Conference Paper Title*

*Note: Sub-titles are not captured in Xplore and should not be used

1st Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

2nd Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

3rd Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

4th Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

5th Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

6th Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

Abstract—This document is a model and instructions for LaTeX. This and the IEEEtran.cls file define the components of your paper [title, text, heads, etc.]. *CRITICAL: Do Not Use Symbols, Special Characters, Footnotes, or Math in Paper Title or Abstract.

Index Terms—component, formatting, style, styling, insert

I. Introduction

As network attacks become increasingly sophisticated and diversified, traditional security measures struggle to comprehensively address emerging threats. In response, the development of an intelligent detection tool that offers a deep and comprehensive perspective has become an urgent need in the field of cybersecurity. The tool introduced in this paper is designed and developed to meet this requirement. It aims to create a multi-layer network threat graph by analyzing network traffic from endpoint devices, event logs from intrusion detection systems (NIDS), and system logs from monitoring devices, providing a holistic view of network security status. This design enables security analysts to understand the security condition of networks from multiple dimensions, thereby more effectively identifying and responding to potential security threats.

The core challenge addressed by the intelligent detection tool lies in utilizing advanced artificial intelligence technologies for deep analysis of vast amounts of network data. This includes employing machine learning algorithms to differentiate abnormal network packets, identify hosts with anomalous behaviors, and analyze clusters of such behaviors. These technologies allow the tool not only to detect known security threats but also to identify unknown or covert threats that traditional security solutions might overlook.

Moreover, the intelligent detection tool presents complex analysis results in a multi-layered, visualized form. This multi-layer threat graph not only shows the connections between nodes in the network but also highlights abnormal events, hosts with unusual behaviors, and the distribution of these abnormal clusters. Such visualization provides an intuitive and easy-to-understand means for security teams to quickly grasp the overall security situation of the network and identify patterns of vulnerabilities and attack behaviors. Additionally, the multi-layer threat graph offers various event entry points, allowing security analysts to analyze and assess from multiple perspectives, whether tracking specific security events, analyzing overall network communication behavior patterns, or even the attack propagation paths of malicious behaviors. This tool provides rich information and deep insights, revealing the structure and characteristics of abnormal network activities, assisting security teams in discovering potential attack paths, and timely adjusting and optimizing network security strategies.

This report focuses on introducing and explaining the design, development, and implementation of the intelligent detection tool, aiming to provide organizations with a comprehensive view of network security status through a multi-layer network threat graph. This tool combines the latest artificial intelligence technologies, including machine learning and deep learning algorithms, as well as big data analytics techniques, to conduct in-depth analysis of data collected from various sources. The report will cover key areas and technologies such as data preprocessing, AI analysis techniques, and the generation and visualization of multi-layer network threat graphs, showcasing the development process, implementation strategy, and practical benefits of the tool. This provides readers with a clear understanding and application framework for leveraging multilayer threat graph detection techniques for

Identify applicable funding agency here. If none, delete this.

correlation and risk assessment of heterogeneous data.

II. Related Work

This document is a model and instructions for LaTeX. Please observe the conference page limits. Test

III. System Architecture

A. A1

B. A2

C. A3

IV. Experiments

A. Introduction

In this section, we introduce our experiments comparing our proposed method to baseline approaches. We focus on identifying and detecting groups of attacking behavior through the analysis of network traffic, including encrypted traffic and untrusted services. We evaluate these in the context of hybrid short-term/long-term scenarios and multiple attacking steps.

B. Experimental Setup

Details on the datasets used and the parameters set for our experiments are introduced here. We employ the CICIDS2017 dataset and real-world data collected from over 700 hosts of an online game service provider. The setup includes the development environment (DeepLog, Hypervision, Python integration) on VMWare with 64GB RAM and a 24-core Intel processor.

C. Dataset and Evaluation Metrics

To evaluate the performance of our intrusion detection system, we employ the following metrics:

- Accuracy: Measures the overall effectiveness of the system in correctly identifying both normal and malicious activities.
- Precision and Recall: Precision quantifies the accuracy of positive predictions, while recall (or sensitivity) assesses the system's ability to detect all relevant instances. High recall is essential in security contexts to minimize missed attacks.
- F1-Score: The harmonic mean of precision and recall, useful in situations where attack instances are much rarer than normal behavior, typical of intrusion detection scenarios.

For our analysis, we utilize the CICIDS2017 dataset, a widely recognized benchmark that simulates modern network traffic scenarios, including various types of attacks. This dataset is crucial for testing the effectiveness of our proposed method. Additionally, we incorporate real-world data collected from corporate network security logs to ensure our method's robustness and applicability across both real and synthetic scenarios.

D. Testbed Configuration

Our testbed features "HyperVision," a state-of-the-art detection platform designed for real-time analysis of network flows. HyperVision excels in detecting encrypted malicious traffic by identifying abnormal interaction patterns, which are starkly different from those observed in benign flows.

Focus Areas of HyperVision:

- Inside Network Detection and Response (NDR): Emphasizes the detection of lateral movements within the network, identifying early signs of infiltration.
- Outside Network Detection and Response (NDR): Targets rapid identification of abnormal protocols and peer-to-peer communications at the network's periphery, crucial for early threat mitigation.
- Abnormal Protocol Connections: Focuses on detecting unusual protocol use that may indicate covert channels or unauthorized data exfiltration.

Utilizing both CICIDS2017 and CICIDS2018 datasets, HyperVision is extensively tested under various encrypted traffic scenarios to fine-tune its ability to distinguish between normal and malicious activities. These datasets provide a comprehensive range of attack simulations essential for robust system evaluation.

Performance Metrics Evaluated:

- Precision and Recall: Critical for assessing HyperVision's effectiveness, where high precision minimizes false positives and high recall ensures no threats are overlooked.
- Adaptability and Real-Time Response: The testbed assesses HyperVision's adaptability to new threats and its performance under real-time conditions, ensuring dynamic application of detection algorithms and responsiveness to sudden traffic pattern changes.

By integrating these elements, HyperVision is thoroughly evaluated for its capability to detect a wide array of encrypted and malicious traffic, ensuring comprehensive network security coverage both internally and externally. The focus on abnormal protocol connections, combined with precise datasets, enables HyperVision to achieve high precision and recall in its detection capabilities.

E. Results

This subsection details the experimental results. It includes data on precision, recall, and f-measure for both the detection of abnormal protocols and the hosts risk assessment. The effectiveness of the DeepLog system for event anomaly detection is discussed, supported by real case statistics (e.g., 20 out of 3 hosts were found compromised).

F. Effectiveness Analysis

- Analysis of network abnormal behavior detection across 8 categories using the CICIDS2017 dataset and real-case scenarios (RDP/P2P). - Sensitivity analysis for tuning parameters. - End-point event anomaly detection in host systems, with results presented in tables and figures.

G. Deep Threat Analysis

This subsection explores the deep threat graph methodology, detailing high-level attack steps and root causes. A qualitative analysis conducted by inviting five domain experts to evaluate the system is also included.

H. Efficiency Analysis and Case Studies

Here, we discuss the efficiency of our approach with specific case studies on APT29 and APT41.

I. Discussion

This final subsection synthesizes the findings, discussing their implications for cybersecurity and threat hunting, and suggesting directions for future research.

V. Conclusions

References

[1] G. Eason, B. Noble, and I. N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955.

[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[3] I. S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[4] K. Elissa, “Title of paper if known,” unpublished.

[5] R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.

[6] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[7] M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.

IEEE conference templates contain guidance text for composing and formatting conference papers. Please ensure that all template text is removed from your conference paper prior to submission to the conference. Failure to remove the template text from your paper may result in your paper not being published.