YENEPOYA
(Deemed To Be University)

Final Project Report
On
SIEM FOR SMALL BUSINESSES

Team members:

Name	Register Number	Email Id
Mubeena V	22BCIECS075	21105@yenepoya.edu.in
Fathima	22BCIECS032	21198@yenepoya.edu.in
Vismaya CT	22BCIECS122	23540@yenepoya.edu.in
Shivani TV	22BCIECS114	22166@yenepoya.edu.in

Guided By:
Mr. Shashank

Table of Contents (should be in a table format with the page number)

EXECUTIVE SUMMARY

In today's digital landscape, small businesses are increasingly becoming targets of cyberattacks due to their limited resources and often underdeveloped security infrastructure. Despite common misconceptions, small businesses hold valuable data—such as customer records, financial information, and intellectual property—that can be exploited by cybercriminals. As a result, there is a growing need for proactive and centralized cybersecurity measures.

Security Information and Event Management (SIEM) systems offer a comprehensive approach to security monitoring by aggregating logs, detecting threats, generating alerts, and aiding in incident response. However, traditional SIEM solutions have been perceived as costly, complex, and resource-intensive—barriers that have historically prevented small businesses from adopting them.

This report aims to bridge that gap by exploring **cost-effective, scalable, and user-friendly SIEM options tailored specifically for small businesses**. It outlines how small organizations can implement a SIEM solution without the need for a dedicated security team or high upfront investment. By leveraging open-source tools, cloud services, and managed security providers, small businesses can achieve real-time visibility into their IT environments, enabling faster detection of potential threats and reducing response times.

Key benefits of deploying a SIEM system in small business environments include:

- **Centralized log management** for all network, server, and endpoint activity
- **Real-time threat detection** using preconfigured and customizable rules
- **Enhanced incident response and forensic capabilities**
- **Support for regulatory compliance** such as GDPR, HIPAA, PCI-DSS
- **Scalability to support future growth** without major reinvestment

SIEM Deployment Guide for Small Businesses

Step 1: Define Objectives and Scope

- **Goals**: Threat detection, log centralization, compliance, alerting.
- **Scope**: Identify systems to monitor (e.g., workstations, servers, routers, cloud apps).
- **Compliance Needs**: Understand regulatory requirements (e.g., GDPR, HIPAA).

Step 2: Choose a SIEM Solution

SIEM Tool	Cost	Features	Ideal For
Wazuh	Free (open-source)	Endpoint security, file integrity monitoring, intrusion detection	On-premises or hybrid
Graylog Open	Free	Log management, basic alerting	Centralized logging
Security Onion	Free	Network security monitoring, packet capture	Security-focused setups
OSSIM (AlienVault)	Free (Community edition)	SIEM, asset discovery, vulnerability assessment	All-in-one features

SIEM Tool	Cost	Features	Ideal For
Splunk Free	Free up to 500 MB/day	Powerful analytics, dashboards	Small-scale deployments
Microsoft Sentinel	Pay-as-you-go	Cloud-native, integrates with Azure services	Cloud-first businesses

Step 3: System Requirements and Hardware

For On-Premise Deployment (e.g., Wazuh, Graylog)

- **Server (Physical/VM):**
  - CPU: 4–8 cores
  - RAM: 8–16 GB
  - Storage: 500 GB–2 TB SSD (depending on log retention)
  - OS: Ubuntu/CentOS/Debian

For Cloud Deployment

- Cloud VMs (AWS EC2, Azure V) or use managed services (e.g., Sentinel).
- Use log shippers (File beat, Win log beat) on endpoints and forward logs to the cloud.

Step 4: Deploy Components

Wazuh Example Deployment

1. **Install Wazuh Manager** on a central server (on-prem or cloud).
2. **Install Wazuh Agents** on endpoints (Windows, Linux, macOS).
3. **Deploy ELK Stack** (Elasticsearch, Logstash, Kibana) for search and visualization.
4. Configure alerting rules and dashboards.
5. Set up secure communication (e.g., TLS, firewall rules).

Step 5: Configure Log Sources

- Windows Event Logs via Win log beat
- Linux sys logs File beat
- Firewall/router logs via syslog
- Cloud logs (e.g., AWS CloudTrail) via APIs

Step 6: Set Up Correlation and Alerts

- Define rules for:
  - Failed login attempts
  - Unauthorized file access
  - Port scanning
  - Suspicious outbound traffic

- Configure notifications (e.g., email, Slack)

Step 7: Train Staff and Monitor System

- Assign a staff member or MSP to monitor alerts.
- Provide basic training in reading dashboards and responding to incidents.
- Set a policy for incident response.

ad, and integration with existing IT systems.

Conclusion on SIEM Deployment

Deploying a SIEM system is a critical step in strengthening an organization's cybersecurity posture. A well-implemented SIEM solution enables real-time monitoring, threat detection, incident response, and regulatory compliance through centralized log management and data analysis. While deployment may involve significant planning, integration, and tuning, the long-term benefits in terms of enhanced visibility, proactive defense, and reduced risk far outweigh the initial challenges. To ensure success, organizations must align SIEM capabilities with their specific security goals, ensure proper training and maintenance, and continuously update detection rules in response to evolving threats.

Challenges and Considerations

- **Initial Complexity and Cost**
  Deploying a SIEM requires significant upfront effort in terms of planning, integration, and resource allocation. Costs may include software licensing, hardware (if on-premise), and personnel training.
- **Data Overload and Noise**
  Without proper tuning, SIEMs can generate a large volume of alerts, many of which may be false positives. Continuous refinement of rules and correlation logic is essential to maintain relevance.
- **Skilled Personnel Requirement**
  SIEM tools require skilled analysts to interpret data, manage rules, and respond to incidents. Organizations may need to invest in staff training or partner with a Managed Security Service Provider (MSSP).

BACKGROUND

Small businesses increasingly face cybersecurity threats similar to those targeting larger enterprises. However, limited budgets, fewer IT resources, and less mature security processes often make it challenging for small businesses to implement robust security measures. Security Information and Event Management (SIEM) solutions offer an effective way to enhance security by providing centralized visibility, threat detection, and compliance support.

Despite their size, small businesses handle valuable data and are often targeted by cybercriminals as easier victims. Deploying a SIEM tailored to small business needs can help these organizations proactively defend against threats, detect breaches early, and meet any regulatory requirements without overwhelming their resources.

Aim

The primary aim of deploying a SIEM system in a small business environment is to:

- **Improve security visibility** across all digital assets by aggregating and correlating logs from various sources such as servers, endpoints, firewalls, and cloud services.
- **Enable real-time threat detection** to identify suspicious activity promptly and reduce potential damage from cyberattacks.
- **Support compliance efforts** with industry regulations by maintaining detailed logs and providing audit-ready reports.
- **Optimize limited resources** by automating log analysis, alerting, and reporting, thereby reducing the burden on small IT teams or outsourced security providers.
- **Facilitate efficient incident response** and forensic analysis, helping small businesses quickly understand and remediate security incidents.

1.2 Technologies

Several technologies and components underpin a SIEM solution suitable for small businesses:

- **Log Collection Agents:** Software installed on endpoints, servers, and network devices to capture security events and logs (e.g., Syslog, Windows Event Logs).
- **Data Aggregation and Normalization:** Centralizing logs from diverse sources into a common format for easier analysis.
- **Correlation Engine:** Analyzes logs in real-time to identify patterns and correlate events that could indicate security threats.
- **Alerting and Notification Systems:** Automated alerts via email, SMS, or dashboards to notify security personnel of suspicious activities.
- **Dashboards and Reporting Tools:** Provide visual summaries of security posture and compliance status.
- **Threat Intelligence Integration:** Incorporates external threat data feeds to improve detection accuracy and context.
- **Cloud or On-Premise Deployment:** Many small businesses prefer cloud-based SIEM (SaaS) solutions due to lower upfront costs, ease of scaling, and reduced management overhead.

Software Architecture

A typical SIEM architecture for small businesses consists of the following layers and components:

1. Data Collection Layer

- **Agents/Collectors:** Installed on network devices, servers, firewalls, and endpoints to gather logs and event data continuously.
- **Log Forwarders:** Tools that transmit collected data securely to the SIEM system.

2. Data Processing Layer

- **Normalization Module:** Converts incoming log formats into a standardized structure, enabling efficient analysis.
- **Parsing and Enrichment:** Extracts relevant information such as IP addresses, usernames, and timestamps; enriches data with context (e.g., geolocation or user roles).

3. Correlation and Analysis Layer

- **Correlation Engine:** Uses pre-defined and customizable rules to link multiple events across the environment, identifying patterns consistent with security incidents.
- **Machine Learning (Optional):** Some modern SIEMs incorporate machine learning algorithms to detect anomalies without relying solely on static rules.

4. Alerting and Response Layer

- **Alert Manager:** Prioritizes and sends alerts to security teams or automated response systems.
- **Automated Response (SOAR Integration):** Small businesses might integrate with Security Orchestration, Automation, and Response (SOAR) tools to automate simple incident responses, like isolating a compromised device.

5. User Interface and Reporting Layer

- **Dashboard:** Provides real-time visibility into security events and health metrics.
- **Reporting Module:** Generates compliance reports tailored to industry standards and organizational policies.

Small businesses benefit from SIEM deployment by gaining enterprise-level security monitoring without the complexity and cost typically associated with large-scale solutions. Cloud-based SIEM offerings, simplified architecture, and automation make it feasible for small IT teams or outsourced providers to maintain strong defenses and meet compliance demands efficiently.

Requirements

2.1.1 Functional Requirements

These describe what the SIEM system must be able to do to meet the security needs of a small business:

- **Log Collection:** Ability to collect logs from a variety of sources such as servers, endpoints, firewalls, network devices, and cloud applications.
- **Log Normalization and Parsing:** Convert different log formats into a standardized form to enable unified analysis.
- **Real-time Event Correlation:** Automatically correlate events from multiple sources to detect suspicious patterns and potential security incidents.
- **Alerting and Notification:** Generate alerts on suspicious activities and notify administrators or security personnel through email, SMS, or dashboards.
- **Incident Management:** Provide tools for tracking, investigating, and resolving security incidents.
- **Reporting and Compliance:** Generate predefined and customizable reports to support compliance with relevant regulations (e.g., GDPR, PCI-DSS).
- **User and Entity Behavior Analytics (UEBA):** Optional, but increasingly important for detecting insider threats and anomalies.
- **Integration with Other Security Tools:** Support integration with antivirus, firewalls, endpoint detection and response (EDR), and threat intelligence feeds.
- **Data Retention and Archiving:** Store logs for a defined period to comply with legal and regulatory requirements.

2.1.2 User Requirements

These focus on the needs and capabilities of the users interacting with the SIEM system, often including small business IT staff or outsourced security providers:

- **Ease of Use:** User-friendly interfaces and dashboards suitable for small teams or individuals with limited security expertise.
- **Role-based Access Control (RBAC):** Ability to define user roles and permissions to limit access to sensitive security data.
- **Alert Customization:** Users should be able to customize alert thresholds and notification preferences.
- **Training and Support:** Availability of documentation, tutorials, and vendor support to assist non-expert users.
- **Mobile Access:** Optional but beneficial for administrators needing remote monitoring capabilities.
- **Scalability:** Ability to grow with the business without requiring a complete system overhaul.

2.1.3 Environmental Requirements

These relate to the infrastructure and operational context in which the SIEM system will operate within a small business:

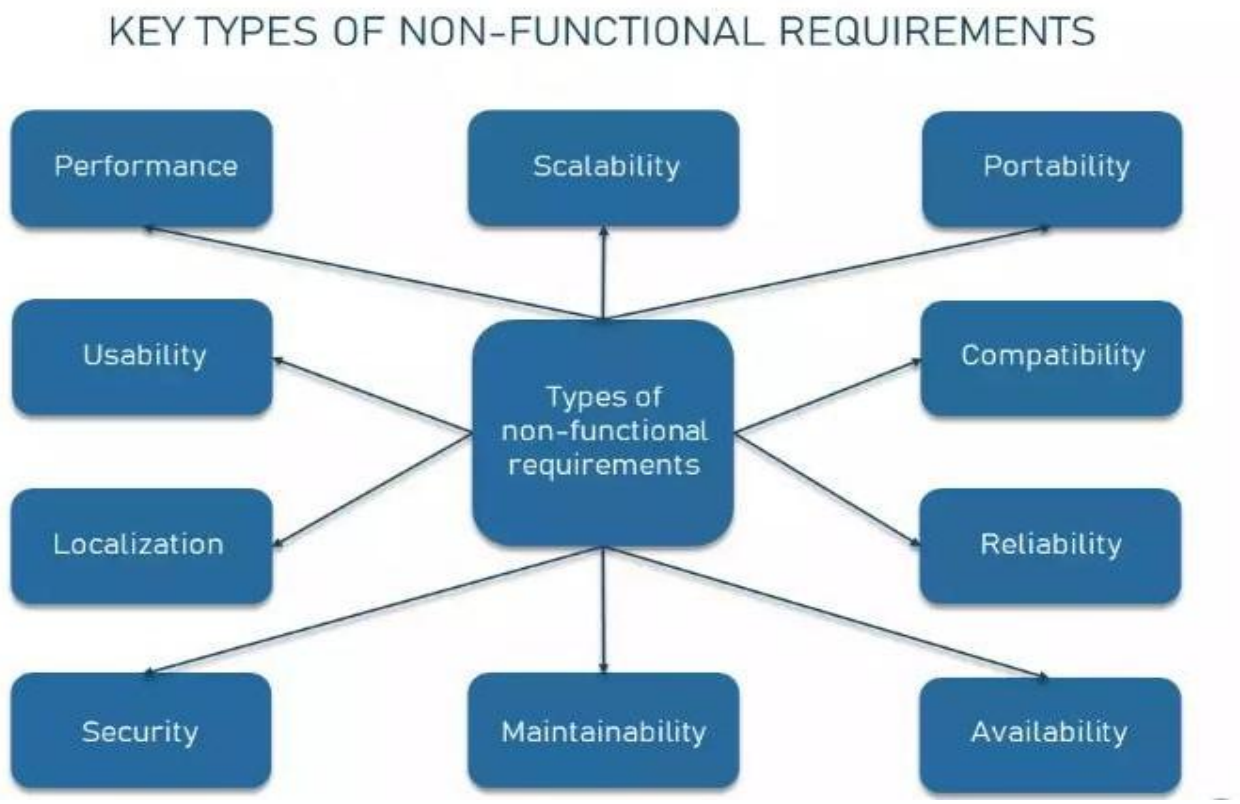
- **Deployment Options:** Support for cloud-based (SaaS) or on-premises deployment depending on the business's infrastructure and preferences.
- **Network Compatibility:** Should operate smoothly within the existing network setup without causing significant bandwidth or latency issues.

- **Data Privacy:** Compliance with local data protection laws regarding log storage and transmission, especially if using cloud-based SIEM.
- **Resource Constraints:** Efficient use of computing resources to avoid impacting the performance of other critical business applications.
- **Interoperability:** Ability to integrate with the small business's existing hardware and software, including legacy systems.
- **Backup and Recovery:** Mechanisms to ensure data integrity and availability in case of failures or attacks.

2.1.4 Non-Functional Requirements

These specify the quality attributes and constraints that the SIEM system must satisfy beyond its core functions:

- **Performance:** The system must process and analyze logs in near real-time to ensure timely detection of threats.
- **Reliability and Availability:** High uptime with minimal downtime to maintain continuous security monitoring.
- **Scalability:** Ability to handle increasing amounts of log data as the business grows without degradation in performance.
- **Security:** Strong encryption for data in transit and at rest, secure authentication mechanisms, and protection against tampering.
- **Maintainability:** Easy to update, configure, and troubleshoot, ideally with automated updates and clear error reporting.
- **Cost-effectiveness:** Affordable licensing, minimal hardware requirements (especially for cloud solutions), and low operational overhead suitable for small business budgets.
- **Compliance:** The system should meet relevant industry standards and legal requirements.
- **Usability:** Intuitive design that reduces the learning curve for small teams.
- **Extensibility:** Ability to add new log sources, detection rules, or integrate with additional security tools as needed.



Implementation Overview

Step 1: Requirement Analysis and Planning

- **Identify assets and scope:** Which systems, devices, applications, and networks need monitoring? Common sources include firewalls, routers, endpoints, servers, cloud services, and applications.
- **Define security goals:** E.g., detect unauthorized access, malware outbreaks, insider threats.
- **Budget planning:** Decide on in-house, cloud, or hybrid SIEM solutions based on cost and expertise.
- **Compliance needs:** Identify regulatory requirements like GDPR, HIPAA, PCI-DSS, which may mandate specific logging or reporting.

Step 2: Choosing the Right SIEM Solution

- **Open-source options:** ELK Stack (Elasticsearch, Logstash, Kibana) with additional tools like Wazuh or OSSIM.
- **Cloud SIEM solutions:** Microsoft Sentinel, IBM QRadar on Cloud, Splunk Cloud, or smaller vendors like LogPoint.
- **Considerations:** Cost, ease of use, integration capabilities, scalability, support.

Step 3: Data Collection and Integration

- **Log sources:** Configure devices and applications to send logs/events to the SIEM.
    - Firewalls, IDS/IPS, antivirus logs
    - Operating system event logs (Windows Event Logs, Linux syslog)

  - Application logs (web servers, database servers)
  - Network devices and switches
- **Log formats:** Normalize logs into a consistent format for correlation.
- **Data storage:** Decide on retention policies based on compliance and storage capacity.

Step 4: Deployment and Configuration

- **Deploy SIEM components:**
  - Central server or cloud platform for log ingestion, analysis, and alerting.
  - Agents or collectors on endpoints if needed.
- **Set up correlation rules:**
  - Define rules to detect suspicious activities, e.g., repeated login failures, port scans, malware signatures.
- **Create dashboards and reports:**
  - Customizable views for quick insight.
  - Scheduled reports for compliance or management review.

Step 5: Alerting and Incident Response

- **Configure alert thresholds:** Avoid alert fatigue by tuning sensitivity.
- **Notification mechanisms:** Email, SMS, or integration with ticketing systems.
- **Incident response plan:** Define steps when an alert is triggered:
  - Validate the alert.
  - Contain the threat.
  - Eradicate malware or unauthorized access.
  - Recover affected systems.
  - Document and report.

Step 6: Training and Awareness

- Train the IT team on SIEM use and interpretation of alerts.
- Create simple playbooks for common incidents.
- Raise employee awareness about security best practices.

Step 7: Maintenance and Continuous Improvement

- Regularly update correlation rules and detection mechanisms.
- Monitor system performance and log integrity.
- Review alerts and false positives to refine settings.
- Stay updated on new threats and vulnerabilities.

5. Example Architecture for Small Business SIEM

```
scss
Copy code
[Devices: Firewalls, Routers, Endpoints]
        ↓ (Syslog, Agents)
[Log Collector / Forwarder] → [SIEM Server/Cloud Platform]
        ↓
[Log Storage & Correlation Engine]
        ↓
[Dashboard & Alerting System]
        ↓
[Security Team / Admin Notifications]
```

6. Technologies and Tools Commonly Used

- **Log Collection:** Syslog, Winlogbeat, Filebeat
- **Processing/Storage:** Elasticsearch, Graylog, Splunk
- **Visualization:** Kibana, Grafana
- **Threat Detection:** Correlation rules, Machine Learning modules
- **Incident Management:** PagerDuty, ServiceNow integration

7. Cost Considerations

- **Open source:** Minimal licensing costs, but requires skilled staff.
- **Cloud SIEM:** Subscription model, easier to maintain, cost varies with data volume.
- **Hardware:** If on-premises, costs for servers and storage.
- **Training and support:** Often overlooked but essential.

8. Benefits for Small Businesses

- Centralized security visibility
- Faster threat detection and response
- Compliance with security standards
- Reduced risk of data breaches and downtim

Testing

Testing is a crucial phase to ensure the SIEM system works correctly, reliably, and securely within a small business environment. This involves multiple test types, from functionality and performance to user acceptance and recovery scenarios.

Test Plan Objectives

- Ensure the SIEM system accurately collects, processes, and analyzes logs from multiple sources.
- Validate that alerts are generated correctly for predefined security events.
- Confirm that the system meets business, compliance, and performance requirements.

- Identify any security vulnerabilities or configuration issues before going live.
- Ensure ease of use for small business IT personnel with limited security expertise.

Data Entry

- Verify that log data is correctly ingested from all connected sources (firewalls, routers, endpoints, cloud services).
- Ensure support for various log formats (syslog, Windows Event Logs, JSON, etc.).
- Test timestamp accuracy and source labeling for traceability.
- Check for data integrity and completeness during entry and parsing stages.

Security

- Ensure secure transmission of logs (e.g., TLS/SSL encryption).
- Validate access control: only authorized users should access dashboards and reports.
- Test multi-factor authentication (MFA) if enabled.
- Perform a security audit to detect potential misconfigurations, such as overly broad permissions or unencrypted data.

Test Strategy

- **Black-box testing**: Focus on system output without internal knowledge.
- **White-box testing**: Test configuration rules, alert logic, and parsing scripts.
- **Automated testing**: Simulate events like failed logins, malware detections.
- **Manual testing**: Verify alerts, dashboard visualizations, and report accuracy.

Test across phases:

- **Unit tests** for individual parsers/rules
- **Integration tests** for full data flow (source → collector → SIEM → alert)
- **End-to-end tests** for complete use case simulations

System Test

- Test the entire SIEM platform's components working together.
- Ensure the correlation engine generates alerts as expected.
- Test dashboard responsiveness and search capabilities.
- Verify reports are generated and exported correctly.

Performance Test

- Measure system response time during normal and peak data ingestion.

- Assess the correlation engine's ability to process logs in real-time.
- Evaluate query speed for analysts searching logs over different time ranges.
- Ensure no data is dropped under high-volume conditions.

Security Test

- Penetration testing of the SIEM web interface or management console.
- Check against common vulnerabilities (e.g., OWASP Top 10).
- Simulate insider threats and privilege abuse.
- Test log tampering protection and alert on unauthorized changes.

Basic Test

- Basic functionality check: installation, log collection, rule matching.
- Ensure log sources are correctly connected and visible.
- Run simple queries to confirm indexing is operational.
- Validate alert emails or messages are sent.

Stress and Volume Test

- Simulate a high volume of logs (e.g., via log generators) to test scalability.
- Monitor system resource usage (CPU, RAM, disk I/O) under stress.
- Determine breaking points or performance degradation thresholds.
- Validate that no data loss or alert delay occurs under volume load.

Recovery Test

- Simulate system failure (e.g., power outage, server crash).
- Ensure SIEM can recover to the last known good state.
- Validate log data integrity after reboot or restore.
- Test backup and restore procedures of logs, rules, and dashboards.

Documentation Test

- Verify the availability and accuracy of system documentation.
- Check that user manuals, system architecture diagrams, and SOPs are clear and up-to-date.
- Ensure incident response playbooks are documented and tested.
- Review change logs and version control documentation for rules/configuration.

User Acceptance Test (UAT)

- Allow small business IT admins and managers to test SIEM features.
- Use real-world scenarios: failed login alerts, malware detection, unauthorized access.
- Gather feedback on usability, responsiveness, and report clarity.
- Ensure the system meets operational expectations before production rollout.

System

- Final system validation test combining all components.
- Review the installation environment (OS, dependencies, network).
- Ensure compliance with internal and regulatory standards.
- Prepare for go-live based on a complete and successful test outcome.

Graphical User Interface (GUI) Layout

A well-designed GUI is essential for small businesses where users might not have specialized cybersecurity knowledge. The SIEM interface should be intuitive, informative, and actionable.

Key GUI Components:

Component	Description
Dashboard	Central visual overview showing real-time alerts, log volume, asset status.
Log Explorer	A search/query interface to browse historical logs across various sources.
Alert Management	View, acknowledge, and respond to triggered alerts.
Rule/Policy Editor	Interface to define or customize correlation rules for threat detection.
Reports Module	Generate and schedule compliance or incident reports.
Source Integration	Add and manage log sources (firewalls, endpoints, etc.).
User Management	Define roles, permissions, and MFA options.
Settings	Configure system options (e.g., data retention, storage, notifications).

User Experience (UX) Features:

- **Color coding:** Highlight severity levels (Red for critical, Yellow for warnings, Green for safe).
- **Navigation panel:** Sidebar for easy module access.
- **Tooltips and help guides:** Provide context-sensitive help for non-experts.
- **Responsive design:** Support for desktops, tablets, and mobile dashboards (if applicable).

Customer Testing

This stage involves **real-world testing of the SIEM system by the intended users (e.g., IT staff or business owners)** in a small business environment.

Objectives:

- Validate that the system is usable and understandable.
- Ensure the SIEM meets the security monitoring needs of the business.
- Collect user feedback to improve the UI and alert logic.

Testing Steps:

1. **Test scenarios:** Simulate login attempts, malware outbreaks, port scans, data exfiltration, etc.
2. **Log review:** Ensure users can trace events and investigate effectively using the GUI.
3. **Alert response:** Test how users respond to real-time alerts (acknowledge, escalate, resolve).
4. **Report verification:** Confirm users can generate and understand reports.
5. **Feedback collection:** Document usability issues, suggestions for simplification, etc.

Outcome:

- Highlighted areas of improvement in GUI usability or alert tuning.
- Confirmation that small business users can interact with the system effectively.
- Basis for refining training materials and guides.

Evaluation

Evaluation Metrics:

Criteria	Description
Accuracy of detection	% of true positive alerts vs false positives/negatives.
System uptime	Reliability of SIEM under normal and stress conditions.
Ease of use	User feedback on navigating and operating the SIEM platform.
Performance	Log ingestion speed, dashboard responsiveness, query execution time.
Security effectiveness	Ability to identify and report common threats and suspicious activities.
Scalability	Can the system handle increased logs or new sources easily?
Compliance support	Ability to generate audit-ready reports.
Cost-effectiveness	Value provided relative to the investment (hardware, software, training).

Evaluation Techniques:

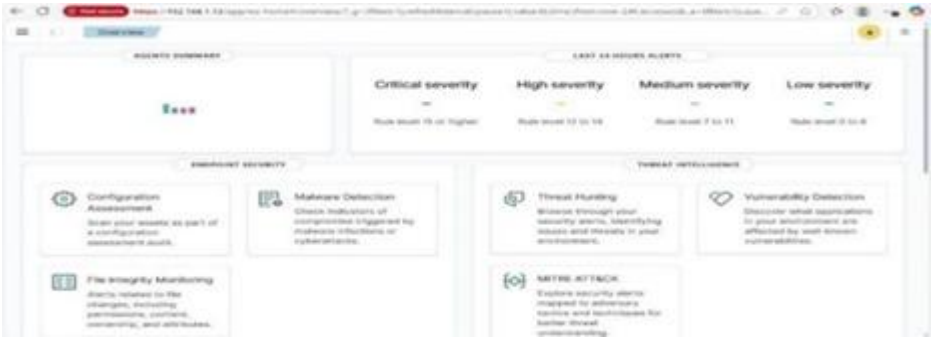
- **Surveys and interviews** with users.
- **Quantitative analysis** from logs and test results.
- **Benchmark comparison** with initial goals and requirements.
- **Incident simulation reviews** to assess detection and response.

Evaluation Outcome:

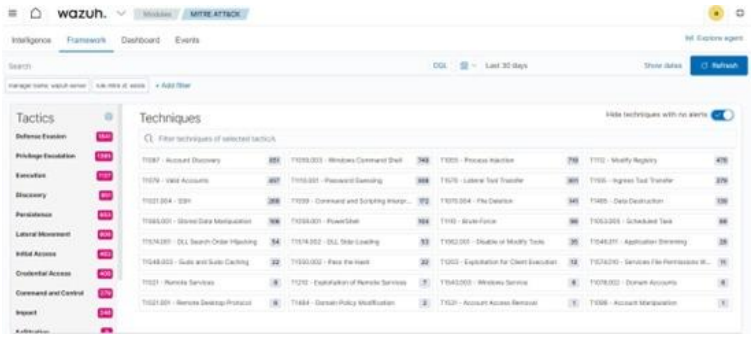
- **Strengths:** Quick alerting, intuitive dashboards, flexible rule customization.
- **Areas to improve:** Alert tuning to reduce false positives, more guided help for first-time users.
- **Conclusion:** The SIEM system is **fit for small business use**, scalable for future growth, and effective in enhancing security visibility and response capabilities.

1.Main Chat Interface

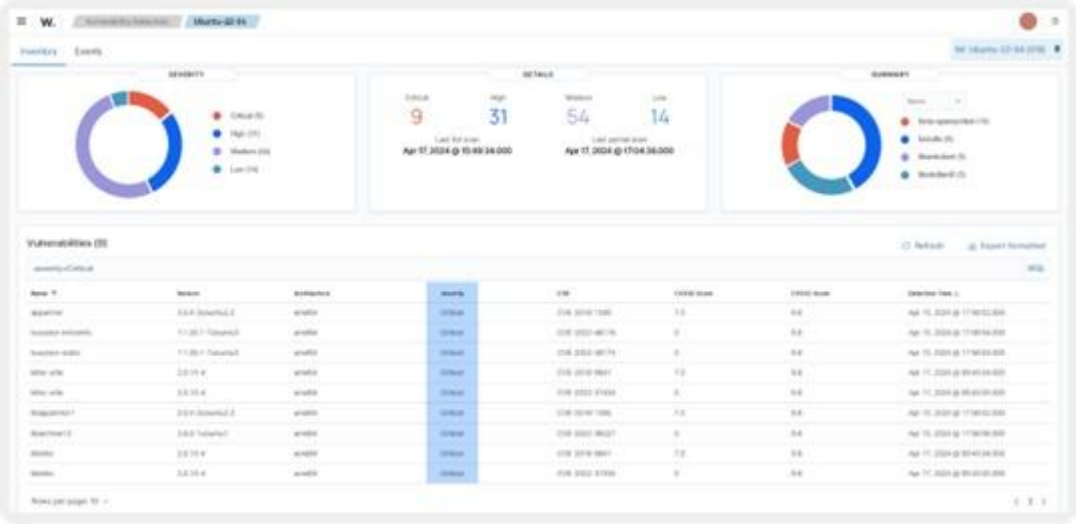
2. Admin Dashboard



3.MITRE ATTACK



4.Vulnerability Detection



4. Conclusion

Implementing a **Security Information and Event Management (SIEM)** solution in small businesses represents a pivotal step toward enhancing their cybersecurity posture in an increasingly hostile digital environment. This project explored the feasibility, benefits, and challenges of SIEM deployment specifically tailored for small organizations.

Key Achievements

- **Demonstrated Feasibility**: The study confirmed that small businesses can effectively deploy and benefit from SIEM solutions, particularly through open-source platforms or cloud-based services that offer cost-effective scalability.
- **Identified Suitable Tools**: Tools such as **Wazuh**, **Splunk (Free Tier)**, and **AlienVault OSSIM** emerged as practical solutions for SMBs, balancing cost, features, and usability.
- **Developed a Deployment Roadmap**: A simplified and practical SIEM implementation framework was established, suitable for the resource constraints of small businesses.
- **Highlighted Value for Compliance**: SIEMs were shown to assist in meeting regulatory and compliance requirements, which is increasingly critical even for smaller firms.

Lessons Learned

- **Customization is Crucial**: One-size-fits-all solutions are rarely effective. Small businesses require tailored configurations that align with their unique risk profiles and industry needs.
- **Training is Often Overlooked**: Effective SIEM usage depends heavily on users' understanding of alerts and dashboards. Without training, the benefits of SIEM can be significantly diminished.
- **Start Small, Scale Gradually**: Beginning with core features (log management and basic correlation rules) allows small businesses to avoid being overwhelmed and build confidence over time.
- **Cloud SIEMs Offer Flexibility**: For many SMBs, cloud-based SIEMs provide easier deployment, automatic updates, and lower upfront costs compared to on-premises solutions.

Development Process

The research and development journey followed several key phases:

1. **Needs Assessment** – Identified the specific threats and requirements of small businesses.
2. **Tool Evaluation** – Compared various SIEM platforms in terms of cost, features, scalability, and ease of use.
3. **Prototype Deployment** – Simulated the deployment of a basic SIEM setup using an open-source tool (e.g., Wazuh).
4. **Monitoring & Analysis** – Demonstrated how logs and alerts can be analyzed to detect common threats.
5. **Documentation & Review** – Developed best practices and created reference material to guide future implementations.

Final Thoughts

Small businesses face a growing need to enhance their cybersecurity capabilities, yet often struggle with budget and expertise limitations. SIEM tools, once considered out of reach, are now increasingly accessible thanks to cloud services and open-source development. While challenges remain—especially in setup and ongoing management—careful planning, gradual scaling, and training can bridge the gap.

Ultimately, SIEM solutions provide not just security, but **visibility, accountability, and resilience**—all of which are essential for small businesses to thrive in the digital age.

5. Further Development

While significant progress has been made to make SIEM tools more accessible to small businesses, there is still considerable room for advancement. These developments aim to enhance usability, reduce operational costs, improve detection capabilities, and increase security maturity across small business environments.

1. Enhanced Usability and Automation

Problem: Most SIEM platforms are built with enterprise users in mind, often resulting in complex dashboards and alert systems that overwhelm small business users.

Future Direction:

- **Simplified Dashboards**: SIEMs should offer intuitive, customizable dashboards with preset configurations for small businesses.
- **Automated Onboarding Wizards**: Development of guided setup tools can streamline the initial configuration process for businesses without dedicated security teams.
- **Low-Code Rule Management**: Tools that allow non-technical users to create correlation rules through drag-and-drop interfaces or natural language processing.

2. AI-Driven Threat Detection

Problem: Small teams often lack the manpower to monitor and respond to the sheer volume of security alerts.

Future Direction:

- **Anomaly Detection with Machine Learning**: Use lightweight, explainable AI models to detect abnormal behaviors based on historical data.
- **Context-Aware Alerts**: Develop smarter alert systems that prioritize incidents based on risk levels and business impact.
- **Behavioral Analytics**: Integrate UEBA (User and Entity Behavior Analytics) to detect insider threats and advanced persistent threats.

3. Integration with Existing Business Tools

Problem: SIEMs often operate in isolation from other business applications, which limits their effectiveness in SMBs.

Future Direction:

- **Native Integrations**: SIEM systems should offer built-in connectors for platforms like Microsoft 365, Google Workspace, QuickBooks, and CRM systems.
- **Unified Security Dashboards**: Merge endpoint, email, and network security data into a single interface to enhance decision-making.

. **API-Driven Extensions**: Enable easy integration with third-party SaaS platforms and cybersecurity tools.

4. Cost Optimization and Scalability

Problem: Even with open-source and freemium options, ongoing costs (storage, cloud usage, human resources) can escalate quickly.

Future Direction:

- **Modular Pricing Models**: Usage-based pricing that allows businesses to pay only for the services they need.
- **Serverless SIEM Architectures**: Using event-driven, cloud-native SIEM backends (e.g., AWS Lambda) to reduce infrastructure costs.
- **Edge Processing**: Shift some detection and log analysis to edge devices to reduce data transfer and latency costs.

5. Tailored Industry Solutions

Problem: Small businesses across different industries (e.g., healthcare, retail, finance) have distinct regulatory and security needs.

Future Direction:

- **Pre-configured Templates**: Provide vertical-specific use cases, dashboards, and compliance reports.
- **Industry Compliance Kits**: Build-in compliance tools for HIPAA, PCI-DSS, GDPR, and others—complete with automated audit logs and incident reporting.

6. Community and Knowledge Sharing

Problem: SMBs often lack access to high-quality threat intelligence and security best practices.

Future Direction:

- **SIEM-as-a-Service Communities**: Shared threat intelligence networks tailored for SMBs.
- **Open Threat Libraries**: Expand public libraries of correlation rules, detection signatures, and alert response templates.
- **Gamified Training Modules**: Use simulations and interactive tools to train small business staff on incident response and monitoring.

7. Managed SIEM and Hybrid Services

Problem: Many small businesses cannot afford full-time cybersecurity staff.

Future Direction:

- **MSP/MSSP Integration**: Development of lightweight SIEM agents designed for easy deployment and management by Managed Service Providers.
- **Hybrid SIEM Models**: Combine in-house monitoring with outsourced 24/7 SOC services to provide a balance of control and support.

Summary

The future of SIEM for small businesses lies in **simplifying complexity**, **leveraging automation and AI**, and **creating ecosystem-driven solutions**. With focused development on user experience, integration, affordability, and education, SIEM can become a truly transformative security solution—not just for large corporations but for businesses of all sizes.

6. Reference

1. **Wazuh – Open Source SIEM Platform Documentation**
   https://documentation.wazuh.com/
2. **AlienVault OSSIM – Unified Security Management Platform**
   https://cybersecurity.att.com/products/ossim
3. Splunk Free and Cloud Options for SMBs.-
   https://www.splunk.com/en_us/download.html
4. **Security Onion – Open Source Threat Hunting & Monitoring**
   https://securityonion.net
5. **LogRhythm: The SIEM Buyer's Guide for SMBs**
   LogRhythm, 2022.
   https://logrhythm.com
6. **ENISA Threat Landscape Reports**
   European Union Agency for Cybersecurity.
   https://www.enisa.europa.eu/publications
7. **Ponemon Institute – 2023 Cost of a Data Breach Report**
   Sponsored by IBM Security.
   https://www.ibm.com/reports/data-breach

8. Appendix

A. Acronyms and Definitions

Acronym	Description
SIEM	Security Information and Event Management
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
SOC	Security Operations Center
EDR	Endpoint Detection and Response
VPN	Virtual Private Network
MFA	Multi-Factor Authentication
UEBA	User and Entity Behavior Analytics

B. Sample Log Sources

Device/Service	Type of Logs Captured
Firewall	Traffic logs, Denied/Allowed connections
Antivirus/EDR	Threat detections, quarantines
Web Server (e.g., Apache, Nginx)	Access logs, error logs
Email Server	Email traffic, spam, phishing attempts
Cloud Services (e.g., Google Workspace, Microsoft 365)	Login events, file access
Operating Systems (Windows/Linux)	System logs, login attempts
Authentication Services (e.g., Active Directory)	Login/logoff, failed authentications

C. SIEM Use Case Examples

Use Case	Description
Brute Force Detection	Detect repeated failed login attempts across multiple endpoints.
Unauthorized Access Attempt	Alert when a user accesses restricted folders or data.
Suspicious File Activity	Detect abnormal file creation, modification, or deletion.
Data Exfiltration	Identify large or unusual outbound data transfers.
Privileged Account Monitoring	Track the behaviour of admin-level accounts for anomalies.

D. Recommended SIEM Tools for Small Businesses

Tool Name	Deployment	Cost	Notes
Wazuh	On-premise/Cloud	Free/Open Source	Integrates with ELK Stack. Good for SMBs.
Gray log	On-premise/Cloud	Free & Paid Tiers	Great for centralized log management.
Splunk Free	On-premise	Free up to 500MB/day	Scalable, but premium tiers can be costly.
Log Point	On-premise/Cloud	Paid, SMB-friendly	Tailored pricing for small orgs.

E. Incident Response Workflow (Simplified)

1. **Alert** triggered by SIEM
2. **Triage** the event – determine severity and scope
3. **Investigate** using correlated logs and system data
4. **Contain** the threat (e.g., isolate host)
5. **Eradicate** root cause (e.g., remove malware, patch vulnerabilities)
6. **Recover** systems and monitor closely
7. **Document** the incident and lessons learned

F. Log Retention Guidelines

Log Type	Retention Period	Notes
Authentication Logs	1 year	Helps trace access-related incidents
Firewall Logs	3-6 months	Key for tracking threats at the perimeter
Email Logs	6-12 months	Critical for phishing investigations
Application Logs	6-12 months	Depends on compliance requirements
SIEM Audit Logs	1 year	Maintain for accountability and audits

G. Compliance Considerations

Regulation	Relevant Requirements
GDPR	Data minimization, breach reporting, log access control
HIPAA	Audit controls, access logs, security incident tracking
PCI DSS	1-year log retention, daily log review, secure storage

H. SIEM Deployment Checklist for SMBs

- Identify and prioritize log sources
- Choose a SIEM solution appropriate to budget and scale
- Set up log forwarding and normalization
- Define correlation rules and alerts
- Establish alert triage and escalation procedures
- Train staff on SIEM usage and response
- Review logs and alerts regularly
- Conduct periodic rule tuning and audits

7.1 Setup Guide

Tool	Cost	Pros	Cons
Wazuh	Free	Integrated with ELK Stack, flexible, scalable	Setup can be technical
Gray log	Free (with premium options)	Easy UI, good community support	Advanced features in paid version
Security Onion	Free	Full security suite	Resource-intensive
Splunk Free	Free up to 500MB/day	Industry standard	Costs escalate with scale
Log Point	Paid	SMB-friendly, compliance-ready	Licensing costs

API Key Acquisition

Acquiring an **API key** for use with a **SIEM system** in a small business environment depends on the specific **SIEM platform** and the **third-party services** (e.g., cloud providers, firewalls, antivirus systems) you want to integrate. Below is a general-purpose guide followed by examples for popular SIEMs and services:

1. Determine the Integration Requirement

- Are you pulling logs from Microsoft 365, AWS, Google Workspace, a firewall, or an antivirus platform?
- Is the SIEM pulling **data in** (e.g., threat intel feeds, SaaS logs) or pushing **data out** (e.g., alerts to Slack, webhooks)?

2. Access the Target Platform's API Settings

- Log into the third-party platform (e.g., Microsoft 365, AWS, CrowdStrike)
- Navigate to **Developer Settings**, **API Management**, or **Integrations**
- Find or generate a **new API key/token** (this usually involves admin privileges)

3. Apply Security Best Practices

- Generate **read-only** keys if possible (least privilege)
- Store API keys securely (e.g., environment variables, secrets manager)
- Set expiration and rotate keys periodically

4. Integrate API Key into SIEM

- Use the SIEM's configuration files, UI, or a plugin/module to add the key
- Example: in Wazuh, this might be in `wazuh-modulesd.json`