Indian Journal of Information Sources and Services
ISSN: 2231-6094 (P) Vol.15, No.2, 2025, pp.154-159

DOI: https://doi.org/10.51983/ijiss-2025.IJISS.15.2.21

A Study on the Adoption of Threat Prevention and Dark Web Monitoring for Information Security Management in India

S. Guru Prasad[1*] and Dr.M.K. Badrinarayanan[2]

[1*]Research Scholar, School of Management, Hindustan Institute of Technology & Science, Chennai, India
[2]Professor & Head, School of Management, Hindustan Institute of Technology & Science, Chennai, India
E-mail: [1]guru@cybertracs.in, [2]mkbadri@hindustanuniv.ac.in
ORCID: [1]https://orcid.org/0009-0008-2371-8871, [2]https://orcid.org/0000-0001-6341-5770
(Received 28 February 2025; Revised 04 April 2025, Accepted 23 April 2025; Available online 25 June 2025)

Abstract - **World over, organizations are facing the threat of breaches of the Information Technology systems and networks they have deployed. Growing threats to the Information Technology assets, Data, Networks, and Systems put a lot of pressure on organizations and they have to deploy, the right set of technologies and solutions, right set of people and processes to prevent such threats. Protection of the Information technology assets against such breaches and attacks is an important task in every organization. This article aims to study if the Chief Information Security officers have taken adequate steps and measures to protect the organization against threats. This article aims to study if they have deployed threat prevention measures and/or used proactive threat monitoring and management measures.**

Keywords: **Threat Prevention Adoption, Dark Web Monitoring, Information Security Management**

I. INTRODUCTION

Communications across the globe have been dominated by the Internet over the past two decades. The Internet has played a significant role. It has been integrated into the lives of everyone around the world. Continuous research and development leading to Innovations in the communications industry and cost-benefit achieved over a period in this area has increased the availability, use, and performance of the Internet in a significant manner.

Organizations worldwide have invested in Information Technology which helps them in their businesses (Al-Assadi & Al Kaabi, 2024). Information Technology plays a major role in achieving their business goals. In India too that trend is felt. Organizations use computers, laptops, mobile phones, the internet, and associated devices for communication. They use storage technologies to store and transmit the Information. Securing the Information Technology Assets of an organization is an important task since the Information stored in digital form is very important (Agrafiotis & Kul, 2021).

All organizations have a team of experts dedicated to managing their Information Technology assets. All organizations have a team of Cybersecurity experts dedicated to defending their organization against any Cyber threats or cyberattacks and data breaches on their Information technology assets. This team is usually led by a Chief Information Security Officer (CISO). We surveyed 30 CISOs of various organizations to understand the Threat Prevention Technologies and solutions they have deployed, to defend and protect their organization's Information technology assets against any form of internet-based attacks and threats. In our survey, we tried to find out if they are using Threat Prevention solutions to prevent any type of attacks, and Security Information and Event Management (SIEM)/Security Operations Centre (SOC) to monitor the alerts from all the security technologies deployed in their organization (González-Granadillo et al., 2021).

In our survey, we also tried and checked with them if they are using any proactive monitoring solutions to defend their organization's Information Technology assets. The objectives of the study are

1. To Study if the organizations in India are deploying Firewall/Unified Threat Management solutions, End Point Protection solutions, and Data leak prevention solutions to defend their network, endpoint, and data from any attacks or breaches.
2. To Study if the organizations are using Vulnerability Assessment Solutions, Security Information and Event Management (SIEM)/Security Operations Centre (SOC) and Dark Web Monitoring solutions for Proactive defense against any attacks or breaches (Thevenon et al., 2022).

II. ABOUT THE STUDY

This study was conducted through a questionnaire using Google Forms. This was sent to their Email IDs. This study was done with the Chief Information Security Officers (CISOs) in India. For this study, the respondents were categorized based on the number of users of Information Technology Devices connecting to the organization's data center (Singh & Katiyar, 2024). They are categorized into 1-500 users, 500-1000 users, 1000-2000 users and, above 2000 users. The survey was conducted with the CISOs in various industry segments like Private Manufacturing, Public Sector Undertaking, BFSI, Education, and IT/ITES.

Below is the industry-wise breakup of the respondents.

TABLE I INDUSTRY-WISE BREAKUP OF THE RESPONDENTS

Industry	Respondents
Education & Research	10.00%
BFSI	10.00%
IT/ITES	50.00%
Manufacturing	16.67%
PSU/Govt	13.33%
Total	**100.00%**

Source: Compiled by Author

The above Table, Table I shows the industry-wise breakup of the respondents.

III. CYBER THREATS AND ITS DIMENSIONS

Organizations across the globe, depend on electronic Technology for storing their information, sharing their information, and communication (Anto Lourdu Xavier Raj & Mario Macrina, 2021). In this process they deploy the required Technology products and solutions for storing, sharing, and communication. These products and solutions deployed are very critical for organizations and protecting them from cyber-attacks is a challenging issue. The purpose of most of the Cyber-attacks is to create a disruption to the target organization and to create financial losses. With the advancement of technology, challenges in managing them and securing them have become very challenging.

IV. CYBER SECURITY THREATS AND SOLUTIONS

Organizations in India and the world are facing various Cyber Security Threats that happen over the internet, frequently. Ransomware, Viruses, Malware, Network intrusions, Unauthorized access, Malicious URLs, Botnets, Data Leaks, Vulnerabilities, and Denial of Service are some forms of Cyber Security threats. Cyber threat prevention measure or framework is a comprehensive program that includes practical actions like deployment of solutions to protect information, data, and networks against any internal or external threats. Cyber-Security experts in the organization make sure that they protect networks, servers, intranets, and computer systems. Cyber-security measures are created by the experts in such a way that ensures that only authorized individuals have access to that information. Some of the solutions available in the market to protect organizations from various attacks are Firewalls, Intrusion Prevention Systems (IPS), Anti-Virus, Anti-Malware, Uniform Resource Locator (URL) protection, Botnet protection, Application Protection, Data Leak Prevention, Anti-Ransomware, Vulnerability Management, Denial of Service protection.

Organizations install Firewalls to protect their network. Firewalls are important in protecting the computer networks. Firewalls are of two types namely, host-based firewalls and network firewalls. Network firewalls provide protection against different types of networks. This runs on hardware connected to the network. Host-based firewalls filter the traffic that flows to the endpoints (Sheth & Thakker, 2011).

Unified threat management (UTM) is a comprehensive technology with features like anti-virus, intrusion detection system or intrusion prevention system (IDS or IPS), spam filtering, and Web content filtering, together with the basic functions of a firewall. The proxy in the solution helps to process and forward all incoming traffic. They work in the application layer. They can work in a transparent mode. A firewall is a hardware device that is configured to allow, deny, encrypt, and decrypt, all computer network traffic between different networks that are managed based on a set of rules that are created. A firewall is a dedicated technology, with dedicated hardware and software. It does the inspection of the network traffic passing through it and allows or denies the data to pass through based on a set of rules (Agham, 2016).

Generally, Anti-Virus and Intrusion Prevention Systems (IPS) are included in a "traditional" UTM firewall. These features are designed to create a protection layer between the company's network and the Internet (Snyder & One, 2016).

Anti-malware software is generally used as the first line of defense at the desktop/laptop level against malware attacks. It is also known as anti-virus software. It must be kept up to date with the latest signatures to provide effective prevention from the various attacks that come through email, software, and any vulnerabilities in the network. (Symantec Labs 2017).

According to Palo Alto Networks, a category of tools used to detect and investigate threats on endpoints is called Endpoint detection and response (EDR). EDR tools generally provide investigation, detection, threat hunting, and response capabilities. In the protection of endpoints in any organization, Endpoint detection and response have become a critical component (www.paloaltonetworks.com).

Check Point's endpoint security includes data security, network security, advanced threat protection, endpoint forensics, remote access VPN solutions, and endpoint detection and response (EDR) (www.checkpoint.com).

The Unauthorized exchange of data between one organization and an external destination or recipient is called a Data Leak. The release of confidential or sensitive information to unauthorized users is called a data breach or data leak (Anbarasi et al., 2015). Data leaks can happen because of an unintentional loss or exposure of data, an intentional leak by employees of the organization, and/or a programmer assault. In this process, the data is transferred electronically or physically by unauthorized means. Data leak usually occurs via optical media, USB keys, laptops, the web, and email (Jadhav & Chawan, 2019).

A vulnerability is a security flaw, which arises from the design of the computer system, its implementation, its maintenance, and its operation (Wang & Guo, 2009).

Security Information and Event Management (SIEM) is a tool used to collect, aggregate, store, and correlate events

generated from all the security controls deployed in a managed infrastructure (Miller et al., 2010).

Security Information and Event Management (SIEM) systems are usually deployed to monitor the security information, and security events and also as a powerful tool to provide prevention, detection, and help in acting and responding against cyber-attacks. SIEM solutions provide comprehensive visibility to identify the high-risk areas and proactively focus and plan on responses and strategies towards reducing costs and the time taken to respond to an incident in case it happens (Miller et al., 2010).

Apart from deploying Threat Prevention technologies and strategies, large organizations are deploying solutions to do proactive monitoring of their assets and thus preventing them from any data leak or attack from unauthorized sources. Two such technologies are Dark Web monitoring tools and Vulnerability Assessment.

In this paper, we shall try and find out how the above-discussed threats are managed by various solutions in various organizations in India. We also try and check if these organizations are using any proactive monitoring mechanisms like Dark web monitoring.

4.1 Firewall/UTM

Firewall/UTM is the first line of defense for the organizations Network. Firewall systems are made and used to filter the traffic based on IP addresses, source addresses, destination addresses, and protocol types (Liu et al., 2003).

S.Cobb in an IEEE conference in June, 1996 discussed the use of a Firewall and its importance. The firewalls that are commercially available in the market are very powerful. They are usually to be near the top of the agenda for those organizations who are thinking of creating, a connection between their office network and another network. However, only firewalls, cannot do the whole job. A firewall system enforces an access control policy between two networks. A firewall is a collection of components that is placed between two different types of networks and allows, all authorized traffic as defined in the company's security policy, from the inside network to the outside network, and vice-versa (Perera et al., 2021). The system is designed to be immune to breach by penetration (Cobb, 1996).

A Firewall is a software running on computer hardware. It inspects the data in the network that is passing through it, and allows or denies the passage of network traffic based on a set of rules. Network address translation (NAT) is a functionality the firewalls have, and the hosts that are protected behind a firewall have addresses in the "private address range". Firewalls can hide the true address of protected hosts (Qi et al., 2007).

Unified threat management (UTM) is a technology solution with software components like an anti-virus, intrusion detection system or intrusion prevention system (IDS or IPS), spam filtering, and Web content filtering, along with the basic functionalities of a firewall (Agham, 2016).

An UTM aims to simplify the perimeter security solution and create a consolidation. The physical consolidation of various point products into a consolidated technology, hence it is called unified threat management (Agham, 2016).

As the hardware powering the enterprise network firewalls became more and more powerful and nowadays, it became possible to add more functions that were traditionally used separately, right into the firewall.

4.2 End Point Detection & Response/End Point Protection (EDR/EPP)

Any device, like a Laptop, Desktop, or OT/IoT device connected to a computer network is called an endpoint. Each endpoint may potentially cause a threat to the computer network that could lead to leakage of data. With more advancements in technology, the number of individual devices that are getting connected to the network is also increasing. Endpoint Detection systems collect data from endpoints deployed in a network and store and process them in its database. Then they correlate the events that are reported in real time to detect any anomalies in the behavior of the host (Sjarif et al., 2019).

Endpoint Detection and Response (EDR) systems provide a more comprehensive approach to the security of an organization. EDRs collect the information and events across multiple hosts of an organization, and correlate them to provide actionable intelligence. Therefore, individual events from endpoints that may get missed during the normal course of action are collected, processed, and correlated, providing the organization and its security officers with clear intelligence into the threats that the perimeter is potentially exposed to (Karantzas & Patsakis, 2021).

4.3 Data leak Prevention (DLP)

The unauthorized exchange of data or information between an organization and an external destination or recipient is called a Data Leak. (www.gartner.com)

The DLP technology has a solution that provides visibility into the data in the organization, its usage, and the movement of data across an organization or its network. DLP technology addresses data-breach related threats, including the risks of the sensitive data leak to unauthorized sources and accidental data loss to unauthorized sources. It involves enforcement of data security policies based on content and/or context for data in transit and or for data at rest. It uses monitoring, alerting, warning, blocking, and quarantining features for data leak prevention (Hutchins et al., 2015).

Data leak prevention focuses on preventing the unauthorized transfer of data outside institutional boundaries. The term data leak refers to an event in which important information or important data is leaked to an unauthorized environment. The

term DLP refers to defending organizations against both data loss and data leak prevention (Hutchins et al., 2015).

The Below Table gives the summary of the survey done among the Chief Information Security Officers (CISOs) to check how many of them have deployed Firewall/UTM, EDR/EPP, and Data Leak Prevention (DLP) solutions in their Networks (Bhatt et al., 2014).

TABLE II COMPANY SIZE AND NUMBER OF RESPONDENTS FOR THE USAGE OF TECHNOLOGIES FOR THREAT PREVENTION

Company Size (Users)	Respondents using Firewall/UTM	Respondents using EDR/EPP	Respondents using DLP	Total Respondents
1-500	9	5	3	9
501-1000	5	2	2	5
1001-2000	6	4	3	6
2001 and above	10	8	6	10
	30	**19**	**14**	**30**

Source: Compiled by Author

The above table, Table II, shows the size of the respondents' company, and the number of respondents who have adopted Firewall/UTM, EDR/EPP, and DLP.

From the above table we can infer the following:

All the Companies are using Firewalls/UTM as the first line of defense.

The larger the size of the company, the better the deployment of Threat-Prevention technologies.

Awareness about EDR/EPP and DLP is less among smaller companies.

4.4 Vulnerability Assessment

Vulnerability is a weakness that exists in the existing system and is susceptible to an attack. It can be a computing element such as a weak software program or sharing of the confidential files without encryption. This has the potential to create damage to the enterprise, organization, individual, program, or a piece of equipment susceptible to an attack (Nath, 2011).

Vulnerability assessment can be defined as the process of understanding the existence of vulnerabilities in the system process or network, assessing the risks due to them and prioritizing them before implementing solutions to mitigate the risks due to the vulnerabilities (Deraison & Gula, 2004).

Vulnerability Assessment is an active use of a network scanner to find vulnerabilities in hosts, services, programs, and networks. (www.gartner.com)

The vulnerability assessment (VA) solutions market is made up of vendors who have the capabilities to identify, categorize, and manage vulnerabilities including missing patches, system configurations that have security issues, and other security-related updates in the systems connected to the enterprise network or in the cloud. (www.gartner.com)

V. CYBER THREAT MONITORING AND MANAGEMENT - TECHNICAL CHALLENGES

CISOs of various organizations, do not get a view of what's happening in their network. This may be due to the lack of visibility of various technologies used and the reports that it generates. Even if the organization uses the best of the solutions to get this visibility of the happenings in their network, they will have to look into various reports, and dashboards and then work on it. This becomes a tedious process due to a lack of resources, lack of knowledge, and lack of time. To overcome these challenges, organizations use Security information and event management (SIEM), Security Orchestration, Automation and Response (SOAR). Most organizations have a Security Operations Centre (SOC). Security information and event management (SIEM) technology refers to the technology that is used in the collection of Security information, and events in the network which is used in threat detection, Information Security compliance, and Information security incident management. This is done in both, near real-time and historical collection and analysis of security events, a wide variety of other events, and contextual data sources. SIEM collects all the logs from the connected devices in the network and does analysis. It stores them and gives actionable intelligence and reports. (www.gartner.com)

Security Orchestration, Automation, and Response (SOAR) refer to technologies that help the orchestration, and automation of the response to security incidents, events, and information. SOAR platform enables organizations to collect inputs that can monitored by the security operations team. It collects alerts from the SIEM system and other security technologies. SOAR performs Incident and event analysis by leveraging a combination of people and technology. SOAR tools have a playbook in which an organization can define incident analysis and response procedures (Gartner, 2017).

A security operations center (SOC) consists of a team, and a facility dedicated to and organized to detect, assess, respond, and prevent cybersecurity threats and incidents, and to fulfill and assess the required regulatory compliances (Schäfer et al., 2019).

5.1 Dark Web Monitoring

Dark Web monitoring technology could be used by organizations to augment their threat prevention capabilities. This technology helps in proactive monitoring and defense against any potential threats or breaches.

The Dark Web is an area in the World Wide Web that is not accessible by normal web browsers. It is a set of illegal services hidden from regular, normal search engines and regular web browsers. It is used by cybercriminals who offer various illegal goods and services. The Dark web has information regarding zero-day exploits, stolen datasets with

login information, or botnets. They are available for hire or sale on the Dark Web (Kaur & Randhawa, 2020).

The Dark web is an untraceable hidden layer of the Internet or World Wide Web. It is used by illegal users to store and access confidential information (Datta et al., 2020).

The Dark Web is the platform used by hackers to leak sensitive data stolen from various organizations or individuals. 9.7 GB of data of 32 million Ashley Madison customers was posted on the dark web by a hacker group. Over 1.4 billion personal records of the company were leaked over the dark web as plain text (Datta et al., 2020).

TABLE III COMPANY SIZE AND NUMBER OF RESPONDENTS FOR THE USAGE OF MONITORING TECHNOLOGIES

Company Size (Users)	Respondents using VA Solutions	Respondents using SIEM/SOC	Respondents using Dark Web	Total Respondents
1-500	5	3	2	9
501-1000	3	2	0	5
1001-2000	5	6	3	6
2001 and above	7	8	5	10
	20	**19**	**10**	**30**

Source: Compiled by Author

The above table, Table III, details the respondents' company size in terms of the number of users and the various threat-monitoring technologies they have adopted.

From the above table, we can infer the following.

The smaller companies show moderate adoption of VA Solutions, but lower adoption of SIEM/SOC. And Dark Web monitoring. This could indicate budget constraints or less perceived need for advanced security measures in smaller organizations.

Adoption increases notably, for larger companies. Larger companies tend to have more complex IT environments and thus see the need for robust security measures.

VI. ANALYSIS OF VARIANCE

Below is the table showing the Analysis of Variance (ANOVA)

TABLE IV ANALYSIS OF VARIANCE

Technologies		Sum of Squares	df	Mean Square	F	Sig.
Firewall/ UTM	Between Groups	0.000	3	0.000		
	Within Groups	0.000	26	0.000		
	Total	0.000	29			
EDR/EPP	Between Groups	0.611	3	0.204	0.833	0.488
	Within Groups	6.356	26	0.244		
	Total	6.967	29			
DLP	Between Groups	0.400	3	0.133	0.488	0.693
	Within Groups	7.100	26	0.273		
	Total	7.500	29			
Dark Web Monitoring	Between Groups	1.111	3	0.370	1.733	0.185
	Within Groups	5.556	26	0.214		
	Total	6.667	29			
VA/PT	Between Groups	0.311	3	0.104	0.424	0.737
	Within Groups	6.356	26	0.244		
	Total	6.667	29			
SIEM /SOC	Between Groups	1.900	3	0.633	3.107	0.044
	Within Groups	5.300	26	0.204		
	Total	7.200	29			

Source: Statistical Analysis

The above table, Table IV, gives the Analysis of variance (ANOVA). The results of the ANOVA analysis presented here suggest that the factors related to the adoption of SIEM/SOC solutions have resulted in varying outcomes among the groups. It indicates statistical significance ($p=0.044$) (Perera et al., 2021; Bhatt et al., 2014; Sheth & Thakker, 2011). This implies that the implementation and operation of SIEM/SOC solutions have a significant impact on the overall information security protection of the organizations in India. In contrast, the analysis found no statistically significant differences between groups for other threat prevention and monitoring technologies, such as EDR/EPP, DLP, Anti-Ransomware, Dark Web Monitoring, and Vulnerability Assessment.

The critical role of Security Information and Event Management (SIEM) solutions in the implementation and operation of a SOC is well-documented in the literature. SIEM systems collect security-related information and security events from multiple technologies deployed within the enterprise network, normalize the data, and provide real-time correlation and analysis. This helps in identifying malicious activities. The effectiveness of the SOC can be further enhanced through the integration of complementing technologies like threat hunting, threat intelligence, and machine learning-based anomaly detection into the SOC. This can help in reducing false positives and increase the overall efficiency and accuracy.

VII. CONCLUSION

This study, shows us that, the CISOs of various organizations in India are aware of threat prevention and proactive threat monitoring and management measures. A Firewall/UTM is the first line of defense in any organization and 100% of the CISOs have confirmed that they are using Firewall/UTM. More than 60% of the organizations are using various Technologies to prevent threats. Adoption of these threat prevention technologies is better and higher in organizations having more than 1000 users.

The adoption of Prevention and Proactive monitoring is not 100%. If it is 100% then the risk towards the organizations will be very minimal or negligible. A further study to identify

the reasons for this non-adoption can help the industry to reduce the number of breaches, and compromises. In this study, various factors like resource availability, awareness, knowledge, funds availability, inter-operability issues, top management mind share, and ability of the CISOs to convince the management can be studied.

REFERENCES

[1] Agham, V. (2016). Unified threat management. *International Research Journal of Engineering and Technology, 3*(4), 32-36.

[2] Agrafiotis, I., & Kul, G. (2021). Guest Editorial: Special Issue on Advances in Insider Threat Detection. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 12*(2), 1-2.

[3] Al-Assadi, K. H. F., & Al Kaabi, A. A. (2024). Geomorphological Changes of the Terrestrial Features of the Euphrates River between the Cities of Al-Kifl and Al-Mishkhab Using Geographic Information Systems (GIS). *Natural and Engineering Sciences, 9*(2), 347-358. https://doi.org/10.28978/nesciences.1574446

[4] Anbarasi, K., Gayathri, R., Venkatesa Kumar, P., & Newlin Rajkumar, M. (2015). Intrusion Detection using Naive Bayes Classifier with Feature Reduction. *International Journal of Advances in Engineering and Emerging Technology, 6*(3), 72–80.

[5] Anto Lourdu Xavier Raj, A., & Mario Macrina, A. (2021). Multiple Heterogeneous Information Source. *International Academic Journal of Science and Engineering, 8*(1), 45–52. https://doi.org/10.9756/IAJSE/V8I1/IAJSE0806

[6] 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.

[7] Check Point. (n.d.). Check Point endpoint security. Retrieved from https://www.checkpoint.com/solutions

[8] Cobb, S. (1996). Establishing firewall policy. *Southcon/96 Conference Record,* 198-205. https://doi.org/10.1109/SOUTHC.1996.535065

[9] Datta, P., Lodinger, N., Namin, A. S., & Jones, K. S. (2020). Cyber-attack consequence prediction. https://doi.org/10.48550/arXiv.2012.00648

[10] Deraison, R., & Gula, R. (2004). Blended Security Assessment: Combining Active, Passive and Host Assessment Techniqiues. *Tenable network security*, *78*.

[11] Gartner. (2017). Security operations centers and their role in cybersecurity. https://www.gartner.com/en/newsroom/press-releases/2017-10-12-security-operations-centers-and-their-role-in-cybersecurity

[12] Gartner. (n.d.). Data loss prevention. https://www.gartner.com/reviews/market/data-loss-prevention

[13] Gartner. (n.d.). Security information and event management. https://www.gartner.com/en/information-technology/glossary

[14] Gartner. (n.d.). Security orchestration, automation, and response (SOAR). https://www.gartner.com/en/information-technology/glossary/security-orchestration-automation-response-soar

[15] Gartner. (n.d.). Vulnerability assessment. https://www.gartner.com/en/information-technology/glossary/vulnerability-assessment

[16] González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures. *Sensors, 21*(14), 4759.

[17] Hutchins, M. J., Bhinge, R., Micali, M. K., Robinson, S. L., Sutherland, J. W., & Dornfeld, D. (2015). Framework for identifying cybersecurity risks in manufacturing. *Procedia Manufacturing, 1,* 47-63. https://doi.org/10.1016/j.promfg.2015.09.060

[18] Jadhav, P., & Chawan, P. (2019). Data leak prevention system: A survey. *Virus, 6*(10), 197-199.

[19] Karantzas, G., & Patsakis, C. (2021). An empirical assessment of endpoint detection and response systems against advanced persistent threats attack vectors. *Journal of Cybersecurity and Privacy, 1*(3), 387-421. https://doi.org/10.3390/jcp1030021

[20] Kaur, S., & Randhawa, S. (2020). Dark web: A web of crimes. *Wireless Personal Communications, 112,* 2131-2158. https://doi.org/10.1007/s11277-020-07143-2

[21] Liu, T., Gao, H., & Zhang, Q. (2003). The enterprise firewall and its foundation. *Journal of Hebei Agricultural University, 26*(2), 89-92.

[22] Miller, D., Harris, S., Harper, A., Van Dyke, S., & Blask, C. (2010). *Security information and event management (SIEM) implementation.* New York, NY: McGraw Hill.

[23] Nath, H. V. (2011). Vulnerability assessment methods - A review. *Communications in Computer and Information Science, 196,* 1-10. http://dx.doi.org/10.1007/978-3-642-22540-6_1

[24] Palo Alto Networks. (n.d.). What is endpoint detection and response (EDR)? https://www.paloaltonetworks.com/cyberpedia/what-is-endpoint-detection-and-response-edr

[25] Perera, U. N. A., Rathnayaka, S., Perera, N. D., Madushanka, W. W., & Senarathne, A. N. (2021, April). The next gen security operation center. In *2021 6th International Conference for Convergence in Technology (I2CT)* (pp. 1-9). IEEE.

[26] Qi, Y., Yang, B., Xu, B., & Li, J. (2007, June). Towards system-level optimization for high performance unified threat management. In *International Conference on Networking and Services (ICNS'07)* (pp. 7-7). IEEE.

[27] Schäfer, M., Fuchs, M., Strohmeier, M., Engel, M., Liechti, M., & Lenders, V. (2019, May). BlackWidow: Monitoring the dark web for cyber security information. In *2019 11th International Conference on Cyber Conflict (CyCon)* (Vol. 900, pp. 1-21). IEEE. https://doi.org/10.23919/CYCON.2019.8756845

[28] Sheth, C., & Thakker, R. (2011, February). Performance evaluation and comparative analysis of network firewalls. In *2011 International Conference on Devices and Communications (ICDeCom)* (pp. 1-5). IEEE.

[29] Singh, N., & Katiyar, S. K. (2024). Developing information system on blackspot severity for travellers by using python and gis techniques. *Archives for Technical Sciences, 2*(31), 284-295. https://doi.org/10.70102/afts.2024.1631.284

[30] Sjarif, N. N. A., Chuprat, S., Mahrin, M. N. R., Ahmad, N. A., Ariffin, A., Senan, F. M., ... & Saupi, A. (2019, October). Endpoint detection and response: Why use machine learning?. In *2019 International Conference on Information and Communication Technology Convergence (ICTC)* (pp. 283-288). IEEE.

[31] Snyder, J., & One, O. (2016). Evaluating Unified Threat Management Products for Enterprise Networks. *Opus One*.

[32] Thevenon, P. H., Riou, S., Tran, D. M., Puys, M., Polychronou, N. F., Majihi, M. E., & Sivelle, C. (2022). iMRC: Integrated Monitoring & Recovery Component, a Solution to Guarantee the Security of Embedded Systems. *Journal of Internet Services and Information Security, 12*(2), 70-94. https://doi.org/10.22667/JISIS.2022.05.31.070

[33] Wang, J. A., & Guo, M. (2009, April). OVM: an ontology for vulnerability management. In *Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies* (pp. 1-4).