ScienceDirect

Computers & Security

Volume 120, September 2022, 102789

Threat classification model for security information event management focusing on model efficiency

Jae-yeol Kim [a], Hyuk-Yoon Kwon [b]

Show more

https://doi.org/10.1016/j.cose.2022.102789

Get rights and content

Abstract

As various types of network threats have increased recently, manual threat response by security analysts has become a limitation. To compensate for this, the importance of security information event management (SIEM), a response system that collects and analyzes threat events from security devices, has been emphasized. In general, SIEM has adopted a signature-based threat classification model that generates large volumes of false threat events and burdens the work of security analysts. To address this limitation of SIEM, research has attempted to develop an AI-based threat classification model. In particular, deep learning-based threat classification models are known to have high accuracy in classifying threats. In this study, we focused on the excessive overhead incurred in learning and classifying large sets of threat events using deep learning models, which becomes an overhead in actual SIEM operations. In this study, we selected representative deep-learning-based models for threat classification, such as CNN, LSTM, and GRU, based on the models used in previous studies. We then extend these models

considering the characteristics of actual threat events collected from a security operation center (SOC) environment. Specifically, CNN-static(2D) and LSTM were extended to use our own encoding method. CNN-static(1D) was developed to reduce the time for model learning and threat classification while minimizing the loss of accuracy compared to CNN-static(2D). GRU was first used for threat classification in this study. In this study, we aimed to identify the most effective deep learning model for SIEM in terms of both threat classification accuracy and learning and classification efficiency. To consider real workloads, we use 2.6 million threat events collected from a representative security vendor in South Korea, and manually annotated by security experts. First, in terms of threat classification accuracy, the LSTM model has the highest F1-score, but all the models show high accuracy between 94.07% and 95.11% in terms of recall, which is the most important metric at SOC. Second, in terms of model learning and classification times, CNN-static(1D) significantly outperformed the other models. To validate the models in the actual SOC environment, we also present two cost-based scenarios to estimate the cost of the models for specific scenarios: the cost of rebuilding the model to respond to zero-day attacks, and the cost of classifying threats in the actual SOC environment. We show that CNN-static(1D) is the most cost-effective model for both scenarios.

Introduction

Security information event management (SIEM) can collect and analyze security events that occur in network or PC environments (Sekharan and Kandasamy, 2017). SIEM monitors real-time threats by storing a large number of events collected from multiple security devices and analyzing each event and the connection between them (Sekharan and Kandasamy, 2017). SIEM analyzes threat events to detect and prevent intrusions on end-user PCs, servers, network devices, and firewalls. Therefore, SIEM is recognized and widely used as an effective control system. For this reason, many companies and government agencies operate security operation centers (SOCs) based on SIEMs. SOCs classify the SIEM-generated events by threat type and respond to each type. Each security device generates events and sends them to SIEM according to predefined rules. Then, SIEM defines integrated rules that are presented differently in various security devices to detect threat events, called tickets (or incidents), that need to be responded to (Scarfone and Mell, 2007). In SIEM, the predefined signatures are often used to define threat events for threat classification. However, since signature-based classification attempts to cover a wide range of threat events to minimize false negatives

(i.e., actual attack events, but classified as normal events), the number of false positives (i.e., actual normal events, but classified as attack events) usually increases. Since the number of tickets detected by SIEM is quite large, security analysts cannot respond to all of them. According to a previous study by C.Zhongetal.(2018), security analysts can only respond to about 29% of tickets detected by SIEM, and 40% of the responding tickets are false positives.

To build effective deep learning-based classification models, we need a large number of events annotated by security experts. Even if deep learning-based threat classification models usually work well, they require a long time to train and update the classification model with new threat events, making it difficult to respond to threat events in real time. In reality, these delayed responses to new threat events cause SOC to fail in developing successive real-time defense systems.

Recently, there have been some research efforts on threat classification models based on artificial neural network models to reduce false positives in the signature-based SIEM model (C.Zhongetal., 2018). A previously conducted study (Leeetal., 2019), validated the effectiveness of the neural network models by applying SVM, K-NN, naïve Bayes, decision tree, FNN, CNN, and LSTM models to threat classification. Another study (Naseeretal., 2018) showed a high classification accuracy (i.e., about 97%) of deep learning-based threat classification models, such as LSTM and deep convolutional neural network (DCNN). In addition to threat classification accuracy, in this study, we emphasize the need for model efficiency in terms of model learning and threat classification.

- **Model learning**: The process of learning and rebuilding the threat classification model is necessary to initially build the SIEM classification model and to respond to new cyberattacks such as zero-day attacks. Therefore, fast learning and updating of threat classification models are critical to building successful SOC defense systems. Therefore, we need to consider the quick learning time of the model as crucial as model accuracy.

- **Threat classification**: We must immediately capture all threat events generated by security devices. Otherwise, target systems may be vulnerable to threats. In practice, threat classification can be performed on environments using PCs or servers that cannot use high-performance processor units such as GPUs, which are required to learn the model. Therefore, we need a classification model that supports fast classification even in environments that use only CPUs.

In this study, we sought to identify the most effective deep learning model for SIEM, both in terms of threat classification accuracy and learning and classification efficiency. To consider real workloads, we use 2.6 million threat events collected from a representative security vendor in South Korea for one year and manually annotated by security experts. The contributions of this study can be summarized as follows:

We selected representative deep learning-based threat classification models, such as CNN, LSTM, and GRU, based on the models used in previous studies. We then extend these models based on our own encoding method, taking into account the characteristics of threat events in actual datasets collected from a SOC operational environment. Specifically, CNN-static(2D) and LSTM have been extended based on previous studies on our encoding method. We also present new classification models that focus on model efficiency. Specifically, CNN-static(1D) was developed to reduce the time for model learning and threat classification while minimizing the loss of accuracy compared to CNN-static(2D). GRU was first used for threat classification in this study.

We evaluated the performance of the threat classification models using real datasets. First, LSTM shows the highest F1-score, but all the models show high accuracy ranging from 94.07 to 95.11% in terms of recall, which is the most important metric in the SOC operation. Second, in terms of the model learning time, CNN-static(1D) is the fastest at 3346s, while LSTM is the slowest at 10,898s. Third, when using CPUs to classify 10,000 events, CNN-static(1D) is the fastest at 5.1s, while both LSTM and CNN-static(2D) were the slowest at 20.8s. In addition, when using GPUs, CNN-static(1D) are the fastest at 1.2s, and GRU is the slowest at 20.4s.

To validate the models in real-world environments, we present cost models to estimate their cost based on the scenarios in terms of 1) model update time for zero-day attacks, and 2) threat classification. For the former, we show that CNN-static (1D) is 2.26 to 2.79 times faster than the other methods. For the second method, CNN-static (1D) is also the

least expensive compared to the other methods by a factor of 3.4 to 16.1 times.

The remainder of this paper is organized as follows. In Section2, we describe related work. In Section3, we explain the background of this study. In Section4, we explain the datasets collected from the actual SOC environment. In Section5, we present the deep learning models for threat classification. In Section6, we explain the experimental results. In Section7, we present the scenario-based cost models of the deep learning models used. In Section8, we conclude the paper.

Section snippets

Related work

In this section, we describe previous studies that have used neural network-based models to classify and detect threats. We classify previous studies for SIEM into the following categories: 1) large-scale event data management (ElArass etal.2019; R.Andradeetal., 2018; Cinqueetal., 2021), 2) signature-based threat detection (B.D.Bryantetal., 2020; Eswaranetal., 2021), and 3) machine learning (ML)-based threat detection (Kim., 2014; Leeetal., 2019; Naseeretal., al.,2018; …

SIEM and SOC

In this section, we describe the components of the SIEM-based security system for SOC and their tasks. We also present the commercial products for SIEM.

Fig1 shows the overall procedure of SIEM based on signature-based rules, because it is a widely used architecture. It comprises the following steps: (a) threat event collection, (b) threat analysis and detection, and (c) response to the threat. In Step (a), we collect the threat events from security devices such as IPS and WAF. In Step (b), …

Datasets

In this section, we describe the real datasets collected by a security vendor in South Korea, over one year. In Section4.1, we present the labeling of the datasets. In Section4.2, we present our data encoding method. …

Threat classification models

In this study, we present four deep learning-based models for threat classification to conduct comparative experiments on threat classification accuracy, learning and classification times, as described in Table5. …

Performance evaluation

In this section, we measure the accuracy, learning, and classification times of four deep learning models: 1) CNN-static(2D), 2) CNN-static(1D), 3) LSTM, and 4) GRU. …

COST models based on soc operation scenarios

In this section, we define two operation scenarios at SOC to respond to threat events and estimate the cost of the models for these scenarios. In Section7.1, we introduce a model-building scenario for responding to zero-day attacks and present the cost model for it. In Section7.2, we present a scenario for constructing the threat classification system in SOC and present its cost model. These are representative scenarios for demonstrating the efficiency of deep learning models for threat …

Conclusions and discussion

In this study, we focused on the excessive overhead incurred in learning and classifying large amounts of threat events with deep learning models, which becomes the overhead in the actual SIEM operations. We selected representative deep learning-based models for threat classification, such as CNN, LSTM, and GRU, based on the models used in previous studies. We then extended these models based on our own encoding method, considering the characteristics of threat events in actual datasets …

CRediT authorship contribution statement

Jae-yeol Kim: Conceptualization, Methodology, Software, Validation, Investigation, Data curation, Visualization, Writing – original draft, Writing – review & editing. **Hyuk-Yoon Kwon:** Conceptualization, Methodology, Investigation, Writing – review & editing, Supervision, Project administration, Funding acquisition. …

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper. …

Acknowledgments

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2022R1F1A1067008). …

KIM JAE-YEOL received the M.S degree in engineering from Korea University in 2017. Since 2020, he has been studying as a Ph.D. student at the Graduate school of Public Policy and Information Technology (SeoulTech). His-main research areas of interest are machine learning, attack event analysis, and cyberattack defense technology. …

…

…

Recommended articles

References (60)

B.D. Bryant *et al.*

Improving SIEM alert metadata aggregation with a novel kill-chain based classification model

Comput. Security (2020)

M. Cinque *et al.*

A graph-based approach to detect unexplained sequences in a log

Expert Syst. Appl. (2021)

S. Eswaran *et al.*
A threshold-based, real-time analysis in early detection of endpoint anomalies using SIEM expertise
Network Security (2021)

N. Hubballi *et al.*
False alarm minimization techniques in signature-based intrusion detection systems: a survey
Comput. Commun. (2014)

H. Liu *et al.*
CNN and RNN based payload classification methods for attack detection
Knowl Based Syst (2019)

P. Radoglou-Grammatikis *et al.*
Spear siem: a security information and event management system for the smart grid
Computer Networks (2021)

N. Zahadat *et al.*
BYOD security engineering: a framework and its analysis
Comput. Security (2015)

S.A. Alharbi
A qualitative study on security operations centers in saudi arabia: challenges and research directions
J. Theor. Appl. Inf. Technol. (2020)

R. Andrade *et al.*
Enhancing intelligence SOC with big data tools

T. Ban *et al.*
Combat security alert fatigue with AI-assisted techniques
Cyber Security Experimentation and Test Workshop(2021)

View more references

Cited by (16)

Detecting cyberthreats in Metaverse learning platforms using an explainable DNN

2024, Internet of Things (Netherlands)

> *Citation Excerpt :*
>
> ...To mitigate prevalent cyberthreats and high false alarm rates, industry, and academic researchers have employed artificial intelligence (AI)-based network intrusion detection systems (NIDS) to effectively monitor and detect anomalous cyber-activities from benign activities in real-time [25]. An effective Metaverse cybersecurity framework is the ISO/IEC 27001 framework that offers an effective guideline for security event and incident management (SIEM) [26], offering effective monitoring and detection of anonymous network traffic behavior. Robust SIEM postures today adopt both machine learning (ML) and deep learning (DL) techniques to categorize and detect various kinds of network traffic [27]....

Show abstract

Self-Training of Cyber-Threat Classification Model With Threat-Payload Centric Augmentation ↗

2024, IEEE Transactions on Industrial Informatics

An Analysis of Key Tools for Detecting Cross-Site Scripting Attacks on Web-Based Systems ↗

2024, Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST

Assessing the Challenges Faced by Security Operations Centres (SOC) ↗

2024, Lecture Notes in Networks and Systems

Implementing Data Exfiltration Defense in Situ: A Survey of Countermeasures and Human Involvement ↗

2023, ACM Computing Surveys

A method for insider threat assessment by modeling the internal employee interactions ↗

2023, International Journal of Information Security

View all citing articles on Scopus ↗

KIM JAE-YEOL received the M.S degree in engineering from Korea University in 2017. Since 2020, he has been studying as a Ph.D. student at the Graduate school of Public Policy and Information Technology (SeoulTech). His-main research areas of interest are machine learning, attack event analysis, and cyberattack defense technology.

HYUK-YOON KWON received the M.S. degree in computer science from Korea Advanced Institute of Science and Technology (KAIST) in 2007, and the Ph.D. degree in computer science from KAIST in 2013. Currently, he is an associate professor at Department of Industrial Engineering, Seoul National University of Science and Technology (SeoulTech). His-research interests include Data-Driven AI, big data management, distributed and clouding computing, databases, machine learning, and Web crawler.

View full text