Conferences > 2024 21st International Bhurb...

Anomaly Detection in HTTP Logs: Leveraging Machine Learning for Uncovering Anomalous Traffic Patterns with SIEM Integration

Publisher: IEEE Cite This PDF

Waqas Ahmad ; Muhammad Faisal Amjad **All Authors**

68
Full
Text Views

Abstract

Document Sections

I. Introduction

II. Proposed Solution

III. Results and Findings

IV. Conclusions and Future Work

Authors

Figures

References

Keywords

Metrics

More Like This

Abstract:
Network traffic continuously rises, and network services become increasingly more complex and vulnerable. Intrusion detection systems are employed to safeguard these networks. Signature-based intrusion detection cannot detect new attacks, so anomaly detection is necessary. Also, most of the traditional security information and event management (SIEM) doesn't have any live dataset creation or anomalous data log detection. In this paper, we propose a framework for detecting anomalies in Hypertext Transfer Protocol (HTTP) logs, enabling fast detection of anomalies, visualization of network traffic, and integration with SIEM solutions. This solution gets HTTP logs from the network and preprocesses them. Then, the solution checks the traffic for anomaly detection by applying the Isolation Forest algorithm using unsupervised learning. Later, we will then explore those anomalies with clustering using the K-means method. The proposed solution uses no predefined dataset file. But, it trains on the live data logs, where the user checks for any anomalous data logs within a given timestamp. The logs from this specified timestamp serve as the dataset for the model's training. The solutions are on live network HTTP logs, but in this paper, we are using this solution on a test network where we have 153 logs, of which 32 are declared anomalous by our proposed solution and after that the clustering on those anomalous data logs were applied. Finally, the results are sent to the SIEM solution, which visualizes the network and the anomalous traffic. Besides this, the solution is quick to detect intrusion attempts. This method is significant in the sense, that because it contributes to proactive cybersecurity strategies specifically designed to meet the requirements of Security Operations Center (SOC) analysts and threat-hunting teams.

Published in: 2024 21st International Bhurban Conference on Applied Sciences and Technology (IBCAST)

Date of Conference: 20-23 August 2024

Date Added to IEEE *Xplore*: 18 February 2025

▸ **ISBN Information:**

⌄ **ISSN Information:**

DOI: 10.1109/IBCAST61650.2024.10877256

Publisher: IEEE

Conference Location: Murree, Pakistan

Sign in to Continue Reading

Authors ⌄

Figures ⌄

References ⌄

Keywords ⌄

Metrics ⌄

Back to Results

IEEE Personal Account

CHANGE USERNAME/ PASSWORD

Purchase Details

PAYMENT OPTIONS

VIEW PURCHASED DOCUMENTS

Profile Information

COMMUNICATIONS PREFERENCES

PROFESSION AND EDUCATION

TECHNICAL INTERESTS

Need Help?

US & CANADA: +1 800 678 4333

WORLDWIDE: +1 732 981 0060

CONTACT & SUPPORT

Follow

About IEEE *Xplore* | Contact Us | Help | Accessibility | Terms of Use | Nondiscrimination Policy | IEEE Ethics Reporting | Sitemap | IEEE Privacy Policy