Leveraging Multilayer Threat Graph Detection Techniques for Correlation and Risk Assessment

1st Eric
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

Falcon Wang
ATD
WNC
Hsinchu, Taiwan
falcon.wang@wnc.com.tw

Eric Mao
ATD
WNC
Hsinchu, Taiwan
eric.mao@wnc.com.tw

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 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

In this section, we compare our proposed method to other baseline approaches, and illustrate the experimental result to justify our proposed method. As our goal is to identify and detect the groups of attacking behavior, all the experiments are designed to answer the question: When identifying the different intensions of intrusion behavior, how effective is it to identify the anomaly sequences (network traffic identify abnormal protocol that might be encrypted traffic or untrusted services....), especially in terms of hybrid short-term/long-term, multiple attacking steps? The applied data and the parameters for our experiments are in- troduced in Sec. IV-A, followed by the experimental results for the datasets in Sec. 4.2.

A. Dataset and Evaluation Metrics

In our analysis, we use a CICIDS2017 dataset public benchmark[1] and real world data collected from online game service provider around 700+ hosts.

Development (deeplog), hyvervision, python integration, VMWare 64GB, 24 core, intel, virtual mahcines

testbed

(1) hypervision: emphasize inside NDR (lateral movement), outside NDR (fast detection abnormal protocol p2p...) CICIDS2017/2018, abnormal protocol connection precision/recall/f-measure inside outside precision/recall precision/recall .....

(2) hosts risk assessment (IDS events) end point event anomaly detection (syslog) wazhu + deeplog(syslog) + deeplog(IDS event) How effectiveness of deeplog for event anomaly detection? True 20 3 compromised how effectiveness of assessing host risk level...... precision/recall precision/recall

(3) deep threat graph deep threat graph attack scenario, high-level attack steps, root cause... qualitative analysis. We might invite 5 domain experts to evaluate...

B. Effectiveness Analysis

(1) network abnormal behavior detection evaluation 8 categories real case CICIDS2017 + RDP/P2P

sensitive analysis (tuning parameters, k,)

(2) hosts risk assessment (IDS events) end point event anomaly detection (syslog) IDS host Precision/Recall risk score is high, actually is attack -> recall is good risk score is low, actually is attack -> precision is not good Table/Figure

host event normal behavior ? host ? time interval attack detected O x host x time attack detected X CICIDS2017 200 hosts 20 attacks records, real data?

(3) deep threat graph questionnaire

C. Efficiency Analysis/case study APT29, APT41

D. Discussion

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.

[1] ”CICIDS2017: https://www.unb.ca/cic/datasets/ids-2017.html”