Int. J. Advanced Networking and Applications
Volume: 17, Issue: 02, Pages : 6806-6812 (2025) ISSN: 0975-0290
https://doi.org/10.35444/IJANA.202517202

Timely and Accurate Detection and Control of Logical Threats and Vulnerabilities as a Precursor for Success in Corporate Information System Security

Paul Abuonji
Department of Networks and Applied Computing; School of Technology, KCA University
Email: pabuonji@kcau.ac.ke

ABSTRACT

Organizations grapple with numerous cyber security challenges on daily basis. Many operate online with limited technical controls in place that cannot adequately detect, report and mitigate against the inherent risks. This paper postulates that timely and accurate detection and control of logical threats and vulnerabilities within a corporate information system's environment is a precursor for success in implementing an effective information system security progrmame. Consequently, in this research, a five-level stratified vigilance structure is developed- and defined as: very low vigilance, low vigilance, moderate vigilance, high vigilance and hyper vigilance- then implemented in a next generation unified threat management (UTM) firewall deployed at the gateway of a high traffic corporate network to monitor activities on the network including threats and vulnerabilities. The UTM was initially deployed with the lowest level of vigilance, then gradually and systematically re-adjusted in a carefully calibrated manner, to represent the various successive levels of vigilance and handled logical threats and vulnerabilities at the various levels. The outcome of the study demonstrated that vigilance is a very important factor in detecting and controlling information systems threats and vulnerabilities in a timely and accurate manner, and this directly translates to the security of the infrastructure.

Keywords – **cybersecurity, firewall, threats, vulnerabilities, vigilance.**

Date of Submission: July 26, 2025 Date of Acceptance: August 20,2025

I. INTRODUCTION

The ubiquitous nature of digital technologies in the modern society, coupled with constantly changing cyberspace have created a conundrum for cyber security experts [1] It has become a powerful playground for cybercriminals, and has triggered a surge in demand for intelligent threat detection systems based on Artificial intelligence [2] [3]. Security in every sense and perspective is synonymous with the concept of vigilance. Whereas this statement is true for all security operations, it is absolutely true for information system security due to the brisk pace and dynamic nature of cybersecurity and related activities coupled with the cardinal role technology plays in modern organizations [1]. Therefore, one of the surest ways to enhance cybersecurity is by increasing vigilance using detective and predictive systems [4]. Consequently, this study contends that security in whatever form- whether administrative, physical or logical is miserably impractical without vigilance on the part of security agents and all stakeholders, including those being protected and the information system itself. According to [5] vigilance is a state of readiness to detect and respond to rare and unpredictable events over extended time intervals, often in monotonous settings. On the other hand, [6] defined vigilance as a brain state marked by sustained readiness and reduced distractibility, mediated by the frontoparietal and default mode networks. Whereas the aforementioned researchers generally defined vigilance from strictly human perspective, [7] related vigilance to performance monitoring and mental workload in environments such as aviation, cybersecurity, and healthcare. In information systems, the security of computers or programs largely depends on the efficiency and effectiveness of its vigilance mechanisms that prompts its users and administrators when an abnormal activity occurs [8]. With brisk and widespread adoption of computer systems coupled with quick-fix application development and deployment tendencies, everything in the information system infrastructure appears to be vulnerable. To that end, security of information systems has become a cause of great concern [9][10]. Therefore, even though the classical risk-based approach to cyber security has previously been considerably effective, in order for cyber security programmes to effectively mitigate against the current challenges, the approach must be augmented with deployment of advanced monitoring systems to improve vigilance.

II. RELATED WORKS

A robust enterprise network infrastructure supports a variety of systems and services such as Enterprise resource planning (ERP) systems, Internet of Things (IoT) devices, virtual reality simulations, learning management systems (LMS), smart classrooms, etc., depending on the nature of the organization [11]. They also support many users both

on-premise and remote. This requires robust monitoring mechanisms [12].

In its cyber security reports of 2014 and 2021, Deloitte indicated that a good financial system must have three main features- secure, vigilant and resilient. It explained that a secure system must have enhanced risk prioritized controls to protect against known and emerging threats and should comply with industry cyber security standards and regulations. A vigilant system must detect violations and anomalies through better situational awareness across the environment. Finally, a resilient system must establish the ability to quickly return to normal operations and repair any damages to the business [13] [14]. It further illustrates that organizations need multipronged approach to cyber security management involving automated systems and people.
As postulated by Deloitte and illustrated above, IT security needs to be implemented in two fronts namely automated systems and human components. These should provide security, vigilance and resilience. Automated system vigilance comes in many forms by different names, but the general principle is that they must have actionable threat intelligence that will enable then detect, interpret, report and respond to threats if possible. For this to happen, the system must have the capacity for experience-based learning and situational awareness. Nevertheless, there are some threats whose actions are either too subtle or severe to be handled by automated systems alone. In such a case, human vigilance at different levels of knowledge, skills, experience and organizational responsibility will be required. Successful implementation of this requires a good training and awareness programme in the organization, coupled with proper reporting and response channels in the organogram [15].

Several studies indicate that many cyber-attacks take place against individuals, organizations or states and either go unnoticed or are detected too late thereafter. These attacks are perpetrated either by lone cyber criminals, organized criminals like Anonymous hackers and hacktivists or government agencies. According to [16]. United States, British and Chinese governments participate in large scale cyber-crimes in the name of gathering intelligence to curb terrorism or for economic and political espionage. To prevent such acts of law breaking by the supposed law enforcers, citizens ought to be vigilant and defend themselves through civil rights activism or the technology community need to over-engineer their systems to prevent unlawful government surveillance that impinge on citizen's fundamental rights to privacy.

In order to appreciate progress in cyber security vigilance in corporate information Systems infrastructure, we review cyber security detection and response capabilities over time. [13] Reported that the response time to cyber-attacks by global financial services firms indicated significant gaps in their preparedness. This was due to inability of these firms to quickly detect and respond to cyber threats. Attack success is the time to compromise the system. It measures time from the first malicious action taken against the victim until the point at which an information asset is negatively affected. Discovery success is the time from compromise of the system to discovery. It measures time from initial compromise to when the victim first learns of the incident. Finally, restoration success is the time from discovery to containment. It measures the time between discovery of a breach to when it is successfully contained. The study showed a big margin between attack success and discovery success, and another big margin between discovery success and restoration success. This clearly shows a lapse in vigilance.

The Deloitte study discovered that 34% of successful attacks to information systems happened within seconds; 8% succeed within minutes and 46% succeed within hours. These statistics showed that a whopping total of 88% of information systems that were attacked and got compromised succumbed to their victims within less than a day. Only 10% resisted attacks for days and another 1% for weeks. The remaining 1% was not allocated. This grim state of IS security in financial systems was worsened by the fact that only 21% of targeted organizations had security systems that could detect attacks within a day while majority took longer to detect- 30% took days to detect, 11% took weeks, 34% took months and 4% took years to detect that they were compromised. When it came to restoring the system, no organization was able to restore its system or services within seconds or minutes. The most efficient was discovered to be able to restore within hours, constituting 40%. The other, 25% took days to restore their systems, 10% took weeks, 20% took months and 5% took years to restore the systems. The disturbing results of this study revealed a huge lapse in vigilance and security of information systems in financial services firms a few years ago.

M-trends 2022 report documented that Enterprise organizations are getting better at detecting intruders in their environment [17]. In 2022, the median dwell time i.e. the amount of time an attacker remains undetected on a network was 16 days, a huge improvement form ten years ago which was 205 days. While ReliaQuest Annual Cyber-Threat Report, 2024 indicated that whereas organizations that utilized traditional incident detection and response mechanisms had an average mean time to respond (MTTR) of 2.3 days, those that had deployed artificial intelligence-based systems had an average MTTR of 58 minutes. Cyber security statistics from many sources have indicted remarkable improvement in threats detection and response; especially for those who had adopted the use of AI [18].

The necessity for vigilance is augmented by the complexity that characterizes information systems security. This is because IS security is pervasive and remains a continuous process not an event. A well designed and implemented security program, if forgotten is as good as no security [19]. Besides, vigilance should be stratified to ensure that the degree of vigilance required for any system or resource is commensurate with the level of risk faced by that system or resource. This requires organizations to diligently assess

Int. J. Advanced Networking and Applications
Volume: 17, Issue: 02, Pages : 6806-6812 (2025) ISSN: 0975-0290
https://doi.org/10.35444/IJANA.202517202

their risk levels and develop a stratified vigilance scheme based on the risk ratings.

It is practically impossible to provide a level of security that would eliminate all risks, but a good security programme should aim at trying to make it as hard as possible for an attacker to breach the system's security [20]. As shown in figure 1 below, vulnerabilities abound within the information systems used by organizations while threats emanate from the environment. However, some systems have more vulnerabilities than others depending on the efforts put by the owners and developers to safeguard them while some environments also present more threats to information systems than others [20].

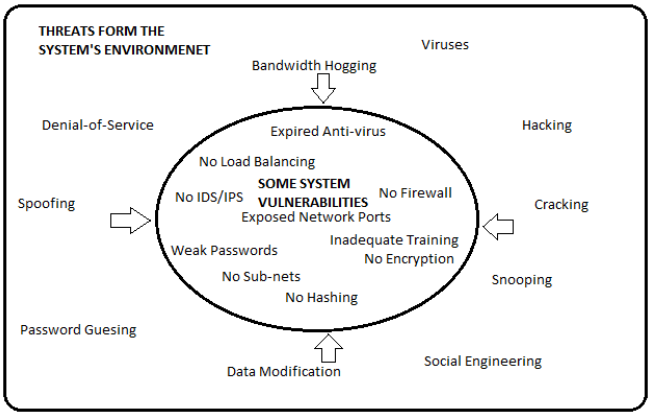

Figure 1: Threats and Vulnerabilities

It's vital to note that for a security breach or incident to take place in an information system, a threat must identify vulnerability in the system and exploit it. It is therefore necessary for security professionals to pair threats to vulnerabilities in order to be able to determine the level of risk their information systems face. However, this is a complex and dynamic process that largely depends on how the systems are designed and configured, how they integrate with other systems, who uses the them and the unique operating environment of the organization being considered.

There is a special class of threats that are within the system and so they are also considered as vulnerabilities. Examples are Trojan horse, logic bombs, spyware and back door viruses that come inbuilt with the software [21] [22]. See figure 2 below.

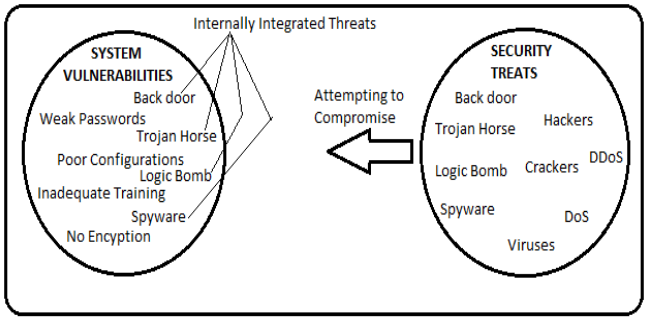

Figure 2: Threats and Vulnerabilities

If a system is developed with such kind of vulnerabilities, that system is a threat to itself, and requires a higher level of vigilance to detect and correct inherent implementation deficiencies. Such scenarios are more subtle and difficult to mitigate since security assessment needs to be conducted from the source code. Code review can be conducted by intelligent automated systems or by programming experts. Whichever approach taken, there is need for high vigilance in order to produce a secure system devoid of internal threat or vulnerabilities [23].

III. METHODOLOGY

The study adopted descriptive and diagnostic research design. Descriptive study was used to collect and record primary data depicting the problems, issues or concerns within the system under study while diagnostic study was used to facilitate an in-depth analysis of the research variables. According to [24] and [25], descriptive research studies are concerned with describing the characteristics of a particular individual or of a group whereas diagnostic research study determines the frequency of occurrence or its association with something else. Furthermore, [26] explains that diagnostic research helps the researcher to investigate the root cause of a particular problem.

The study was carried out in a corporate network environment with a complex information system infrastructure consisting of a local area network, high speed internet, many server computers, client computers, Enterprise Resource Planning (ERP) system, as well as a wireless LAN. In addition, the organization had over 12,000 computer users who share resources and were spread over a wide geographical area. This brought about competing interests among the users and exposure to many internal and external threats.

An advanced next generation Unified Threat Management (UTM) system firewall with functionalities such as Intrusion Prevention System, bandwidth management system, user identification system, traffic discovery system and weighted round robin load balancing algorithm was configured and deployed on the network getaway to monitor traffic and collect data in-situ. Data was collected based on the UTM system configurations and network activities and reports generated from time to time. The UTM rulesets, policies, QoS, IDS, IPS, etc. were systematically and gradually adjusted to provide the desired level of vigilance. From very low vigilance where almost not monitoring and detection controls were in place, an upward adjustment was done five steps, all the way to hyper-vigilance where the highest level of monitoring, detection and response controls were activated. Data from the logical threats and vulnerabilities was captured. This data was analyzed to reveal common logical cyber threats to and vulnerabilities in the information system infrastructure. Different levels of vigilance were identified and classified and illustrated in table 1 below:

Table 1: Time Constrain Metrics for Vigilance

Vigilance Level	**System Administration Activities**
Very Low Vigilance	System is setup but unmonitored. Owners are content with its existence.
Low Vigilance	System is monitored to ascertain system health.

Moderate Vigilance	If there is a problem, system diagnosis is done to identify cause.
High Vigilance	Ensures that a solution is found and test its effectiveness.
Hyper Vigilance	If no concrete solution is found, propose a solution and escalate.

IV. THREATS AND VULNERABILITIES DETECTION AND CONTROL

The study was conducted over a period of three months. During this period, data was collected about logical threats such as viruses, attacks, attackers, applications and protocols used in the attacks and the countries from where these attacks originated. For each item under study, the system was adjusted to represent the desired level of vigilance before data was collected. However, the said data collection was done within short time constraints before undesirable changes influenced by the environment took place. The system detected a total of 154 viruses within the said period of study. The most commonly detected virus was PUA/MyWebSearch.lddk which was detected 279 times while the least detected virus was TR/Downloader.jktrc which was detected 1 time. The total numbers of detections were 2533. Top ten viruses were selected and compared based on absolute counts per system configuration in terms of system vigilance, as shown in table 2 below.

Table 2: Common threats detected under different levels of vigilance

Threat Name	VLV	LV	MV	HV	HypV	Total_Counts
PUA/MyWebSearch.lddk	0	15	116	137	11	279
ANDROID/Roversa.SAN.Gen	0	14	99	131	7	251
JS/Mindspark.CE, JS/	0	32	74	116	12	234
ANDROID/Agent.XBT.Ge	0	8	42	133	0	183
PUA/MyWebSearch.MB.s	0	11	39	125	7	182
ANDROID/Agent.TT.Gen	0	01	48	76	3	137
ADWARE/ANDR.HiddAdd.	0	6	38	87	1	132
ANDROID/FakeUpdates.	0	6	17	92	1	116
ANDROID/Hiddad.pgzbq	0	5	42	63	1	111
ANDROID/Roversa.SAN.	0	5	45	59	1	105

At very low vigilance level, no viruses were detected. As the level of vigilance increased, the number of detections steadily increased from low, medium to high vigilance where the highest number of viruses were detected. However, at hyper vigilance level, we observed a sharp decline in the numbers of viruses detected in the system since most viruses were detected and locked at high vigilance level. Therefore, the remaining viruses needed human intervention to control them. Figure 3 below is a line graph depicting top three viruses and how their activities are affected by system vigilance.

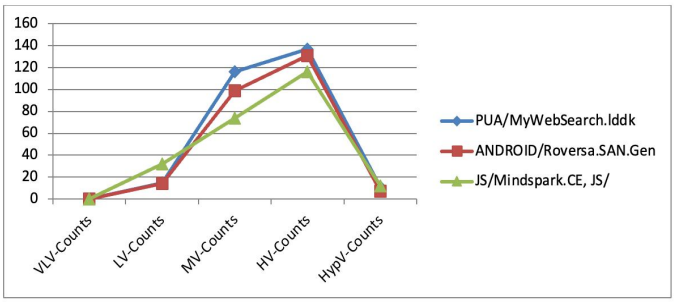

Figure 3: Effect of Vigilance of Virus Detection as Control

Regarding the attacks on the system, the most common type of attack was ICMP ping with 1,450,749 hits while the least was FTP LIST directory traversal attempt with 1 hit. Figure 4 below illustrates this information.

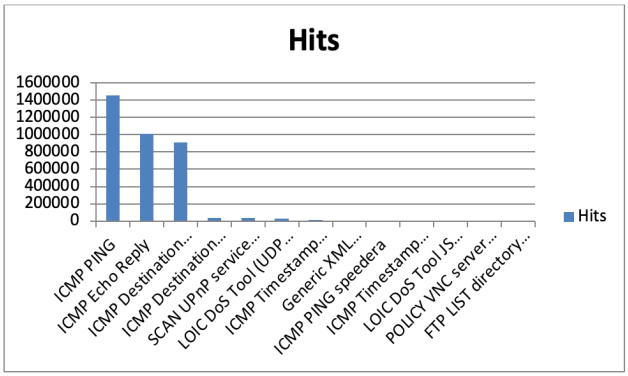

Figure 4: Common Attacks Detected in the Network

An analysis was done to determine the effect of vigilance on these attacks on the network infrastructure. Figure 5 below shows the results.

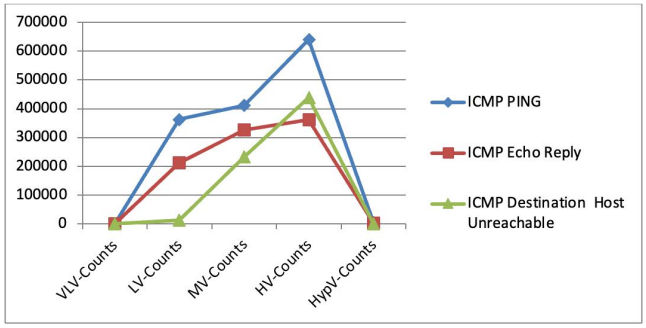

Figure 5: Effect of Vigilance on ICMP Attacks

As the level of vigilance increases, the attacks on the network such as ICMP ping, ICMP echo reply and ICMP destination host unreachable decreased. This was as a result of reconfiguring the system to prevent unwanted ICMP packets in the network.

In the wake of the high number of attacks on the network, the researcher also sought to investigate the sources of these attacks. It was discovered that these attacks emanated from within and outside the organization. A total of 27, 967 IP addresses were used to attack the network. Out of this, 1688 were local IPs while 26,279 were public IPs. This means that 93.9% of attackers were not within the organization and only 6.1% were from within the organization.

Int. J. Advanced Networking and Applications
Volume: 17, Issue: 02, Pages : 6806-6812 (2025) ISSN: 0975-0290
https://doi.org/10.35444/IJANA.202517202

However, the most notorious attacker was a local IP 192.168.2.250 constituting 12.8% of the attacks. The five other top attacking IP addresses were public IPs as shown in table 3 below. It was also noted that these five public IP addresses belonged to the organization where the research was done except 8.8.4.4 which was a universal DNS and was also used in the configuration of the WAN interface of the gateway appliance. This clearly shows that the attackers were sophisticated enough to disguise themselves by IP spoofing. By so doing, they were trying to give an impression that the organization if attacking itself.

Table 3: Top Attackers in the LAN Network

Attack IP Address	Number of Attacks	Percentage	Cumulative Percentage
192.168.2.250	445830	12.8	12.8
62.24.113.210	289768	8.7	21.5
62.24.102.116	283508	8.4	29.9
212.49.70.22	280054	8.3	38.2
41.204.179.134	219914	6.8	45
8.8.4.4	182585	5.7	50.7
Other IPs	1701659	49.3	100

The researcher then reconfigured the system to test whether different levels of vigilance would affect the attackers' activities on the network.

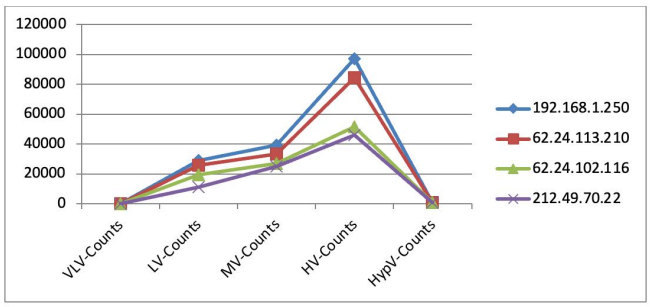

Figure 6: Effect of Vigilance on Network Attacks

The graph on figure 6 above shows that levels of vigilance affected the detection and control of network attacks.

The researcher also analyzed data about top network victims. The victims were classified into three categories namely LAN victims with private IPs, LAN victims with public IPs and external computers falling victim of attacks from the LAN. Table 4 below summarizes the data on network victims.

Table 4: Network Attack Victims

Victims Category	Number of Attacks	Percentage	Cumulative Percentage
Organization's Private IPs	4275	17.2	17.2
Organization's Public IPs	48	0.2	17.4
Other Network's IPs	20578	82.6	100.0

Over the duration of the study, it was noted that 17.2 percent of local IP addresses were attacked and only 0.2 percent of the organization's public IPs were attacked. However, the bulk of the attacks were performed using the organization's IPs on other networks. Most of these cases were IP spoofing, where attackers from within and outside the LAN, having realized that they could not do much in the LAN with respect to their malicious intentions like hacking and denial of service, opted to use the organization's public IPs to try and attack other vulnerable networks in a bid to try and disguise themselves. As illustrated in figure 5, most of the attacks were as simple as ICMP pings.

A further study was done to test the effect of stratified vigilance on the victims of attacks. Top five attack victim IPs were selected for this analysis. As illustrated on figure 7 below, it was detected that for all the IPs, the number of attack detections increased steadily up to vigilance level four after which it declined sharply due to controls put in place to mitigate the threats. Thereafter, the considerably fewer unmitigated threats are escalated to human actor for unstructured decisions and subsequent actions.

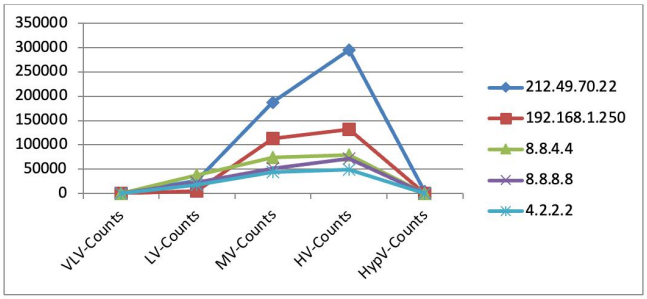

Figure 7: Effects of Vigilance on Network Victims

The IPs 192.168.2.250 and 212.49.70.22 appeared in the top five lists of attackers and victims. This confirmed that those IPs are victims of IP spoofing.

An analysis of the applications and ports that were being used to attack the network was also done. Table 5 below shows a summary of these applications/ ports and the number of attacks.

Table 5: Applications and Ports used to Attack the Network

Application/ Port	Number of Attacks	Percentage	Cumulative Percentage
ICMP:0	2476180	71.032	71.032
ICMP:256	906895	26.016	97.048
ICMP:3328	36178	1.039	98.087
UDP:1900	33070	0.949	99.040
UDP:80	28686	0.822	99.862
HTTP:80	4795	0.137	99.995
TCP: (Different Ports)	173	0.005	100.00

The port that was used most by attackers was ICMP:0 constituting 71.032 percent followed by ICMP:256 at 26.016 percent. The least risky applications were those running on TCP ports constituting 0.005 percent of the total number of attacks. It therefore means that an ICT

security specialist managing a network infrastructure needs to be more vigilant on ICMP:0 and ICMP:256.

Finally, we investigated the sources of attacks in terms of countries of origin. Table 6 below shows the cyber-attacks on the organization network based on countries where they originated.

Table 6: Cyber-attacks on the Network Based on Countries of Origin

Country	Number of Attacks	Percentage	Cumulative Percentage
Anonymous	1582515	45.40	45.40
Kenya	1236822	35.48	80.88
United States	487198	13.98	94.86
United Kingdom	12490	0.36	95.22
Russia	11776	0.34	95.56
Poland	10068	0.29	95.85
Australia	9998	0.29	96.14
India	9063	0.26	96.40
Italy	8694	0.25	96.65
Canada	7813	0.22	96.87
Others	109541	3.13	100.00

The results show that 45.40 percent, the highest proportion originates from anonymous sources. This owes to the fact that most cyber criminals attempt to hide their identity in a bid to protect themselves either from law enforcers or counter attacks. The second highest source of attacks is from Kenya, the country where the study was done, representing 35.48 percent. This may have been influenced by geographical proximity and local interest within the organization such as Computer Security and Forensic students who trying to breach the system on experimental basis to hone their skills. Apart from Kenya the other country in Africa where the highest attacks came from was Namibia at 0.20 percent. Thereafter the security of the network was adjusted to test the effect of vigilance on the volume of attacks on the network. The result was as shown in figure 8 below.

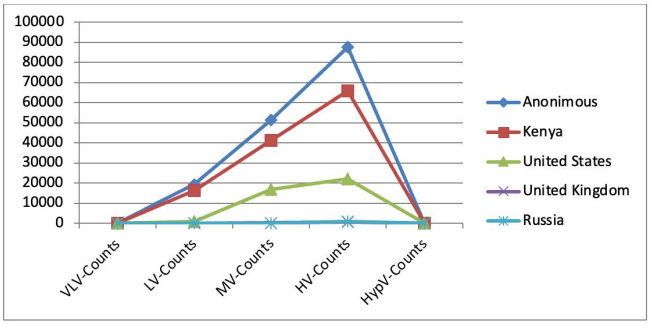

Figure 8: Effects of Vigilance on Attacks from Different Countries

The effect of variation of vigilance was that at lower level of vigilance, no detections were made. However, as vigilance increased, more detections were made until after level four where control were instituted to prevent the attacks, then there was a sharp decline in the number of detections.

V. Conclusion

The variation of vigilance on the information system from very low to low all the way up to hyper vigilance had profound effects on the security of the information system in terms of controlling logical threats and vulnerabilities. As demonstrated in the analysis of data used in this study, at very low vigilance there is false sense of security where many threats and active attacks go un-noticed. The same applies to many system vulnerabilities that go undetected. However, as vigilance increases, threats and attacks are detected and controlled thereby increasing security of the information systems tremendously. The research therefore concludes that organizations need to ensure that they deploy hyper-vigilance systems that continuously monitor, detect, report and control logical threats and vulnerabilities in order for their systems to remain secure.

References

[1] Schmitt, M. (2023); Securing the Digital World: Protecting smart infrastructures and digital industries with Artificial Intelligence (AI)-enabled malware and intrusion detection*; Journal of Industrial Information Integration, December 2023.*

[2] Uddin, M., Irshad, M.S., Kandhro, I.A. *et al.* (2025) Generative AI revolution in cybersecurity: a comprehensive review of threat intelligence and operations. *Artif Intell Rev* **58**, 236 (2025). https://doi.org/10.1007/s10462-025-11219-5

[3] Salem, A.H., Azzam, S.M., Emam, O.E. *et al.* Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. *J Big Data* **11**, 105 (2024). https://doi.org/10.1186/s40537-024-00957-y

[4] Danish, M. (2024). *Enhancing Cyber Security through Predictive Analytics: Real-Time Threat Detection and Response***.** Published on **arXiv** July 15, 2024 (arXiv:2407.10864

[5] Parasuraman, R., & Galster, S. (2020). Human Performance in Vigilance Tasks. In Cognitive Engineering and Human Factors.

[6] Langner, R., & Eickhoff, S. B. (2020). Sustaining attention to simple tasks: A meta-analytic review of the neural mechanisms of vigilant attention. *Psychological Bulletin*, 146(6), 489–507.

[7] Thompson, G., Walker, B., & Miller, L. (2023). Vigilance and Performance Monitoring in Safety-Critical Systems. *Applied Ergonomics*, 110, 103931.

[8] Pandey, S. K. (2012), Security Vigilance System Through Level Driven Security Maturity Model; *International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol.2, No.2.*

[9] Klösch, G., Zeitlhofer, J., & Ipsiroglu, O. (2022) authored the Perspective article *"Revisiting the Concept of Vigilance"* in Frontiers in Psychiatry**,** volume 13, article 874757**.**

[10] Oken, B. S, Salinsky, M. C., Elsas, S. M. (2006); Vigilance, alertness, or sustained attention: Physiological basis and measurement; *Published in final edited form as:* Clin Neurophysiol. 2006 Apr 3;117(9):1885–1901. doi: 10.1016/j.clinph.2006.01.017

[11] Alarbad, A. H., Alsharif, A. M. & Sati, S. O. (2024); Campus Network Design for Information Technology Faculty; *Int. J. Advanced Networking and Applications Volume: 15 Issue: 06 Pages: 6211 – 6217 (2024) ISSN: 0975-0290*

[12] Quader, F. & Janeja, V. P. (2021); Insights into Organizational Security Readiness: Lessons Learned from Cyber-Attack Case Studies; *J. Cybersecur. Priv.* 2021, *1*, 638–659. https://doi.org/10.3390/jcp1040032

[13] Deloitte whitepaper (2014), Transforming cyber security in the Financial Services Industry New approaches for an evolving threat landscape; retrieved from: *www2.deloitte.com/content/dam/.../ZA_ Transforming_Cybersecurity_05122014.pdf*

[14] Deloitte whitepaper (2021), Cybersecurity in a post-pandemic world: A focus on financial services; Retrieved on 21st August, 2025; from: https://www.deloitte.com/na/en/services/risk-advisory/perspectives/gx-financial-services-cybersecurity-global-organizations.html?utm_source=chatgpt.com

[15] National Institute of Standards and Technology –NIST SP (2024), Building a Cybersecurity and Privacy Learning Program; *NIST Special Publication 800, NIST SP 800-50r1. Retrieved on 25th July, 2025 from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/ NIST.SP.800-50r1.pdf*

[16] Greenwald, G. (2014), No Place to Hide: Edward Snowden, the NSA & the Surveillance State; Penguin Random House, UK.

[17] M-Trends report 2022*: Cyber security metrics, insights and guidance from frontline investigations*. Retrieved on 25th July, 2025, from: https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2022?utm_source=chatgpt.com

[18] ReliaQuest Threat Research Team. (2024). *ReliaQuest Annual Cyber-Threat Report: 2024* [Threat report]. ReliaQuest. Retrieved on 25th July, 2025; from ReliaQuest website: https://reliaquest.com/resources/research-reports/annual-threat-report-2024/?utm_source=chatgpt.com

[19] Stewart, J. M., & Chapple, M. (2024), CISSP: ISC² CISSP Certified Information Systems Security Professional Official Study Guide, 10th Edition. Sybex Inc.: London

[20] Awodele, O., Onuiri, E. E. & Okolie, S. O. (2012), Vulnerabilities in Network Infrastructures and Prevention/ Containment Measures: Proceedings of Informing Science & IT Education Conference (InSITE).

[21] O'Brien, J. A. & Marakas, G. M. (2011). Management Information Systems, 10th ed. McGrow-Hill/ Irwin: New York

[22] Laudon, K. C. & Laudon, J. P. (2013). Management Information Systems: Managing the Digital Firm, 12th ed. Dorling Kindersley (India) Pvt. Ltd: New Delhi

[23] Goyal, A. (2011), Systems Analysis and Design. Asoke K. Ghosh, PHI Learning Private Limited: New Delhi

[24] Kothari, C. R. & Garg, G. (2014): Research methodology: Methods and techniques. New Delhi: New Age International (P) Ltd, Publishers.

[25] Nzioki, P.M., Kimeli, S. K., Abudho, M. R., Nthiwa, J. M. (2013): Management of working capital and its effects on profitability of manufacturing companies listed at NSE, Kenya: *International Journal of Business & Financial Management Research, 1:35-42.*

[26] Farooq, U. (2013), Types of Research Design. *Referred Academic Journal, 08:21*