):** Yes – enables prioritization according to severity of campaign stage (p.8–9).
- **Other Dimensions Named by Authors:** Completeness across all campaign stages; interpretability; re

---

Theoretical or Conceptual Foundations

- Cyber Kill Chain model (Hutchins et al., 2011) for campaign stage definitions.
- NLP concepts: BERT, CBERT augmentation, trigger-based attention mechanisms.

Indicators or Metrics for Actionability

- Campaign stage correctly assigned to IOC.
- Classification performance (Accuracy, F1 score).
- Coverage across all campaign stages.
- Verified maliciousness via VirusTotal relationships.

Barriers and Enablers to Actionability

- **Barriers:** Scarcity of annotated cybersecurity corpora; complexity of sentences with multiple stages;
- **Enablers:** Trigger-based explainability; data augmentation; automated large-scale processing; valida

---

Relation to Existing Literature

The paper critiques prior IOC extraction and threat action identification work for lacking campaign stage c

---

Summary

This paper presents TriCTI, an NLP-based, trigger-enhanced neural network framework for discovering a

---

Scores

- **Overall Relevance Score:** 95 – Strong, explicit conceptualization of actionability with comprehensive
- **Operationalization Score:** 92 – Detailed, step-by-step operationalization with system architecture, wo

---

Supporting Quotes from the Paper

- “[Actionable CTI] conveys a richer context of IOCs by revealing their campaign stages” (p.2)
- “SOC teams can take appropriate mitigation actions based on contextual information of the alerts” (p.2)
- “We introduce the ‘campaign trigger’… to improve the performance of the classification model” (p.1)
- “Applying actionable CTI to intrusion detection systems can guide security operators to make faster, bet

---

Actionability References to Other Papers

- Hutchins et al. (2011) – Cyber Kill Chain model.
- Yadav and Rao (2015) – Technical aspects of the cyber kill chain.
- Liao et al. (2016), Zhou et al. (2018), Long et al. (2019) – IOC extraction methods.
- Zhu and Dumitras (2018) – Campaign stage identification with rule-based approach.