Journal of Ecohumanism
2025
Volume: 4, No: 3, pp. 322 – 333
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i3.6644

Implementing Robust Cyber Security Strategies to Protect Small Businesses from Potential Threats in the USA

Anamika Tiwari[1], Barna Biswas[2], Md Azharul Islam[3], Md Imran Sarkar[4], Sanchita Saha[5], Mohammad Zahidul Alam[6], Syeda Farjana Farabi[7]

Abstract

The increasing threat of cyber-attacks is a significant concern for organizations, particularly those in the USA. To mitigate these risks effectively, organizations must employ competent IT security professionals to implement effective security controls. However, there is a shortage of cyber security talent in the job market, necessitating extensive education and training. A good cyber security education program should be supported by a cyber security lab equipped with various software, equipment, and tools used by real professionals in the industry. This paper proposes a model of a cyber security lab equipped with honeypot and SIEM systems to enhance the quality of cyber security education. The research provides students with experience analyzing the behavior of hackers, while the SIEM system aggregates logs data of the Campus Network Firewall in real time. Security information and event management (SIEM) is a security solution that helps organizations recognize and address potential security threats and vulnerabilities before they disrupt business operations. SIEM systems help enterprise security teams detect user behavior anomalies and use artificial intelligence (AI) to automate many of the manual processes associated with threat detection and incident response. This research study aims to explore the defensive security strategies needed by small businesses in the USA to protect their information assets. Many businesses lack proper security tools, policies, and procedures, leaving them vulnerable to cyber-attacks. The research question is what strategies cyber security managers need to improve their cyber defense in small businesses in the USA.

Keywords: *Small Business Strategies, Security Threats, Cyber Security, Cyber Help, The SIEM System.*

Introduction

Information technology (IT) has significantly improved service provision flexibility and reliability, making it increasingly crucial for both commercial and non-commercial firms. However, businesses are increasingly concerned about protecting essential IT devices from cybercriminals, which can lead to hacking, intrusion, money theft, and confidential information theft. As organizations increasingly move to the cloud, new data breaches and vulnerabilities are likely to occur[1]. Most organizations worldwide lack coordinated activities on IT security-related issues, such as cyber security, highlighting the need for improved cyber security measures. Cyber security professionals in small businesses face the challenge of protecting their assets from cyber-attacks, as they depend on every single user and are perceived as gateways or attack vectors[2]. Defensive cyber security strategies are essential for small businesses to protect their information assets, but many struggle to protect critical assets and provide an environment where data is safeguarded. Cybercriminals target small businesses with weak cyber security defenses because it is easy to exploit their business vulnerabilities.

The online version of the Oxford English Dictionary defines security as "the state of being free from danger or threat." However, cyber security is a complex term used by various professionals, including politicians, computer specialists, IT managers, and health industry professionals. The term covers government institutions' measures to protect the public and themselves from cyber threats, as well as individual protection against viruses and malware on computers. The definition of cyber security is less clear, as it

[1] Department of Business Administration, Westcliff University, Email: a.tiwari.8501@westcliff.edu
[2] Department of Technology & Engineering, Westcliff University, Email: B.Biswas.133@westcliff.edu.
[3] Department of Business Administration, Westcliff University, Email: m.islam.552@westcliff.edu.
[4] Department of Information Technology, Westcliff University, Email: m.sarkar.129@westcliff.edu.
[5] Department of Business Administration, Westcliff University, Email: s.saha.552@westcliff.edu
[6] Department of Information Technology, Westcliff University, Email: m.alam.154@westcliff.edu
[7] Department of Business Administration, Westcliff University, Email: s.farabi.184@westcliff.edu

Journal of Ecohumanism
2025
Volume: 4, No: 3, pp. 322 – 333
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i3.6644

does not specify which threats it secures against. Attempts to define cyber security have been made since the end of the Cold War[3].

The U.S. Small Business Administration defines small businesses as privately owned corporations, partnerships, or sole proprietorships with fewer employees and annual revenue. These businesses face unique challenges, such as fewer human resources and up-front capital, but can implement quality management systems found in larger corporations[4]. Upper management commitment and accessibility can be stronger in small businesses, and internal communications can be more straightforward. Organizational values, expressed by concepts such as values, mission, vision, policies, and objectives, are essential for small business culture development. These concepts are established by leadership and adopted by personnel, contributing to the overall success of the business[5]. Small businesses often view investment in cyber security as discretionary spending rather than an essential cost critical for long-term survival in the market. Cyber attacks have skyrocketed worldwide due to the limited resources, lack of technology, and inability to launch multi-faceted defenses. Small businesses viewed investment in cyber security as discretionary spending rather than an essential cost critical for long-term survival in the market[6, 7].

Advanced persistent threat (APT) attacks are on the rise, targeting small, medium, and large enterprises. The impact of a cyber-incident is disproportionately high for the smallest companies because they typically have fewer resources for cyber-attack readiness even when the cyber threat is imminent[8]. Small businesses are more likely to be targets of phishing attacks than larger companies, leading to a reactive approach to information security[9, 10].

Recent cyber-attacks on critical infrastructure have prompted extensive cyber-attack studies, but small businesses remain vulnerable to sophisticated cyber-attacks due to vulnerabilities in operational technologies[11]. Research investigations have identified gaps in knowledge needed to create effective defensive cyber security strategies for small businesses to stay afloat in this competitive market. Further research is required to understand how these strategies could impact small businesses' cyber defense[12].

In short, Small businesses often lack effective defensive security strategies to protect their information assets, making them targets for hackers. Lack of awareness and resources can lead to data leakage and financial and reputational losses. Implementing cyber security strategies with automation and adaptive cyber defenses can help protect enterprise assets. Training in information security can raise awareness and help businesses protect their assets. Despite financial capacities, investments in information security have not been sufficient to counter the rise of cyber-attacks.

This research study aims to explore the defensive security strategies needed by small businesses in the USA to protect their information assets. Many businesses lack proper security tools, policies, and procedures, leaving them vulnerable to cyber-attacks. The research focuses on updating security policies, deploying advanced detection and response tools, and enhancing the security posture as technology changes rapidly. The research questions about what strategies cyber security managers need to improve their cyber defense in small businesses in the USA. The research report also highlights internet security concerns and provides a broad-based overview of cyber security threats to business entities, along with mitigation and enhanced defense strategies.

Literature Review

Small businesses are crucial to the United States economy, accounting for 39% of the gross national product and creating two out of every three new jobs. To succeed, they require seven prerequisites: adequate financing, qualified personnel, efficient operation and production, marketing and sales, customer service, and information management and administration. The Small Business Administration (SBA) was established in 1953 by the Federal Government to provide low-interest loans to small business borrowers who would not otherwise have access to credit. However, there is criticism that these SBA programs unfairly benefit financial institutions participating in the guaranteed loan programs. Another significant source of debt financing for small businesses is micro-financing, started by Nobel Peace Prize winner Muhammad Yunus in Bangladesh. Small businesses contribute significantly to the total US economy,

Journal of Ecohumanism
2025
Volume: 4, No: 3, pp. 322 – 333
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i3.6644

employing over 40% of high-tech workers and filling under-represented labor market niches with high unemployment rates. They also employ higher rates of Hispanics, individuals 65 or older, disabled workers, and rural workers. In general, the number of new small business firms that are started is approximately equal to the ones those that are closed due to failure in the same year. Lack of adequate finances appears to be one of the main causes of failure among small business entrepreneurs. The Small Business Administration's loan programs may benefit financial institutions more than small businesses. Further research is needed to assess the efficacy of micro-financing in providing effective help to small business entrepreneurs[13].

The digital age has exposed various individuals, businesses, and government entities to potential cyber security vulnerabilities. A case study was conducted in Melbourne, Florida, to explore the strategies of four retail small- and medium-sized enterprises (SMEs) that successfully protected their businesses against cyber attacks. The study found three themes: cyber security strategy, reliance on third-party vendors for infrastructure services, and cyber security awareness. The findings suggest that SME owners' successful cyber security strategies could serve as a foundational guide for others to assess and mitigate cyber threat vulnerabilities. This could empower other SME owners, new entrepreneurs, and academic institutions to affect changes within the community. SME owners who survive cyber attacks may spur economic growth by employing local residents and catalyzing consumer confidence, leading to greater economic prosperity[14]. Small businesses often lack the resources and knowledge to address cyber security issues, putting them at a high risk of system compromise. A study of over 370 interviews with small business owners revealed that while they have basic tools for technology risk management, they lack policies, procedures, and training to secure their information resources. Additionally, most respondents do not use strong passwords to protect their information assets, highlighting the need for improved management and resources to ensure the security of small businesses[15].

Small businesses, particularly those with fewer than 19 employees, are becoming increasingly vulnerable to cyber-criminals. Despite their significant workforce, these businesses struggle to implement the same cyber security measures as larger enterprises. This paper explores the unique characteristics of Australian small businesses, such as agility, large cohort size, and piecemeal IT architecture, which can enhance cyber-security. The study highlights the need for effective solutions and legal and policy work to help these businesses become more cyber-resilient, highlighting the need for a comprehensive approach to cyber-security in Australian businesses[12]. A panel analysis of 48 U.S. states over a ten-year period analyzed the contribution of small businesses to productivity, Gross State Product (GSP), unemployment, and wage inflation at the state level. The results showed that states with higher proportions of very small business employment experienced higher levels of productivity growth and GSP growth while having less wage inflation and lower unemployment rates. These findings highlight the importance of considering the empirical issue of the benefits of small business employment at both state and national levels[16].

A study explores the effectiveness of cyber security strategies for small businesses in Washington, D.C. Over five years, five successful business owners implemented strategies to minimize cyber attacks. Key themes included security policy and procedures, employee training, and risk management. Strategic recommendations include investing in antivirus software, hiring IT experts, and learning from other companies' experiences. By protecting customers, employees, and confidential company data, small business leaders can improve their effectiveness and increase employment opportunities for local communities[17]. SIEM (Security Information and Event Management) is a key cyber security solution that helps organizations learn from their IT infrastructure and identify anomalies like cyber attacks. The total cost of ownership (TCO) is a key metric in SIEM cases, and organizations need to consider it. If a company is serious about deploying an SIEM, it should also consider SOC (Security Operations Centre) as a key security technology. SOC is a framework of technologies, people, and processes that identifies, protects, detects, responds, and recovers from all security-related incidents, acting like a well-oiled machine[18].

SIEM is a crucial tool for organizations to centralize log management and enhance information security. It collects and aggregates log data from various devices and applications using software called agents or connectors. SIEM filters uninteresting data, normalizes it to a proprietary format, analyzes it through correlation using contextual information, and alerts administrators in case of an attack. It provides proactive

Journal of Ecohumanism
2025
Volume: 4, No: 3, pp. 322 – 333
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i3.6644

threat detection and real-time analysis of system activity. However, even the most expensive SIEM solution does not guarantee success. Organizations should focus on building various use cases to make their SIEM solution a success. This paper proposes a new model and architecture for SIEM implementation using multiple hierarchical SIEM Managers, called the "Hierarchical Managers Model." This model and architecture can be created and enabled in the leading SIEM system, ArcSight ESM. The use cases shown in this paper are created using the security event correlation framework from Hewlett-Packard - ArcSight ESM[19].

The internet has made it indispensable for organizations, but the problem of security threats has emerged as a significant concern. SIEM systems, in conjunction with SOAR systems, are an integral part of a security operation center (SOC) to provide a holistic view of an organization's security status and protect IT infrastructure. This research paper discusses the latest and most advanced SIEM systems, including both open-source and proprietary solutions. Currently, there is no comprehensive SIEM

system architecture available, so this research proposes a comprehensive, well-defined, and modular architecture of the SIEM system. Each module is discussed in detail, focusing on input parameters, processing, and output details. This modular approach allows developers to extend the functionality of the SIEM system without compromising overall performance and integration issues. There are many SIEM systems available today, and discussions about their features are also provided. The method of choosing the suitable SIEM system for a specific organization has been discussed. The proposed SIEM system architecture will help organizations make the development or deployment of an SIEM system more efficient, effective, and easier[20].

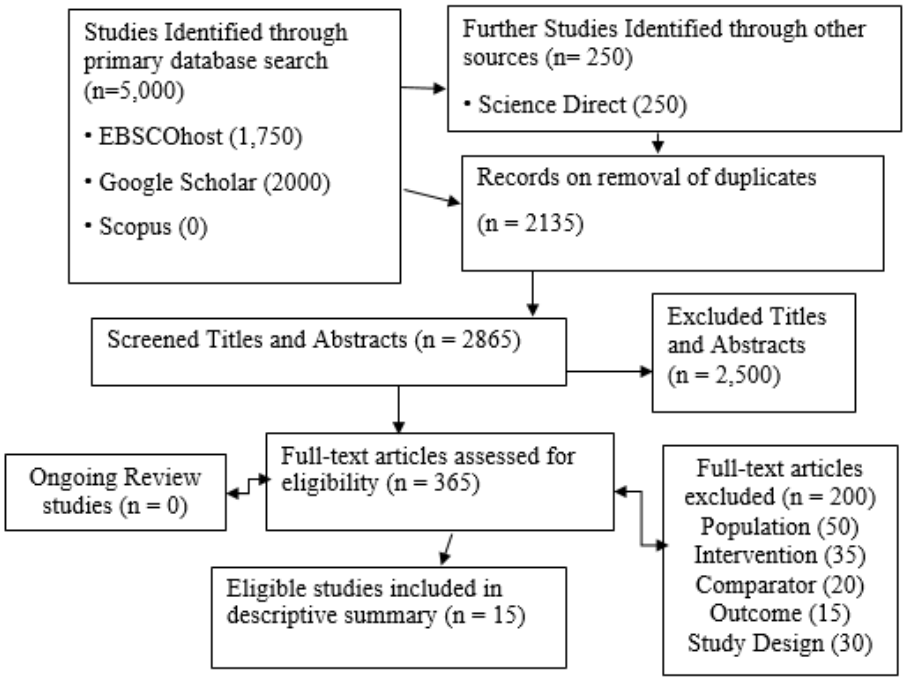
The literature consists of the background for cyber security and strategies for the threats. However, they do not compress the strategy details along with the problems associated with the system. This research aims to clarify the suitable strategy with all its advantages and disadvantages.

Methodology

To find cyber security threats and solutions to lessen them, a literature review was conducted. There were enough secondary sources for study in the form of books, journals, and magazines on cyber security [4]. Using the university library database, books and other scholarly papers were located, as seen in Figure 1. Before creating an article, pertinent keywords were entered into databases on computer systems. EBSCOhost, Academic OneFile, Google Scholar, and ERIC were among the databases from which the researcher searched for various peer-reviewed papers. In the search, a variety of keywords were employed; some examples of these terms were "organization culture," "security culture," "information security culture," "cyber security culture," and "security culture."

Journal of Ecohumanism
2025
Volume: 4, No: 3, pp. 322 – 333
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i3.6644

Figure 1. PRISMA Study Flowchart of Search Results



The search approach used in numerous organizational databases was represented by 5000 documents, which also contained traditional instructional studies and other organizational papers. Even though the search technique made numerous data accessible, the data cleaning process was strictly enforced, removing any duplicates. Following the removal of all duplicates, the titles and abstracts of the 2865 papers that remained were examined. An additional 2,500 individuals were excluded due to their noncompliance with the inclusion criteria. Furthermore, no research on "ongoing analysis" was mentioned. Other studies were excluded based on general research techniques and architecture.

Results and Discussions

Cyber Security Threats

Cyber-security risks have significantly increased, with 430 million new malware pieces discovered in 2023, a 36% increase from 2020 in the USA. Small businesses are particularly vulnerable due to the increasing adoption of technology. Cyber-attacks can lead to financial consequences such as data theft, manipulation, and corruption, affecting an organization's brand and decreasing competition in financial markets. In some cases, cyber-attacks target organizations' ICT systems, allowing hackers to gain access to an organization's information system. This poses a significant challenge for businesses, necessitating a complex security infrastructure to protect their computer networks from dangerous threats. This includes firewalls, intrusion detection and prevention systems, patch management solutions, and strong antivirus. Therefore, businesses need to develop robust security measures to protect their systems from cyber-attacks.

Some cyber security threats for small businesses in the USA can be stated as:

Malware

A cyber attack that "executes unauthorized actions on the victim's system" is referred to as malware or malicious software. This can be spread by viruses, ransom ware, phishing, or other malicious methods. Malware comes in three primary forms: worms, viruses, and trojan horses. Trojan Horses are scams in which malicious software disguises itself as a game or online download. a harmful code that targets

Journal of Ecohumanism
2025
Volume: 4, No: 3, pp. 322 – 333
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i3.6644

operating system components, data, or programs. In the part that follows, we'll go into viruses in greater detail. A system and other related programs can be infected by worms, a type of malware.

Viruses

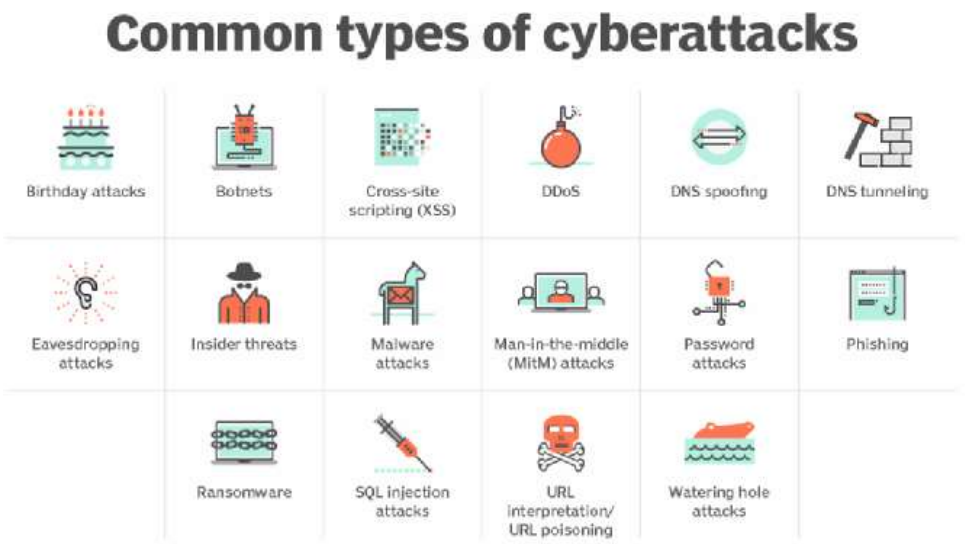
Viruses come in various forms, but they are all designed to damage your electronics. Programs, files, and computer performance can all be harmed by computer viruses. There are several methods to become infected with a virus: sharing data, opening contaminated emails, going to malicious websites, and downloading malicious apps. An increase in pop-up windows, unauthorized password changes to your account, destroyed files, and a decrease in network performance are all indicators that you have a virus on your computer.

Ransomware

Ransomware is a type of cyber attack that demands a ransom, often through email spam or network attacks, to secure a company's valuable assets. It typically requires payment within 24-48 hours to prevent the loss of files or public disclosure of compromised information. In July of last year, the REvil gang orchestrated a large attack via Kaseya, a company providing IT and security management solutions. The attack left 800 to 1,500 small businesses vulnerable, and despite Kaseya's swift response, the situation negatively affected many businesses. Each affected business may have had to pay for an investigation and notify customers if their personal information was stolen.

Some other and random cyber threats for small businesses are shown in Figure 2.

Figure 2. Common Cyber Threats for Small Businesses in the USA



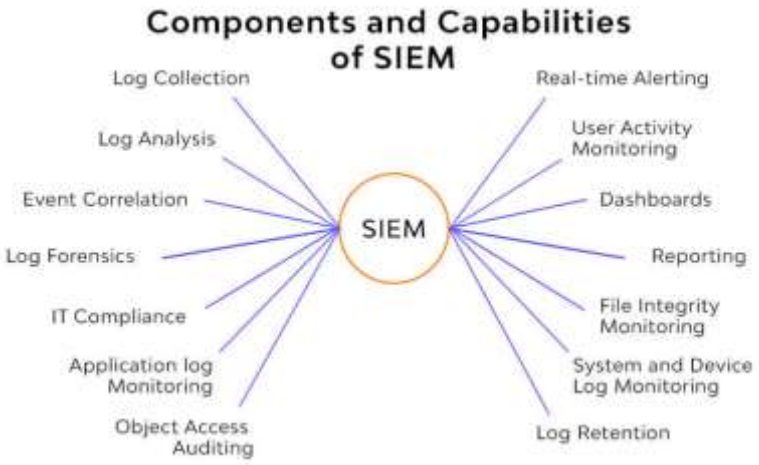
Preventative Strategy

Non-profit organizations are undergoing a drastic transition to adopt modern information technology, recognizing the importance of defending against cyber threats. As organizations transition to E-services and digital information, there is a growing demand for granular systems that provide vital protection for online data. In today's complex cyber landscape, sophisticated tools are needed to protect entire computer systems. A comprehensive protection framework, including firewalls, intrusion detection and prevention systems, path management solutions, and reliable antivirus, is essential for securing existing computer networks from external and internal threats[21].

Journal of Ecohumanism
2025
Volume: 4, No: 3, pp. 322 – 333
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i3.6644

Security Incident Event Management (SIEM) software is an effective tool for organizations in this transition. SIEM software allows security analysts to gain insight into security threats targeting IT processes by searching logs generated by network devices and identifying signs of an ongoing attack. The SIEM system must be capable of correlating a large number of logs from different sources and detecting attacks with a high detection rate and low false-positive rate. This approach is crucial for organizations to manage their IT security effectively and protect their IT systems from potential threats.

Figure 3. The Intervention of the SIEM System



Management plays a crucial role in addressing cybercrime by identifying and prioritizing threats within different departments. The SIEM method provides mechanisms for aggregating, interpreting, and associating events from different sources, with primary capabilities including threat detection, incident response, and log management. Intrusion Detection Systems (IDS) are another security tool that can improve communication and information systems security, similar to firewalls, antivirus software, and access control systems. IDS monitors system or network operations for policy violations or malicious activities, sending a report to the management station. Despite its infancy, IDS is considered a reliable protection and plays an important role within the information security architecture. As cybercrime continues to grow globally, a consistent legal structure is essential for managing and addressing these threats[22].

The SIEM Strategy

The implementation of a Security Information and Event Management (SIEM) system is crucial for organizations' cyber security. It provides real-time monitoring, threat detection, and incident response capabilities, enabling seamless integration with existing security frameworks[23]. A successful SIEM strategy involves understanding the scope of SIEM capabilities and defining clear objectives to ensure a streamlined implementation process. A clear business case for SIEM is essential, identifying specific goals and objectives, prioritizing critical tasks and processes, reviewing existing security policies, and assessing current controls.[22] During the discovery phase, it is advisable to pilot the SIEM system on a small subset of the organization's technology and policies. This allows for the collection of crucial data, guiding any necessary modifications and enhancements before full-scale deployment. The primary aim is to identify and address any weaknesses or gaps in the execution of controls, ensuring they are resolved before integrating them into the SIEM framework. This strategic approach sets the stage for a successful and effective security management system[21, 23].

Journal of Ecohumanism
2025
Volume: 4, No: 3, pp. 322 – 333
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i3.6644

Best Practices for SIEM Implementation[24]

Preventing Bottlenecks by Optimizing the Discovery Phase

- SIEM integrations require significant investments in time, money, and skilled personnel.
- Measure Your Current Infrastructure: Evaluate your current IT and security infrastructure to understand the volume of data that will be ingested by the new SIEM system.
- Forecast Future Growth: Discuss forecasts with financial and development stakeholders to assess potential future growth.
- Understand Your SIEM Capacity: Understand the SIEM solution's capacity in terms of data ingestion, processing, storage, and analysis capabilities.
- Plan for Scalability: Ensure the SIEM solution can scale to meet current and future needs.
- Leverage Professional Services: Consult with SIEM vendors or professional services for advice on infrastructure planning and optimization.

Achieving Comprehensive Visibility Early

- Run the new SIEM on a small subset of technology that's representative of all of your organization's devices and policies.
- Set Up for Log Diversity: Include logs from as wide a source as possible, including logs from critical network security and infrastructure components within the SIEM system.
- Normalize to Avoid Blind Spots: Incompatibilities can hinder the SIEM's ability to provide a comprehensive view of security events across the organization.
- Keep an Eye on Compliance Regulations: Apply lessons learned from the data collected and implement improvements on a larger subset of policies and devices.

Understanding Regulatory Requirements for SIEM Implementation

- Understand and align your organization's practices with regulations like GDPR, HIPAA, SOX, and PCI-DSS.
- Balancing data retention and storage costs is crucial for SIEM implementation.

Classifying Data According to Sensitivity

- Establish a data retention policy that meets regulatory requirements.
- Ensuring sensitive data encryption, access control, and only necessary data collection and processing minimizes the risk of non-compliance.
- Keep logs for a few months to ingest into SIEM's behavioral analytics.

Use your SIEM System to Generate Compliance Reports

- These reports should demonstrate adherence to regulatory requirements.

Journal of Ecohumanism
2025
Volume: 4, No: 3, pp. 322 – 333
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i3.6644

- Incorporating regulatory requirements in the pilot phase of the SIEM rollout can improve security.

Post-Implementation Strategies for SIEM Management

- Optimize Intelligence Sources.
- Transform raw event data into actionable threat information.
- Streamline Reporting.
- Ensure the SIEM tool has some degree of personalized reporting.
- Regularly monitor the performance of your SIEM system to identify and address bottlenecks.
- Automation.
- AI applications focus on automating data aggregation and normalization.
- AI can correlate data around an alert to identify its criticality and automatically generate incidents for further investigation.
- Automation tools and playbooks can establish automated response actions, reducing response time and expediting threat management.

Siem Systems Tend to Follow A Four-Step Process[23]

Data Collection from The Source

Real-time data is gathered by information gathering tools like firewalls, loggers, and others from sources including routers, domain controllers, and network devices. The following phase is then reached with this information.

Aggregate Data

To facilitate human analysis, the data is now connected to related events. In order to expedite the process, the SIEM tools and software also make the data easier for humans to use and comprehend.

Journal of Ecohumanism
2025
Volume: 4, No: 3, pp. 322 – 333
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i3.6644

Figure 4. The SIEM Progress Flow

Threats Analysis

In order to alert the IT administrators, threats are now identified in the data. IT administrators are informed of potential hazards when potentially harmful data is distinguished from non-problematic data through the use of various analytics.

Identify the Breaches and Fix Threats

Data is gathered, and analyzed, and vulnerabilities discovered are located and fixed. This last measure makes sure that similar breaches won't be discovered in future data harvesting efforts.

The process flow is shown in the figure 4.

The Complicated Environment of SIEM Application

Small organizations should recognize the complex issues inside the continuously changing SIEM deployment framework and be prepared to address them head-on. These problems are undoubtedly solvable, despite their seeming complexity. Organizations may overcome obstacles and leverage the power of SIEM to improve security for a range of use cases by using the appropriate techniques.

These are the seven typical SIEM implementation issues[25].

- Configuration Complexity: The crucial phase of configuring an SIEM system involves meticulous attention to detail, ensuring the system is well-tuned to respond to threats. This phase is crucial as configuration errors can lead to false positives or missed threats, emphasizing the importance of skilled personnel in ensuring the system is well-suited to an organization's unique cyber security needs.

- Integration Hurdles: SIEM tools pose a formidable challenge in integrating seamlessly with existing infrastructure, ensuring smooth data flow between systems. This process requires careful planning and execution, as the lack of compatibility can hinder the SIEM's ability to provide a holistic view of security events.

Journal of Ecohumanism
2025
Volume: 4, No: 3, pp. 322 – 333
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i3.6644

- Resource Constraints: Achieving a successful SIEM implementation requires a significant investment in time, money, and skilled personnel. Smaller organizations may struggle to allocate resources, requiring them to prioritize cyber security needs and focus on critical areas within their resource constraints for a successful implementation.

- Hidden cost: SIEM offers enhanced security, but hidden costs can arise when the volume of data exceeds expectations, straining budgets and disrupting the implementation process. The expense of processing and storing vast amounts of data can be overlooked.

- Data Onboarding Challenges: The SIEM solution requires proper onboarding of data sources, ensuring they have the same structures and log formats as the systems and applications. This is crucial for the SIEM's effectiveness in threat detection, as varying log formats and structures can compromise the system's efficiency. Therefore, organizations must develop strategies to manage diverse data sources effectively.

- Scalability Limitations: As an organization expands, scalability is crucial for long-term success. A SIEM system that can handle increasing log data and events is essential for long-term success. Without adequate scalability, the system may struggle to keep pace with the influx of data, leading to performance issues and incomplete event capture. Planning for scalability during the implementation phase is essential for maintaining system effectiveness.

- Retention and Compliance Regulations: The SIEM solution is crucial for organizations to manage data retention efficiently for compliance and investigative purposes. By implementing robust data archiving and purging mechanisms, organizations can avoid unnecessary storage costs and comply with regulations. Clear policies for data retention and disposal are also essential to maintain compliance and minimize storage costs.

Conclusion

Cyber security is a critical issue in today's information, communication, and technology-driven world. It involves the protection of data, confidentiality, integrity, and reliability/availability of information systems. These security threats can have significant financial consequences for both individuals and organizations, including money theft, digital assets, and confidential information. Despite the complexity of cyber security, small companies are constantly evolving to embrace the new information age, making information technology a valuable tool for managing their key service deliveries. The Security Incident Event Management (SIEM) framework is an effective tool for analyzing network device-generated logs and detecting ongoing attacks. SIEM tools must be able to compare logs from different sources and detect attacks with a high detection rate and low false positive rate. Prioritizing warnings allows security analysts to focus on high-threat alerts.

To protect against cyber threats, businesses need a comprehensive protection framework, including antiviruses, firewalls, and SIEM tools. Intrusion Detection Systems (IDS) can be used in the same way as firewalls, antivirus software, and access control systems to improve the security of communication and information systems. By implementing effective security measures, organizations can better protect themselves from potential threats and maintain a secure digital environment.

References

T. Akter, A. S. A. Samman, A. H. Lily, M. S. Rahman, N. N. I. Prova, and M. I. K. Joy, "Deep Learning Approaches for Multi Class Leather Texture Defect Classifcation," in 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), 24-28 June 2024 2024, pp. 1-6, doi: 10.1109/ICCCNT61001.2024.10725952.

B. Fakiha, "Business organization security strategies to cyber security threats," International Journal of Safety and Security Engineering, vol. 11, no. 1, pp. 101-104, 2021.

M. Bay, "What is cybersecurity," French Journal for Media Research, vol. 6, pp. 1-28, 2016.

Journal of Ecohumanism
2025
Volume: 4, No: 3, pp. 322 – 333
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i3.6644

H. Arpita, A. Ryan, M. Hossain, M. Rahman, M. Sajjad, and n. prova, "Exploring Bengali speech for gender classification: machine learning and deep learning approaches," Bulletin of Electrical Engineering and Informatics, vol. 14, pp. 328-337, 11/19 2024, doi: 10.11591/eei.v14i1.8146.

E. Hurst and B. W. Pugsley, "What do small businesses do?," National Bureau of Economic Research, 2011.

N. N. I. Prova, "Improved Solar Panel Efficiency through Dust Detection Using the InceptionV3 Transfer Learning Model," in 2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 3-5 Oct. 2024 2024, pp. 260-268, doi: 10.1109/I-SMAC61858.2024.10714631.

M. Prabha, M. A. Hossain, M. Samiun, M. A. Saleh, S. R. Dhar, and M. A. A. Mahmud, "AI-Driven Cyber Threat Detection: Revolutionizing Security Frameworks in Management Information Systems," in 2024 International Conference on Intelligent Cybernetics Technology & Applications (ICICyTA), 17-19 Dec. 2024 2024, pp. 357-362, doi: 10.1109/ICICYTA64807.2024.10912927.

J. Aurelien, Exploring Effective Defensive Cybersecurity Strategies for Small Businesses. Colorado Technical University, 2021.

D. F. Kuratko, G. Fisher, and D. B. Audretsch, "Unraveling the entrepreneurial mindset," Small Business Economics, vol. 57, no. 4, pp. 1681-1691, 2021.

A. Debnath, M. Z. Hossan, S. Sharmin, M. S. Hosain, F. T. Johora, and M. Hossain, "Analyzing and Forecasting of Real-Time Marketing Campaign Performance and ROI in the U.S. Market," in 2024 International Conference on Intelligent Cybernetics Technology & Applications (ICICyTA), 17-19 Dec. 2024 2024, pp. 332-337, doi: 10.1109/ICICYTA64807.2024.10913226.

N. N. I. Prova, "Garbage Intelligence: Utilizing Vision Transformer for Smart Waste Sorting," in 2024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI), 28-30 Aug. 2024 2024, pp. 1213-1219, doi: 10.1109/ICoICI62503.2024.10696177.

T. Tam, A. Rao, and J. Hall, "The good, the bad and the missing: A Narrative review of cyber-security implications for australian small businesses," Computers & Security, vol. 109, p. 102385, 2021.

R. R. Yallapragada and M. Bhuiyan, "Small business entrepreneurships in the United States," Journal of Applied Business Research (JABR), vol. 27, no. 6, pp. 117-122, 2011.

K. D. Cook, "Effective cyber security strategies for small businesses," Walden University, 2017.

C. T. Berry and R. L. Berry, "An initial assessment of small business risk management approaches for cyber security threats," International Journal of Business Continuity and Risk Management, vol. 8, no. 1, pp. 1-10, 2018.

D. K. Robbins, L. J. Pantuosco, D. F. Parker, and B. K. Fuller, "An ampirical assessment of the contribution of small business employment to US State economic performance," Small Business Economics, vol. 15, pp. 293-302, 2000.

D. Joel Chagadama and D. S. Luamba, "Cyberattacks: A Huge Concern for Small Business Sustainability."

O. Podzins and A. Romanovs, "Why siem is irreplaceable in a secure it environment?," in 2019 Open Conference of Electrical, Electronic and Information Sciences (eStream), 2019: IEEE, pp. 1-5.

I. Anastasov and D. Davcev, "SIEM implementation for global and distributed environments," in 2014 World Congress on Computer Applications and Information Systems (WCCAIS), 2014: IEEE, pp. 1-6.

M. Sheeraz et al., "Effective security monitoring using efficient SIEM architecture," Hum.-Centric Comput. Inf. Sci, vol. 13, pp. 1-18, 2023.

J. M. López Velásquez, S. M. Martínez Monterrubio, L. E. Sánchez Crespo, and D. Garcia Rosado, "Systematic review of SIEM technology: SIEM-SC birth," International Journal of Information Security, vol. 22, no. 3, pp. 691-711, 2023.

H. Mokalled, R. Catelli, V. Casola, D. Debertol, E. Meda, and R. Zunino, "The applicability of a siem solution: Requirements and evaluation," in 2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), 2019: IEEE, pp. 132-137.

R. Montesino, S. Fenz, and W. Baluja, "SIEM-based framework for security controls automation," Information Management & Computer Security, vol. 20, no. 4, pp. 248-263, 2012.

H. Caldeira, "Security Information and Event Management (SIEM) Implementation Recommendations to Enhance Network Security," Utica College, 2021.

L. Coppolino, S. D'Antonio, L. Romano, L. Sgaglione, and M. Staffa, "Addressing security issues in the eheatlh domain relying on SIEM solutions," in 2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC), 2017, vol. 2: IEEE, pp. 510-515..