A STIX Schema Design for Interoperable Feature Sharing Among AI Security Models*

Taehun Kim, and Hwankuk Kim†
Kookmin University, Seoul, South Korea
{hun010510, rinyfeel} @kookmin.ac.kr

Abstract

This study proposes an extension approach for consistently representing model metadata and detection context generated in AI-based security operations within the STIX framework. While preserving the fundamental structural consistency of STIX, we present three methods for structuring AI-related information. The proposed approach enhances the interoperability and reproducibility of AI detection results and facilitates the automation and sharing of detection rules. Future work will focus on validating the conformity of the proposed schema and contributing to the standardization process to strengthen the scalability and ecosystem integration of AI-based CTI.

KeyWord: STIX, CTI, AI-based Security Operations, AI-driven Cybersecurity Framework

1 Introduction & Background

With the increasing sophistication and diversification of cyberattacks, the importance of cyber threat intelligence (CTI) has become ever more pronounced. As security operations shift toward an AI-centric paradigm, there is a growing need for a systematic representation that enables the application and comparison of diverse AI detection options under identical conditions to identify threats, and that supports the creation and management of AI detection rules based on these results[1]. To address this need, this study proposes an extension approach that effectively integrates AI model information into STIX while preserving its fundamental structure.

STIX (Structured Threat Information Expression) is a standardized format designed to represent cyber threat information in a structured manner. It systematically describes both threat intelligence and observable data through various object types. The main components of STIX are classified into SDO, SCO, and SRO [2].

(SDO, STIX Domain Object) SDOs represent threat intelligence from a conceptual or analytical perspective. They describe higher-level concepts of cyber threats such as attack campaigns, threat actors, malware, and indicators. In other words, an SDO corresponds to a knowledge entity that explains malicious behaviors or attacker activities.

(SCO, STIX Cyber Observable Object) SCOs represent entities that can be directly observed in the real world. These include concrete observable elements such as files, IP addresses, URLs, domain

* Proceedings of the 9th International Conference on Mobile Internet Security (MobiSec'25), Article No. P-46, December 16-18, 2025, Sapporo, Japan.
† Corresponding author: Hwankuk Kim, Kookmin University, Seoul, South Korea, rinyfeel@kookmin.ac.kr

names, and hash values. For instance, an SCO may contain tangible information such as the attacker's IP address, the victim server's domain, or the hash of a malicious file.

(SRO, STIX Relationship Object) SROs define the relationships between objects or record the associations observed in specific incidents. For example, an SRO can describe a relation such as "a specific IP (SCO) was used in a particular campaign (SDO)", thereby expressing the structural linkage of threat activities.

2 Proposed Method

(AI-based Custom Property) The Custom Property approach adds new attributes to existing SDO or SCO objects, inserting the properties x_model_id, x_model_name, and x_model_score into an Indicator object to describe AI model information. This method is simple and highly compatible, but it has limitations when representing complex structures or numerous model-related details.

(AI-based Custom Object) The Custom Object approach creates new SDO or SCO object types not defined in the STIX standard by defining an x-ai-model object type and specifying fields such as model_id, model_name, model_version, score, and features_used. It is suitable for extending concepts that are difficult to express within the existing STIX structure and enables separate management of AI-based detection results and inter-model relationships.

(AI-based Custom Extension) The Custom Extension approach extends the attributes of existing SCOs to include AI-related information by adding x-ai-model-ext to the extensions of an SCO object and defining the fields model_name, model_version, input, and features_used. This method maintains compatibility with the STIX standard while enabling the linkage of AI analysis information at a concrete file/object level.

3 Conclusion

The method proposed in this study is significant in that it enables the structured representation of AI model metadata, detection results, and input features while maintaining the structural consistency of STIX. Through this approach, a foundation is established for comparing and utilizing various AI detection options within the same environment, as well as for automating and sharing AI detection rules. Future work will focus on validating the compatibility of the proposed extensions with the STIX standard framework and contributing to the standardization process to enhance the interoperability and scalability of AI-based cyber threat intelligence.

References

[1] M. Khayat, E. Barka, M. Adel Serhani, F. Sallabi, K. Shuaib and H. M. Khater. 2025. "Empowering Security Operation Center With Artificial Intelligence and Machine Learning—A Systematic Literature Review." In IEEE Access, vol. 13, pp. 19162-19197.

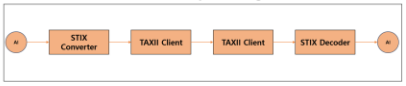
[2] Czekster, Ricardo M., Roberto Metere, and Charles Morisset. 2022. "Incorporating Cyber Threat Intelligence into Complex Cyber-Physical Systems: A STIX Model for Active Buildings" Applied Sciences 12, no. 10: 5005.

A STIX Schema Design for Interoperable Feature Sharing Among AI Security Models

ICSR Intelligent Cyber Security Research Lab
Taehun Kim* and Hwankuk Kim**
*Kookmin University, **Kookmin University

Introduction

With the increasing sophistication and diversification of cyberattacks, the importance of cyber threat intelligence (CTI) has become ever more pronounced. As security operations shift toward an AI-centric paradigm, there is a growing need for a systematic representation that enables the application and comparison of diverse AI detection options under identical conditions to identify threats, and that supports the creation and management of AI detection rules based on these results. To address this need, this study proposes an extension approach that effectively integrates AI model information into STIX while preserving its fundamental structure.



AI-based STIX Communication Architecture

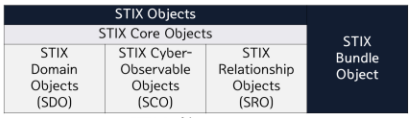
Background

STIX (Structured Threat Information Expression) is a standardized format designed to represent cyber threat information in a structured manner. It systematically describes both threat intelligence and observable data through various object types. The main components of STIX are classified into SDO, SCO, and SRO.

SDO An SDO represents threat intelligence from a conceptual and analytical perspective, describing higher-level entities such as Campaign, Threat Actor, Malware, and Indicator. In other words, it serves as a knowledge unit that explains malicious behaviors or attacker activities, enabling analysts to trace attack patterns and understand causal relationships among threat events.

SCO An SCO represents directly observable entities in the real world. It includes concrete and physical cyber elements such as File, IP Address, URL, Domain Name, and Hash. For example, it may contain evidence data such as an attacker's IP address, the victim server's domain name, or the hash value of a malicious file.

SRO An SRO defines the relationships and associations between SDOs and/or SCOs. For instance, it can describe relationships such as "a specific IP (SCO) was used in a particular campaign (SDO)" or "a specific malware (SDO) was distributed by a certain threat actor (SDO)."Through this structure, SROs enable the systematic representation of linkages, chains, and propagation paths among threat activities.



STIX Architecture

Proposed Method

AI-based Custom Property

The Custom Property approach directly adds AI-related attributes to existing STIX objects (e.g., Indicator).In this method, attributes such as x_model_id, x_model_name, and x_model_score are inserted into the Indicator object to record the identifier, name, and confidence score of the AI model used for detection. Limited expressiveness for representing complex model architectures, feature lists, and training configurations.

AI-based Custom Object

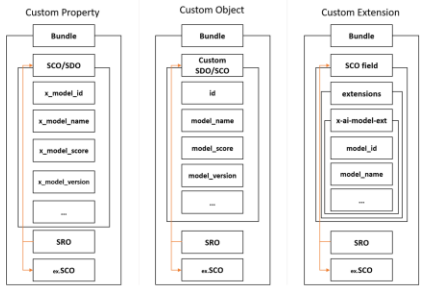
This approach creates a new object type not defined in the STIX standard, representing the AI model itself as an independent object. A new object type, x-ai-model, is defined and includes the following fields: model_id, model_name, model_version, score, features_used, and training_dataset. Particularly effective for multi-model operational environments, model version tracking, and structured performance comparison.

AI-based Custom Extension

This approach utilizes the extensions field of existing SCO objects (e.g., File, Network Traffic) to incorporate AI analysis information. For example, an extension named x-ai-model-ext can be defined within the File object, including fields such as model_name, model_version, input_vector, features_used, and score.

Proposed Method	Advantage	Application
AI-based Custom Property	Guarantees simple structure and high compatibility with existing STIX systems.	Suitable for recording the prediction results of a single AI model at the Indicator level.
AI-based Custom Object	Enables independent management of detailed AI model attributes and relationships among detection results.	Defines comparison relationships (e.g., related-to) between different AI models. Expresses linkages between AI models and detection results (e.g., Indicator, Malware).
AI-based Custom Extension	Maintains full compatibility with the STIX standard structure while enabling the integration of detailed file- or network-level analysis information.	Directly attach AI-based malware classification results to a file object. Combine with AI-driven anomaly detection results from network traffic logs.

Advantages & Applications of the Proposed Methods



Proposed Method Architecture

Conclusion

The method proposed in this study is significant in that it enables the structured representation of AI model metadata, detection results, and input features while maintaining the structural consistency of STIX. Through this approach, a foundation is established for comparing and utilizing various AI detection options within the same environment, as well as for automating and sharing AI detection rules. Future work will focus on validating the compatibility of the proposed extensions with the STIX standard framework and contributing to the standardization process to enhance the interoperability and scalability of AI-based cyber threat intelligence.