# A SIEM Study and Enterprise-Oriented ELK Prototype

Mai Trung Đức
Thai Nguyen University of Information and Communication Technology
Thai Nguyen University, Thai Nguyen, Vietnam
student544@ictu.edu.vn

***Abstract*—This undergraduate thesis investigates security information and event management in an enterprise context. Security teams need to collect and inspect events from different systems to recognize suspicious activity. The author reviews SIEM concepts and constructs a test environment using the ELK stack and Suricata. The report describes log collection, processing, storage, visualization, and alert-oriented examination of network events. The source describes a laboratory SIEM setup and selected event-monitoring views. It supports a technical demonstration of integration, but does not verify company-wide deployment, a particular incident-reduction rate, or large-scale throughput claims. A small test system does not establish coverage of every enterprise source, reliable detection at scale, or the quality of investigation decisions. Alert tuning and data governance remain important. The contribution is a documented student study or prototype whose stated scope can guide further testing.**

***Index Terms*—SIEM, ELK, Suricata, security monitoring**

## I. Introduction

Security teams need to collect and inspect events from different systems to recognize suspicious activity. This thesis investigates security information and event management in an enterprise context. It begins from a practical engineering need and explains the technologies and workflow chosen for the case. The objective is to document a student implementation or comparative investigation, together with the evidence available in the manuscript. Broader operational or economic effects require separate measurements and are not assumed from the existence of a prototype [1]. Earlier ICTU student work on related designs is included here for context [2], [3]. Related published studies provide context for the subject and methods [4], [5], [6], [7], [8], [9], [10]. These contextual works were selected for this English summary; they are not asserted to appear in the original thesis bibliography.

## II. Methods

The author reviews SIEM concepts and constructs a test environment using the ELK stack and Suricata. The report describes log collection, processing, storage, visualization, and alert-oriented examination of network events. The source is summarized through its stated design, implementation material, examples, and conclusion. Features shown in the manuscript are distinguished from proposals for later development. This review does not add a new experiment, fill missing measurements with estimates, or treat a planned capability as an observed result. The source thesis remains the provenance for the reported work [1].

Supervisor: Nguyễn Anh Chuyên, Thai Nguyen University of Information and Communication Technology (nachuyen@ictu.edu.vn).

## III. Results

The source describes a laboratory SIEM setup and selected event-monitoring views. It supports a technical demonstration of integration, but does not verify company-wide deployment, a particular incident-reduction rate, or large-scale throughput claims. The report's screens, configurations, examples, or measurements constitute the evidence for this summary. A capability described only as a design intention is not counted as a validated operational outcome. No additional performance, adoption, financial, or safety figure has been introduced here. The result is interpreted within the scope of the student's documented setup [1].

## IV. Discussion

A small test system does not establish coverage of every enterprise source, reliable detection at scale, or the quality of investigation decisions. Alert tuning and data governance remain important. Further work could add more log sources, test known attack traces, report false positives and detection delay, and validate retention and access controls. These limitations affect how the evidence should be read. The current manuscript can support understanding of the design and reported demonstration, while independent tests would be needed for stronger claims. Any later deployment should document its environment and separate observed outcomes from intended benefits [1].

## V. Conclusion

The thesis documents security information and event management in an enterprise context. The source describes a laboratory SIEM setup and selected event-monitoring views. It supports a technical demonstration of integration, but does not verify company-wide deployment, a particular incident-reduction rate, or large-scale throughput claims. A small test system does not establish coverage of every enterprise source, reliable detection at scale, or the quality of investigation decisions. Alert tuning and data governance remain important. Further work could add more log sources, test known attack

traces, report false positives and detection delay, and validate retention and access controls. Accordingly, the present contribution is a source-grounded account of the student work and its tested or illustrated scope. Claims about broader effectiveness should be assessed in later work using explicit evaluation conditions [1].

## References


[1] Mai Trung Đức, ”A SIEM Study and Enterprise-Oriented ELK Prototype,” internal undergraduate thesis (original in Vietnamese), Thai Nguyen University of Information and Communication Technology, 2024.

[2] ICTU Student 102, ”Development of an Intrusion Detection System Based on Data Mining Techniques,” internal undergraduate thesis, Thai Nguyen University of Information and Communication Technology, 2009.

[3] ICTU Student 90, ”SNMP Protocol and Its Application in Remote Network Management,” internal undergraduate thesis, Thai Nguyen University of Information and Communication Technology, 2009.

[4] Fahri Choirul Anam et al., ”Implementation of Security Information and Event Management (SIEM) for Monitoring IT Assets Using Alienvault OSSIM (Case Study: Udayana University Information Resources Unit),” JITTER : Jurnal Ilmiah Teknologi dan Komputer, 2023. doi:10.24843/jtrti.2023.v04.i03.p03.

[5] Bandr Siraj Fakiha, ”Effectiveness of Security Incident Event Management (SIEM) System for Cyber Security Situation Awareness,” Indian Journal of Forensic Medicine & Toxicology, 2020. doi:10.37506/ijfmt.v14i4.11587.

[6] ShivaDutt Jangampeta et al., ”Impact of SIEM on Compliance: Achieving Security and Adherence Simultaneously,” Turkish Journal of Computer and Mathematics Education (TURCOMAT), 2020. doi:10.61841/turcomat.v11i1.14413.

[7] S. O. Gakhov, ”Analysis of methods for detecting events and incidents of information and cyber security by SIEM systems,” Modern information security, 2018. doi:10.31673/2409-7292.2018.040611.

[8] Liudmyla Savytska et al., ”METHOD AND MEANS OF SECURITY MONITORING IN A COMPUTER NETWORK BY SIEM MEANS,” Information technology and computer engineering, 2023. doi:10.31649/1999-9941-2023-58-3-22-32.

[9] Akhigbe-mudu Thursday Ehis, ”Optimization of Security Information and Event Management (SIEM) Infrastructures, and Events Correlation/Regression Analysis for Optimal Cyber Security Posture,” Archives of Advanced Engineering Science, 2023. doi:10.47852/bonviewaaes32021068.

[10] Aamna Tariq et al., ”Open source SIEM solutions for an enterprise,” Information & Computer Security, 2022. doi:10.1108/ics-09-2021-0146.