

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

YAU TI DUN

MASTER OF SCIENCE
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

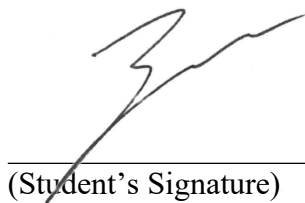
(Supervisor's Signature)

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



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.


(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 researcher. 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 sendiri. 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 penggadam, 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

DECLARATION	
TITLE PAGE	
ACKNOWLEDGEMENT	ii
ABSTRAK	iii
ABSTRACT	iii
LIST OF TABLES	viii
LIST OF FIGURES	x
CHAPTER 1 INTRODUCTION	1
1.1 Background	1
1.2 Motivation	2
1.3 Problem Statement	2
1.4 Aim and Objectives	4
1.5 Scope	5
1.6 Research Significance	5
1.7 Research Organization	5
CHAPTER 2 LITERATURE REVIEW	7
2.1 Framework	7
2.1.1 NIST Cybersecurity Framework (CSF)	9
2.1.2 Control Objectives for Information and Related Technology (COBIT)	9
2.1.3 Information Security Management System (ISMS) ISO 27001	10
2.2 Stakeholder	11
2.2.2 Service Management	12
2.2.3 SOC Management	14
2.2.4 Stakeholder Reporting	18
2.3.1 Facilities Management	20
2.3.2 People Management	21
2.3.3 Operational Management	23
2.3.4 Framework	25
2.4 Security	27
2.4.1 Policy, Procedure, and Process	27
2.4.2 Physical Security	30
2.4.3 Technical Security	30
2.4.4 Data Security	30
2.4.5 People Security	30
2.5 Technical	32
2.5.1 SOC Architecture	33

2.5.2	Technology Selection	34
2.5.3	Tool Selection	35
2.5.4	Operations	37
2.6	Functionality	39
2.6.1	Identify	41
2.6.2	Protect	42
2.6.3	Detect	43
2.6.4	Respond	45
2.6.5	Recover	45
2.7	Intelligence	48
2.8	Summary	50
CHAPTER 3 METHODOLOGY		51
3.1	Research Methodology	51
3.2	Summary	58
CHAPTER 4 RESULT - FRAMEWORK		59
4.1	Design NGSOC Framework	59
4.2	Stakeholder	62
4.2.1	Stakeholder requirement	63
4.2.2	Service Management	63
4.2.3	NGSOC Management	64
4.2.4	Stakeholder Reporting	64
4.3	Governance	65
4.3.1	Facilities Management	67
4.3.2	People Management	71
4.3.3	Operational Management	76
4.3.4	Framework	78
4.4	Security	91
4.4.1	Policy, Procedure, Process	91
4.4.2	Physical Security	94
4.4.3	Technical Security	98
4.4.4	Data Security	100
4.4.5	People Security	102
4.5	Technical	103
4.5.1	Architecture	103
4.5.2	Technology Selection	105
4.5.3	Tool Selection	107
4.5.4	Operations	109
4.6	Functionality	110
4.6.1	Identify	110
4.6.2	Detect	112
4.6.3	Protect	111
4.6.4	Response	112
4.6.5	Recover	113
4.7	Intelligence	114
4.7.1	Threat Intelligence	114

4.8 Summary	117
CHAPTER 5 FRAMEWORK VALIDATION	118
5.1 Correlation Rules Process Flow	118
5.2 Hermes Ransomware V2.1	120
5.3 Use of AES with RSA	123
5.4 Indicator of Compromised (IOC):	123
5.5 Affected File Formats.....	124
5.6 Impact.....	124
5.7 Vulnerability	124
5.8 Recommendation.....	125
5.9 Correlation Rules For “Ransomware Hermes V2.1.”	125
5.10 Filtering.....	126
5.11 Enriching.....	126
5.12 Aggregating.....	127
5.13 Combining Rules	127
5.14 Actions.....	128
5.15 IOC matching	128
5.16 Analytics And Baselining.....	128
5.17 Performance Considerations	129
5.18 Discussion.....	130
5.19 NGSOC Framework Validation Survey	138
5.20 Summary	154
CHAPTER 6 CONCLUSION.....	155
6.1 Study Revisit	155
6.2 Conclusion.....	158
6.3 Limitation Of Research.....	160
6.4 Future Research	161
REFERENCES	162
APPENDIX A PUBLICATION.....	168
Publication 1 IJNAA	168
Publication 2 IJASEIT	169
Publication 3 IOP	170
Publication 4 ICSECS-ICOCSIM.....	171
Publication 5 CORE OIJ.....	172
APPENDIX B Questionnaire	173

LIST OF TABLES

Table 1.1: Summary of problem statement	13
Table 2.1: Pros and Cons of the SOC Model	25
Table 2.2: Comparison between all frameworks in the aspect of stakeholder	29
Table 2.3: Security Analysts Roles	32
Table 2.4: Staff Duties and Training Needs	33
Table 2.5: Counteraction Capabilities	35
Table 2.6: Deployment Scenarios	35
Table 2.7: Various Form Of SOC	37
Table 2.8: Framework	38
Table 2.9: Comparison between all frameworks in the aspect of governance	39
Table 2.10: Comparison between all frameworks in the aspect of security	44
Table 2.11: Technical Domain	45
Table 2.12: Technical Criteria	50
Table 2.13: Comparison between all technical frameworks	52
Table 2.14: Heatmap of tools used by SOC	53
Table 2.15: Correlation Technique	58
Table 2.16: Comparison between all functionality frameworks	62
Table 2.17: Levels of intelligence	62
Table 2.18: Sources of intelligence	63
Table 2.19: Comparison between all intelligence frameworks	64
Table 3.1: Questionnaire	68
Table 4.1: NGSOC Models Comparisons	72
Table 4.2: Certificates and Experience in the NGSOC area	84
Table 4.3: Responsibilities of Security Analysts	84
Table 4.4: Duties and Training for Each Tier in NGSOC	84
Table 4.5: Comparisons between Counteraction Capabilities in NGSOC	88
Table 4.6: Comparisons between Centralized and Distributed NGSOC	87
Table 4.7: Various Form Of NGSOC	90
Table 4.8: Framework	91
Table 4.9: Disciplines in ISO 27001:2013	93

Table 4.10: Process in Security Incident Response	107
Table 4.11: Secure Physical and Environmental Control and descriptions	109
Table 4.12: Equipment Controls and Subsections	111
Table 4.13: Technology Selection	123
Table 4.14: Tools Selection Criteria	125
Table 5.1: Hermes Ransomware	137
Table 5.2: Indicator of compromise for Hermes Ransomware v2.1	148
Table 5.3: Building Correlation Rules for Ransomware	149

LIST OF FIGURES

Figure 1.1: Research organization	15
Figure 2.1.1: Building Blocks of SOC	18
Figure 2.1.2: Building Blocks of NGSOC	18
Figure 2.2: Location and Centralization of SOCs, 2017	25
Figure 2.3: Incident Response Process	41
Figure 2.4: Architecture Model	46
Figure 2.5: Data Aggregation	48
Figure 2.6: Technical Operation Flow of a SOC	51
Figure 3.1 Research Methodology	69
Figure 3.2: Threat Intelligence Function	70
Figure 3.3: Building Complex Correlation Rules	70
Figure 3.4: Lab simulation flow	71
Figure 4.1: NGSOC Framework	71
Figure 4.2: Classification of Stakeholders	72
Figure 4.3: Governance Role	75
Figure 4.4: NGSOC Design Facilities	78
Figure 4.5 NGSOC Organization Chart	82
Figure 4.6: ISMS ISO 27001 Framework	92
Figure 4.7: ISMS ISO 27001 Discipline	94
Figure 4.8: PDCA Model Structure for ISMS	96
Figure 4.9: Phase 1 in PDCA Model	97
Figure 4.10: Phase 2 in PDCA Model	98
Figure 4.11: Phase 3 in PDCA Model	99
Figure 4.12: Phase 4 in PDCA Model	101
Figure 4.13: Process to Obtain ISO 27001:2013 Certification	104
Figure 4.14: Ongoing ISO 27001 Audit Cycle	105
Figure 4.15: Security of NGSOC	103
Figure 4.16: Security Incident Escalation Process	115
Figure 4.17: Methods in Technical Security	121
Figure 4.18: Technical Overview in SOC	122
Figure 4.19: General architecture concept in GNSOC	123
Figure 4.20: The Architect Detail of NGSOC	124

Figure 4.21: Technology Selection	128
Figure 4.22 NGSOC Functionality	129
Figure 4.23: Threat Intelligence Method	132
Figure 4.24: Threat Intelligence Flow	133
Figure 5.1: Correlation Rules Update Flow	136
Figure 5.2: NGSOC Correlation Rules Structure	137
Figure 5.3: Visualization of a BMP file before and after being encrypted by this ransomware	139
Figure 5.4: File drop by ransomware	140
Figure 5.5: Script to delete shadow copy	140
Figure 5.6: Additional File drop by ransomware	141
Figure 5.7: Infection Alert	142
Figure 5.8: Adding more information regarding Indicator of compromise	145
Figure 5.9: Lab simulation flow and result	146
Figure 5.10: Security Analyst initiates the incident analysis	146
Figure 5.11: Security Analyst manual validation using IOC	147
Figure 5.12: Security Analyst searching for malicious activity	147
Figure 5.13: Security Analyst identifies and confirms “No Petya” malware attack	148
Figure 5.14: Security Analyst initiates the incident analysis	148
Figure 5.15: Security Analyst immediately identifies the correlation triggered	149
Figure 5.16: Security validates the alert information and confirms to initiate the incident escalation process.	149
Figure 5.17: Type of organization where respondent currently working	152
Figure 5.18: Respondent Job Role	153
Figure 5.19: Responder length of working experience	153
Figure 5.20: Responder prioritization requirement when building NGSOC	154
Figure 5.21: Order of prioritization requirement when building NGSOC	154
Figure 5.22: Responder services requirement when building NGSOC	155
Figure 5.23: Order of services requirement when building NGSOC	155
Figure 5.24: Inclusion of Service Level Agreement (SLA) In NGSOC	156
Figure 5.25: Type Of NGSOC Services Implemented	156
Figure 5.26: Provide Periodic Input To Stakeholder	157
Figure 5.27: NGSOC Provide Facility Management Documentation Such As Policy, Process and Guidelines	157

Figure 5.28: Documentation Provided Meet ISO27001 Standard	158
Figure 5.29: NGSOC Have Organization Chart And Job Scope	158
Figure 5.30: NGSOC Key Focus Area In Term Of People, Process and Technology	159
Figure 5.31: NGSOC Formal Third-Party Review Of Controls	159
Figure 5.32: NGSOC Have Specific Documented Policy, Procedure And Processes	160
Figure 5.33: NGSOC Has Physical Security Perimeter Control	160
Figure 5.34: NGSOC Have Technical Security Perimeter Control	161
Figure 5.35: NGSOC Have Data Security Control	161
Figure 5.36: Frequency Of Security Awareness Training For NGSOC Staff	162
Figure 5.37: SOC have a clearly defined NGSOC design/architecture document	162
Figure 5.38: NGSOC design/architecture document covers the technology selection (e.g., SIEM, log management)	162
Figure 5.39: NGSOC design/architecture document covers the tool selection (e.g., ticketing system, Endpoint Detection & Response)	163
Figure 5.40: NGSOC have an incident management workflow defined & documented	163
Figure 5.41: NGSOC monitoring covers all the assets in organization	164
Figure 5.42: Security solutions that the NGSOC monitor	164
Figure 5.43: NGSOC have a process to update correlation rules or playbook to detect threats	165
Figure 5.44: NGSOC have a formal incident response plan	165
Figure 5.45: NGSOC have a formal Business Continuity/Disaster Recovery plan	165
Figure 5.46: NGSOC have the Business Continuity Plan tested annually	164
Figure 5.47: NGSOC have subscribed to cyber threat intelligence feeds	164
Figure 6.1 : Six Domain of NGSOC Framework	168
Figure 6.2 : NGSOC Framework	169

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.Alsershani. (2013) “ A framework for Multi-stage Atrack Detection.” Conference: Electronics, Communications and Photonics Conference (SIEPC), 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](http://www.srjis.com/pages/pdfFiles/149544238718.HONORENO%20JOHNSON.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 Local 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