AN ENHANCED NEXT GENERATION SECURITY OPERATION CENTER FRAMEWORK FOR INFORMATION SYSTEM SECURITY MANAGEMENT

YAU TI DUN

MASTER OF SCIENCE
UNIVERSITI MALAYSIA PAHANG

اونيۏرسيتي مليسيا ڤهڠ
UNIVERSITI MALAYSIA PAHANG

SUPERVISOR’S DECLARATION

I hereby declare that I have checked this thesis and in my opinion, this thesis is adequate in terms of scope and quality for the award of the degree of Master of Science.

TS. DR. MOHD FAIZAL BIN AB RAZAK
HEAD OF PROGRAM (CYBER SECURITY)
FACULTY OF COMPUTING
UNIVERSITI MALAYSIA PAHANG
26600 PEKAN, PAHANG DARUL MAKMUR
TEL : 09-431 5589

(Supervisor’s Signature)

Full Name : TS. DR MOHD FAIZAL BIN AB RAZAK
Position : HEAD OF PROGRAM (CYBER SECURITY)
Date : 3 AUGUST 2023

اونيۏرسيتي مليسيا ڤهڠ
UNIVERSITI MALAYSIA PAHANG

STUDENT’S DECLARATION

I hereby declare that the work in this thesis is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at UNIVERSITI MALAYSIA PAHANG or other institutions.

PROFESSIONAL TECHNOLOGIST
MBOT
PT19090035
Ts. Yau Ti Dun
(Alan)
CYBER SECURITY TECHNOLOGY
(CS)
MALAYSIA BOARD OF TECHNOLOGISTS

____
(Student’s Signature)

Full Name : Ts YAU TI DUN
ID Number : MCC17003
Date : 3 AUGUST 2023

AN ENHANCED NEXT GENERATION SECURITY OPERATION CENTRE FRAMEWORK FOR INFORMATION SYSTEM SECURITY MANAGEMENT

YAU TI DUN

Thesis submitted in fulfilment of the requirements
for the award of the degree of
Master of Science

Faculty of Computing
UNIVERSITI MALAYSIA PAHANG

AUGUST 2023

ACKNOWLEDGEMENT

Throughout the entirety of this research project, Ts. Dr. Mohd Faizal Bin Ab Razak was there to offer important direction, supervision, and encouragement. I want to begin by expressing my most heartfelt gratitude to him for all of his hard work. My desire to finish this study was considerably bolstered by his leadership, thoughtfulness, and words of support. He instructed me on efficiently carrying out research and providing the results in the shortest time. The opportunity to work and learn under his leadership is an exceptional honour and privilege. Because of everything he has done for me, I owe thanks to him.

Additionally, I'd like to convey gratitude towards Associate Professor Ts. Dr Mohamad Fadli Bin Zolkipli for the idea, guidance and support of my journey as a Throughout the entirety of this research project, Ts. Dr. Mohd Faizal Bin Ab Razak was there to offer important direction, supervision, and encouragement. I want to begin by expressing my most heartfelt gratitude to him for all of his hard work. My desire to finish this study was considerably bolstered by his leadership, thoughtfulness, and words of support. He instructed me on efficiently carrying out research and providing the results in the shortest time possible. The opportunity to work and learn under his leadership is an exceptional honour and privilege. Because of everything he has done for me, I owe thanks to him. In addition, I'd like to thank Associate Professor Ts. Dr Mohamad Fadli Bin Zolkipli for the idea, guidance, and support throughout my journey as a researcher. I owe gratitude to my parents for constantly encouraging me and praying for me to complete my studies. I owe gratitude to my family for their diligence, prayers, and respect in assisting me in completing this research work. Finally, a heartfelt thank you to En Juhari and Cik Hazwani for their role as my research assistants.

I owe gratitude to my parents for constantly encouraging me and praying for me to complete my studies. I owe gratitude to my family for their diligence, prayers, and respect in assisting me in completing this research work.

Finally, a heartfelt thank you to En Juhari and Cik Hazwani, for their role as my research assistant.

ABSTRAK

Saban harian organisai berhadapan dengan serangan siber. Akibatnya, keselamatan siber menjejaskan individu dan entiti. Adalah penting untuk bertindak balas dengan pantas terhadap insiden keselamatan untuk menghalang penyerang daripada mengakses sumber penting apabila serangan siber menjadi lebih canggih. Penyelidikan ini mengenal pasti bidang utama dalam NGSOC, pihak berkepentingan, tadbir urus, keselamatan, teknikal, fungsi dan risikan ancaman. Rangka kerja cadangan disahkan menggunakan soal selidik dan peraturan korelasi menggunakan perisikan ancaman. Untuk mengesahkan keberkesanan keupayaan pengesanan NGSOC, peraturan korelasi digunakan untuk mengesahkan keberkesanan perisikan ancaman. Rangka kerja ini bertujuan untuk membantu merapatkan jurang antara metodologi teori, pelaksanaan proprietari, dan sistem kendiri. NGSOC membantu perniagaan bersedia untuk pencerobohan. Untuk merealisasikan potensi penuh mereka, mereka mesti dicipta dengan betul, digunakan, disepadukan, dinilai secara tetap dan dipertingkatkan dari semasa ke semasa. Mereka meningkatkan keupayaan syarikat untuk melawan penggodam, kerugian kewangan dan pelanggaran data apabila digunakan dengan jayanya.

ABSTRACT

Cyberattacks is becoming more common than ever. As a result, cybersecurity affects individuals and entities. It is crucial to respond rapidly to security incidents to prevent attackers from accessing vital resources as cyberattacks become more sophisticated. This research identify key areas in NGSOC, stakeholder, governance, security, technical, functionality, and threat intelligence. The propose framework is validate using a questionnaire and correlation rules utilizing threat intelligence. In order to verify the efficacy of NGSOC's detection capabilities, correlation rules is use to validate the effectiveness of threat intelligence. The framework is intended to help bridge the gap between theoretical methodologies, proprietary implementations, and standalone systems. NGSOC helps businesses prepare for intrusions. To realize their full potential, they must be properly created, deployed, integrated, evaluated on a regular basis, and enhanced over time. They boost a company's ability to fight against hackers, financial losses, and data breaches when deploy successfully.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

REFERENCES

A. Gorod, R. Gove, B. Sauser, and J. Boardman, (2007) ``System of systems management: A network management approach," in Proc. IEEE Int. Conf.

Y. O Abel, A.O. Fransica, (2023) Mitigating cybercrimes in an evolving organizational landscape

Akalanka, Shanith, Perera, Madushanka, Amila (2021). The Next Gen Security Operation Center

Babu Veerappa Srinivas, (2014) SECURITY OPERATIONS CENTRE (SOC) IN A UTILITY ORGANIZATION.

Bank Negara Malaysia. (2018, September 4). *Risk Management in Technology (RMIT).* Retrieved from Bank Negara Malaysia: http://www.bnm.gov.my/index.php?ch=57&pg=144&ac=725&bb=file

Bhatt, S., Manadhata, P. K., & Zomlot, L. (2014). The Operational Role of Security Information and Event Management Systems. *IEEE Security & Privacy, 12*(5), 35-41.

B.A.Nor, P. Maria, F. Steven, and C.Nathan, (2012) "Incident prioritisation using analytic hierarchy process (AHP): Risk Index Model (RIM)" Security and Communication Network DOI: 10.1002/sec.673.

B.A.Nor, P.Maria, F.Steven, P.Maria, and C.Nathan, (2011) " A risk index model for security incident prioritization", 9th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, 5th -7th December.

B.Ahmad, (2017) “Intrusion Detection With Tree-Based Data Mining Classification Techniques BY Using KDD DataSet.” European Journal of Computer Science and Information Technology Vol.5, No.6, pp.11-18.

Byung, I K. Nakhyun, K. Seulgi, L. Hyeisum, C. Junhyung, P. (2018). A Study on a Cyber Threat Intelligence Analysis (CTI) Platform for the Proactive Detection of Cyber Attacks Based on Automated Analysis

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer Security Incident Handling Guide. *NIST Special Publication, 800*(61), 1-147.

Crowley, C. (2017). *Future SOC: SANS 2017 Security Operations Center Survey.* Maryland: SANS Institute.

C. Pfleeger, J. Margulies and S. Pfleeger, (2015) *Security in computing*.
Matt Stevens, (2017) *Security Information and Event Management (SIEM)*.

Chuvakin, A., Schmidt, K., & Phillips, C. (2012). Logging and log management: the authoritative guide to understanding the concepts surrounding logging and log management. Newnes.

Cyber Security article for Mirai Botnet, (2021) Cloudflare Inc. https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/

D. Shahjee, N. Ware, (2022) Integrated Network and Security Operation Center: Systematic Analysis

E.Allison Newcomb, J.H.II Robert., H.Steve., (2016) "Effective Prioritization of Network Intrusion Alerts to Enhance Situational Awareness", Conference Paper. IEEE Conference on Intelligence and Security Informatics (ISI)

Frost & Sullivan. (2017). *Global Information Security Workforce Study.*

F.Alserhani. (2013) " A framework for Multi-stage Atrack Detection." Conference: Electronics, Communications and Photonics Conference (SIECPC), 2013Saudi International

Gordon, A. (2015). *Service Level Agreements (SLA)* (Vol. 4). Auerbach Publications.

Grobler, M., Jacobs, P., & Niekerk, B. v. (2017). Cyber Security Centres for Threat Detection and Mitigation. *Threat Mitigation and Detection of Cyber Warfare and Terrorism Activities*, 21-51.

G.S.-Tangil, E.Palomar, A.Ribagorda, and I.Sanz., (2015) "Providing SIEM systems with self-adaptation." Information Fusin 21.

Honoree, J. (2017). Understanding The Role Of Triangulation In Research. *SRJIS,4/31*, 91-95. Retrieved December 7, 2018, from http://www.srjis.com/pages/pdfFiles/149544238718. HONORENO JOHNSON.pdf

ISACA. (2012). *COBIT 5: An Introduction*. Retrieved from ISACA: http://www.isaca.org/COBIT/Documents/An-Introduction.pdf

ISO/IEC. (2013). *Information Technology -- Security Techniques -- Information Security Management Systems -- Requirements (ISO/IEC 27001:2013)*. Retrieved from https://www.iso.org/standard/54534.html

J.A. Altena Nijmegen, (2012) ISO/IEC 27002 Baseline Selection Control selection based on effectiveness and cost within a fixed budget.

János, F. D., & Dai, N. H. (2018). Security Concerns Towards Security Operations Centers. *Applied Computational Intelligence and Informatics (SACI)*.

Josh Fruhlinger (2020). The CIA Triad: Definition, components and examples. CSO Asean Online. Retrieved from https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html

Jungsuk Song, Younsu Lee, Jang-Won Choi, Joon-Min Gil, Jaekyung Han and Sang-Soo Choi , (2017) Practical In-Depth Analysis of IDS Alerts for Tracing and Identifying Potential Attackers on Darknet.

K. Sebastian, M.D Schultz, P. Seele, (2021) Cyberattacks as “state of exception” reconceptualizing cybersecurity from prevention to surviving and accommodating

K. Zetter, (2016) “Why hospitals are the perfect targets for ransomware,” Wired, 2016.

K. Zetter, (2016) “4 ways to protect against the very real threat of ransomware,” 2016. [Online]. Available: https://www.wired.com/2016/05/4-ways-protectransomware-youre-target/

Kowtha, S., Nolan, L., & Daley, R. (2012). Cyber Security Operations Center Characterization Model and Analysis. *IEEE*, 470-475.

Kristie Magowan (2020). *IT Governance vs IT Management: Mastering the Differences*. BMC Blogs. Retrieved from https://www.bmc.com/blogs/governance-vs-management/

Keragala, Dilshan. (2017) Detecting Malware and Sandbox Evasion Techniques. 1st ed. Dilshan Keragala, 2016.

K. Anya, H.K. Myong, Z. L. Jim, Alex V., (2014)" A Framework for Event Prioritization in Cyber Network Defense," Center for High Assurance Computer Systems Information Technology Division.

Luke Irwin (2019). How to Document the Scope of Your ISO 27001 ISMS. IT Governance UK. Retrieved from https://www.itgovernance.co.uk/blog/how-to-document-the-scope-of-your-isms

MANFRED V, FABIAN B, INES F, AND GÜNTHER P (2020) Security Operations Center: A Systematic Study and Open Challenges IEEE

Max V H, , Guy G, Gilad T, Rolan K, Cristian P, Dumitru D, Adrian R, Louis B, Samuel F, Jose F R, Esteban A, Matthieu B and Marco S. (2021) A Shared Cyber Threat Intelligence Solution for SMEs

M. Pokrinchak and M. M. Chowdhury, (2021) "Distributed Denial of Service: Problems and Solutions," IEEE International Conference on Electro Information Technology (EIT).

MDEC. (2018). *Industry Guidance For Next-Generation Managed Security Operating Centre.* Kuala Lumpur.

Miloslavskaya, N. (2016, August). Security operations Centres for information security incident management. In *Future Internet of Things and Cloud (FiCloud), 2016 IEEE 4th International Conference on* (pp. 131-136). IEEE.

N. Miloslavskaya,(2020) ``Security zone infrastructure for network security intelligence centers,".

M. Vielberth, F. Bohm, I. Fichtinger, and G. Pernul, (2020)``Security operations center: A systematic study and open challenges,'.

Nabil, M., Soukainat, S., Lakbabi, A., & Ghizlane, O. (2017). SIEM selection criteria for an efficient contextual security. *Networks, Computers, and Communications (ISNCC)*, 1-6.

NetIQ Corporation. (2016, September). *Operations Center Service Level Agreement Guide.* Retrieved from NetIQ: https://www.netiq.com/documentation/operations-center-57/pdfdoc/service_level_agreement/service_level_agreement.pdf

NIST. (2018). *Cybersecurity Framework's Five Functions*. Retrieved from NIST: https://www.nist.gov/cyberframework/online-learning/five-functions

NIST 800-150 (2016) Guide to Cyber Threat Information Sharing

Nicolett and K. Kavanagh, (2017) "Magic quadrant for security information and event management.".

N. Skabcovs and A. Latkov, (2011) "Enterprise security perimeter — E-mail server protection," 2011 Baltic Congress on Future Internet and Communications.

N. Hernandez, (2018) ``NoC and SOC integration opportunities increased Efficiency incident response cyber security," SANS Inst., Bethesda, MD, USA, Tech. Rep., Onwubiko, C. (2015). Cyber Security Operations Centre: Security Monitoring for Protecting Business and Supporting Cyber Defense Strategy. *Cyber Situational Awareness, Data Analytics, and Assessment (CyberSA)*, 1-10.

Official Manual of Splunk®, Enterprise - Alerting Manual, version 8.2.2, Copyright © 2021 Splunk Inc.

Palo Alto Networks. (2018, December 26). *Build a Next-Generation SOC Techbrief*. Retrieved from Palo Alto Networks: https://www.paloaltonetworks.com/resources/techbriefs/build-next-generation-soc

R.Leonard, H. Felix, D.R.Gabi, (2017) "Modeling and Learning Incident Prioritization." The 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications., Bucharest, Romania

Ristov, Sasko & Gusev, Marjan & Kostoska, Magdalena. (2011). *Information Security Management System for Cloud Computing.* ICT Innovations 2011 Web Proceedings ISSN 1857-7288

S.Pritpal., B.Sunny, K.Krishan, (2015) "Performance Enhancement of a Malware Detection System using Score Based Prioritization of Snort Rules." 2015 International Conference on Green Computing and Internet of Things.

S. Riyanat, H. Alex, G.H. Robert, B.Robin, M. Rajarjan, (2014) " OutMet: A New Metric for Prioritising Intrusion Alerts using Correlation and Outlier Analysis", 39th Annual IEEE Conference on Loca Computer Networks.

SANS, (2017) *Understanding-intrusion-detection-systems*. SANS Institute InfoSec Reading Room.

Sander Dorigo, (2018) Security Information and Event Management, Master Thesis, Radboud University Nijmegen.

Shenk, J. (2014). *Ninth Log Management Survey Report.* Maryland: SANS Institute.

Schinagl, S., Schoon, K., & Paans, R. (2015). A framework for Designing a Security Operations Centre (SOC). *IEEE*, 2253-2262.

Survey Monkey. (2017). *Using quantitative research effectively*. Retrieved from Survey Monkey: https://www.surveymonkey.com/mp/using-quantitative-research-effectively/

S. A. Mirheidari, S. Arshad, and R. Jalili. (2013) : Alert Correlation Algorithms: A survey and taxonomy. In Cyberspace Safety and Security.

The Hacker News (2021). Why Human Error is the #1 Cyber Security Threat to Businesses in 2021. Retrieved March 2, 2022, from https://thehackernews.com/2021/02/why-human-error-is-1-cyber-security.html

Thomas D. Wagner (2014). Sharing Cyber Intelligence in Trusted Environments – A Literature Review.

Torres, A. (2015). *Building a World-Class Security Operations Center: A Roadmap.* SANS Institute.

Townsend, M. (2017, June 10). How a crippling shortage of analysts let the London Bridge attackers through. Retrieved November 5, 2018, from https://www.theguardian.com/uk-news/2017/jun/10/london-bridge-attackers-intelligence-overload

T. Su, S. Wang, Y. Chen and C. Liu, (2016) "Attack detection of distributed denial of service based on Splunk," International Conference on Advanced Materials for Science and Engineering (ICAMSE).

Wood, P., & Egan, G. (2017). Symantec Internet Security Report 2017 (Rep.). Mountain View, CA: Symantec Corp.

Yuan, S., & Zou, C. (2011). The security operations center is based on correlation analysis. *Communication Software and Networks (ICCSN)*, 334-337.

Yau T D, M Faizal, M F Zolkipli, Tan F B, Ahmad F (2021) Grasp on Next Generation Security Operation Centre (NGSOC): Comparative Study