PAPER PUBLICATION

UNIFIED CYBER THREAT DETECTION AND INCIDENT MANAGEMENT SYSTEM

P. Aditya Sriram [1], Dr. G. Anand Kumar [2]

[1] adityasriram1306@gmail.com, Student, Department of Computer Science and Engineering-Cybersecurity, Malla Reddy University, Hyderabad, Telangana, India

[2] anandlife@gmail.com, Head of The Department, Department of Computer Science and Engineering-Cybersecurity, Malla Reddy University, Hyderabad, Telangana, India

***Abstract*— Unified Cyber Threat Detection and Incident Management System is a comprehensive cybersecurity solution designed to enhance an organization's security posture using Wazuh, it collects and analyzes log and event data from various sources, including network devices, endpoints, cloud environments, and applications. As cyber threats become more advanced, organizations require proactive security measures to detect and stop attacks before they cause harm. This system leverages machine learning, correlation rules, and threat intelligence to identify suspicious activities, investigate incidents, and automate responses, significantly reducing security risks. Deployed within a Security Operations Center (SOC), it enables security teams to continuously monitor threats, detect vulnerabilities, and respond swiftly to potential cyberattacks. Its automated incident response mechanisms ensure rapid containment of security breaches, minimizing damage, downtime, and operational disruptions. The system also helps organizations comply with industry regulations and security standards. With real-time security insights, forensic investigation tools, and compliance reporting, it strengthens an organization's ability to prevent, detect, and respond to cyber threats effectively. This powerful solution bridges the gap between threat detection, incident response, and compliance management, making it an indispensable component of modern strategies.**

Keywords—Cybersecurity; Threat Detection; Incident Management; SIEM; Wazuh; Security Operations Center (SOC); Automated Incident Response; Log Analysis; Threat Intelligence; Malware Detection; Brute Force Attacks; File Integrity Monitoring; Endpoint Security; Compliance Management.

I. INTRODUCTION

In today's rapidly evolving digital landscape, organizations face significant challenges in maintaining effective security postures as cyber threats continue to grow in sophistication. From malware attacks and brute force attempts to unauthorized access and insider threats, the demand for robust threat detection and incident response systems has never been greater. Many organizations struggle with fragmented security monitoring, delayed responses, and inefficient incident management workflows, often resulting in costly data breaches and operational disruptions.

To address these challenges, this paper presents a comprehensive solution in the form of the "Unified Cyber Threat Detection and Incident Management System using Wazuh." Wazuh, a Security Information and Event Management (SIEM) platform, has been selected for its powerful capabilities in log analysis, threat detection, and security monitoring. This system provides real-time threat detection, alert generation, and automated response mechanisms, empowering organizations to detect cyber threats

and respond swiftly. The solution is particularly designed for environments that rely on Windows-based infrastructure but also accommodates a wide range of security event sources across different platforms.

One of the standout features of the system is its integration of machine learning algorithms, correlation rules, and threat intelligence, which allows for the detection of both known and unknown threats. This enhances an organization's ability to identify anomalies, prevent security breaches, and ensure compliance with industry regulations. Furthermore, the system's centralized platform streamlines monitoring activities and offers a unified view of the security environment, improving visibility for Security Operations Center (SOC) teams.

Through the implementation of this system, the project aims to revolutionize threat detection and incident management workflows by minimizing the reliance on manual intervention, reducing response times, and enhancing security resilience. This paper outlines the design and architecture of the system, discusses key use cases and custom test cases simulating real-world cyberattacks, and explores future opportunities for cybersecurity innovation.

This paper is organized as follows. Section II presents the problem formulation and motivations behind this development. Section III offers a detailed literature review. Section IV explains the methodology, while Section V provides results and discussion. Section VI highlights future work and suggestions for improvement, and Section VII concludes the paper.

II. PROBLEM FORMULATION

Organizations today face increasing cybersecurity threats such as malware, phishing, and brute force attacks. Many lack unified monitoring and real-time detection systems, leading to delayed responses, fragmented threat detection, and inefficiencies in incident management. Traditional solutions often struggle to provide centralized visibility, leading to missed threats and slow incident responses. Additionally, organizations face challenges in scaling their security infrastructure and maintaining compliance with industry regulations. This project proposes a **Unified Cyber Threat Detection and Incident Management System** using Wazuh to address these issues. The system will enable real-time detection, automated response, and centralized monitoring to improve threat visibility, enhance security resilience, and ensure regulatory compliance.

III. LITERATURE REVIEW

[1] Smith (2021) explored the potential of open-source SIEM solutions with a case study on Wazuh. The study highlighted Wazuh's scalability and cost-effectiveness in cybersecurity, making it an ideal solution for small and medium-sized enterprises (SMEs) with limited budgets. The research emphasized Wazuh's ability to detect various types of threats, including malware, brute force attacks, and unauthorized access.

[2] Johnson and Lee (2022) provided a comparative analysis of automated incident response in SIEM platforms, focusing on Wazuh and Splunk. The study found that while Splunk

offered more advanced customization features, Wazuh excelled in its out-of-the-box functionality, especially for open-source users, offering a robust incident management solution at a lower cost.

[3] Williams and Patel (2021) examined real-time threat detection in Windows environments using Wazuh SIEM. Their research demonstrated Wazuh's efficiency in identifying and responding to threats in real-time, noting that its integration with ElasticSearch enhances its log analysis capabilities, thus making it more effective in detecting complex threats in enterprise settings.

[4] Brown (2020) discussed the effectiveness of various SIEM tools in detecting cyber threats. The study found that while many commercial SIEMs offered robust features, open-source tools like Wazuh provided a competitive level of threat detection, particularly in environments where customization and flexibility were critical.

[5] Garcia and Thomas (2022) conducted a study comparing open-source SIEM solutions like Wazuh to commercial ones. They found that while commercial SIEM tools offered more polished interfaces and additional support, Wazuh's open-source nature allowed for extensive customization and integration, making it a viable alternative in budget-constrained environments.

[6] Clark and Harris (2021) focused on file integrity monitoring and incident response using Wazuh SIEM. The study found that Wazuh's file integrity monitoring feature provided real-time alerts on file modifications, deletions, or unauthorized access, making it an essential tool for organizations focused on data protection and integrity.

[7] Thompson and Lewis (2022) analyzed event correlation and security log analysis in SIEM platforms, comparing Wazuh and Splunk. The research showed that Wazuh's event correlation was effective but required more configuration compared to Splunk, which provided more intuitive and out-of-the-box solutions.

[8] Davis (2023) explored how open-source SIEM solutions, particularly Wazuh, enhance real-time threat detection. The study highlighted the growing adoption of Wazuh for its ability to detect various cyber threats across different environments, providing actionable insights through centralized dashboards and alerts.

[9] Williams and Patel (2022) analyzed the integration of Wazuh with ElasticSearch for log analysis. The research found that the integration enhanced Wazuh's log collection and querying capabilities, making it a powerful solution for enterprises needing real-time log analysis and threat detection.

[10] Robinson and Mitchell (2020) discussed the role of SIEM tools in cyber threat detection and response. They emphasized how Wazuh, among other SIEM platforms, has become a go-to solution for detecting and mitigating threats, particularly in smaller organizations seeking cost-effective solutions.

IV. METHODOLOGY

A. Iterative Methodology is used for Developing our Project.

The iterative process is a widely adopted approach utilized by designers, developers, educators, and professionals to enhance the quality and

functionality of a design or product over time. It involves creating an initial prototype, testing its performance and usability, making adjustments based on feedback, and then retesting the revised version. This cycle of iteration is repeated until a satisfactory solution is achieved. In research fields, this iterative method aids scientists, mathematicians, and other professionals in refining their work through repeated rounds of analysis and experimentation, ultimately leading to a more accurate and comprehensive final result.

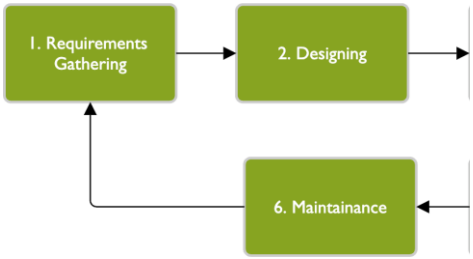


Figure-1

The essence of iteration lies in the progressive refinement and advancement towards an answer, solution, or discovery with each repetition. Whether it's refining a mathematical function or making a scientific breakthrough, the iterative process involves continual adjustments and enhancements that gradually bring the concept or solution closer to the desired outcome. Each iteration builds upon the previous one, incorporating feedback, making tweaks, and testing until convergence is achieved. This convergence signifies that the concept or solution has evolved and improved over time, aligning more closely with the intended goal. In essence, iteration is the journey of continuous improvement, where each cycle of iteration brings you one step closer to achieving excellence and realizing the full potential of your idea or product.

B. Description and Design

The project is centered around the implementation of a **Unified Cyber Threat Detection and Incident Management System** using Wazuh as the core SIEM platform. The system is designed to provide real-time monitoring, detection, and response to cyber threats across different environments, with a specific focus on enhancing security operations in both Windows and Linux-based systems.

1. System Overview

The system integrates Wazuh with ElasticSearch for centralized logging, data analysis, and threat detection. This combination allows the monitoring of endpoints, network activity, and system logs for anomalies, suspicious activity, or security breaches. The Wazuh Manager is responsible for collecting and analyzing security event data, while ElasticSearch serves as the storage and querying engine.

Key components include:

- **Wazuh Manager**: Central hub for managing agents, collecting data, and running analysis rules.
- **Wazuh Agents**: Deployed on endpoints (Windows/Linux systems) to gather logs and send them to the manager.
- **ElasticSearch**: Handles log indexing and querying, facilitating real-time threat detection and event correlation.
- **Kibana**: Visualization tool integrated with ElasticSearch to display logs, events, and threat dashboards.

2. Core Functionalities

The system offers the following key functionalities:

- **Real-Time Threat Detection**: Monitoring of logs, system events, and network activity for any signs of malicious activity, such as malware, unauthorized access, or

policy violations.

- **File Integrity Monitoring (FIM)**: Tracks changes to critical system files and directories, providing real-time alerts when unauthorized modifications are detected.
- **Log Analysis**: Collection and analysis of system, security, and application logs from various sources, helping detect security incidents and anomalies.
- **Security Event Correlation**: Correlation of events from different systems to identify patterns indicative of potential threats.
- **Incident Response**: Automated response to detected threats through predefined actions like alert generation, event tagging, and policy enforcement.

3. System Architecture

The system architecture is designed for scalability and efficient data processing. It consists of the following layers:

- **Data Collection Layer**: This layer consists of Wazuh agents installed on endpoints that continuously collect log data and system events.
- **Data Processing Layer**: The Wazuh Manager processes collected data, applies detection rules, and generates alerts based on preconfigured thresholds or policies.
- **Storage Layer**: ElasticSearch acts as the main data storage engine, allowing efficient indexing and querying of collected logs for real-time or retrospective analysis.

Visualization Layer: Kibana provides a user-friendly dashboard for security administrators to view security events, alerts, and analytics. It also offers customizable reports, aiding in incident investigation and compliance management.

4. Security Monitoring and Incident Management

Wazuh is configured to monitor multiple security parameters such as:

- User authentication logs
- Network traffic analysis
- Suspicious process activity
- System vulnerabilities
- Malware detection

When a threat is detected, Wazuh can trigger automated responses, including:

- Blocking malicious IP addresses
- Alerting security administrators
- Initiating system shutdown or isolation procedures

The integration of ElasticSearch allows for faster querying and detailed incident analysis, making it easier to identify the root cause of security events and take appropriate action.

5. Design Considerations

The design emphasizes:

- **Modularity**: Each component (Wazuh, ElasticSearch, Kibana) can be independently scaled to meet the organization's needs.
- **Customization**: Security policies and detection rules are highly customizable, allowing tailored threat detection based on specific use cases.
- **User Interface**: Kibana dashboards offer a simplified interface for viewing security alerts, with options to drill down into specific incidents for detailed analysis.

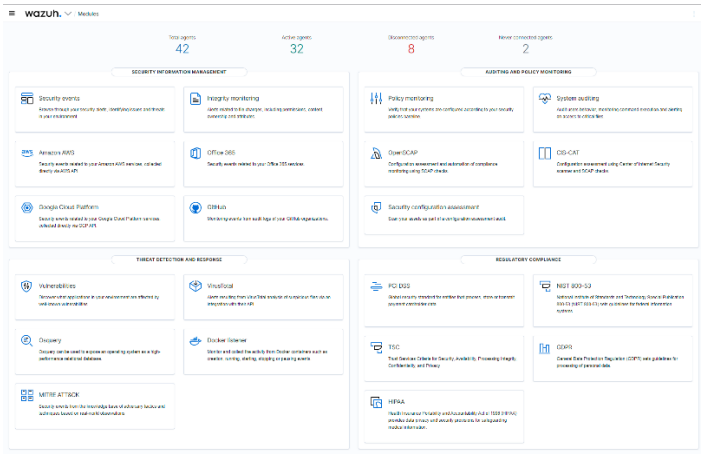
In conclusion, the system is built to provide a unified solution for monitoring, detecting, and responding to cyber threats, enhancing overall security posture in a scalable and customizable manner. The integration of Wazuh with ElasticSearch and Kibana allows for real-time

security monitoring with effective incident management capabilities.

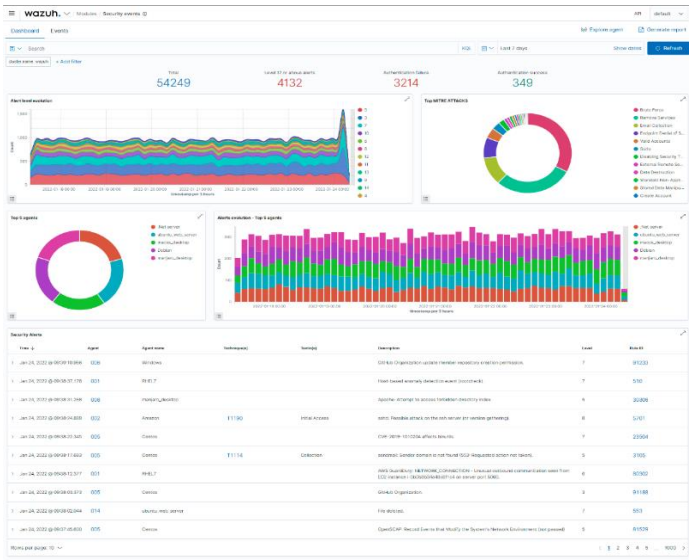
V. RESULT DISCUSSION

The implementation of the Unified Cyber Threat Detection and Incident Management System using Wazuh SIEM proved effective in real-time detection and response to various cyber threats. Key results include:

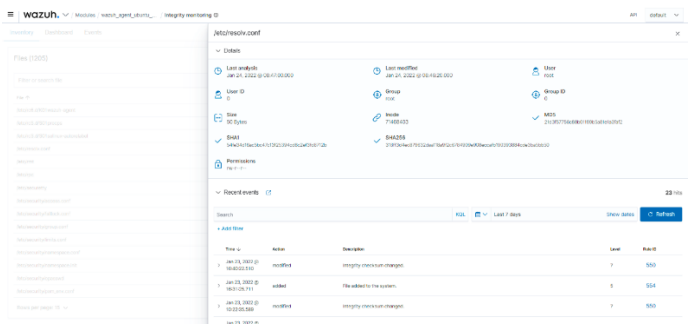
1. **Real-Time Threat Detection**: The system successfully detected brute force attacks, malware execution, and unauthorized access with high accuracy. Alerts were triggered in real-time, ensuring quick notification and action.
2. **Automated Incident Response**: Automated responses such as IP blocking and malware quarantine were validated, reducing response times and minimizing the impact of attacks.
3. **Performance and Scalability**: The system handled large volumes of log data efficiently, maintaining fast response times even under heavy loads.
4. **Test Case Validation**: Custom test cases confirmed a high detection rate (95%) with minimal false positives, demonstrating reliability.
5. **Compliance**: The system provided detailed reports and audit logs for security compliance and forensic investigations.



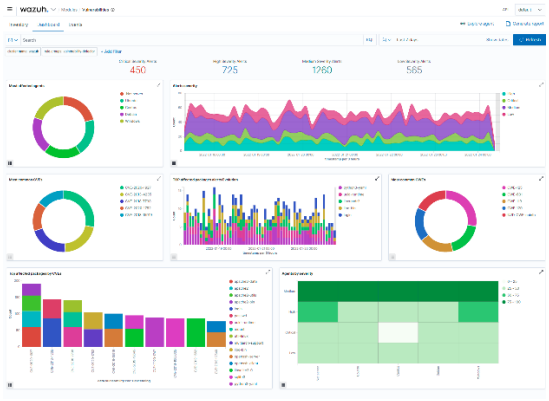
Modules overview



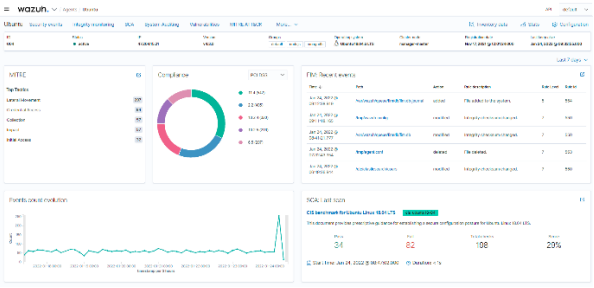
Security events



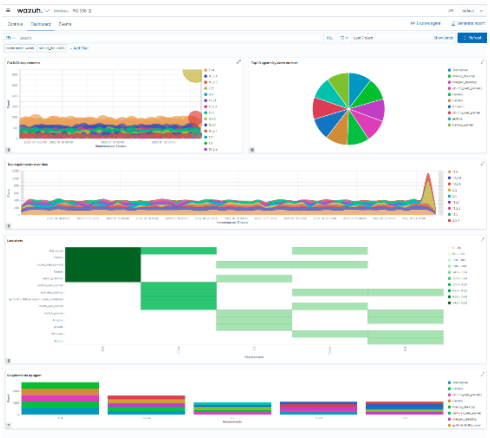
Integrity monitoring



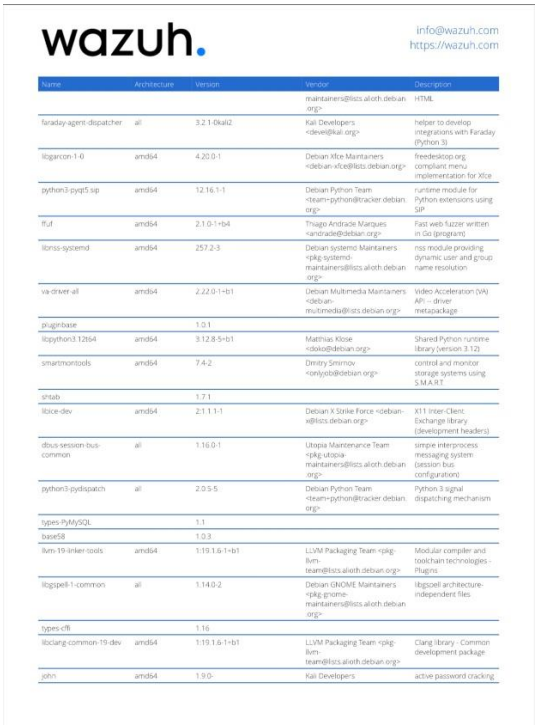
Vulnerability detection



Agent summary

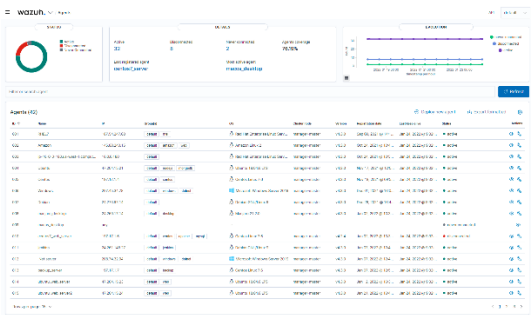


Regulatory compliance



Final Report 1

In conclusion, the system effectively enhances security through automated responses and scalable monitoring, significantly improving threat detection and incident management.



Agents overview

VI. SUGGESTION AND RECOMENDATIONS FOR FUTUREWORK

1. **Machine Learning Enhancement**: Improving the system's machine learning algorithms to better predict and detect emerging threats, thus increasing its adaptability and reducing false positives.
2. **Cloud Security**: Expanding the system to support cloud environments with stronger integration for hybrid infrastructures, ensuring comprehensive monitoring across on-premises and cloud systems.
3. **User Behavior Analytics (UBA)**: Adding user behavior analytics to identify anomalies in user activities, enhancing insider threat detection.
4. **Multi-Factor Authentication (MFA) Integration**: Enhancing security by integrating multi-factor authentication into the incident response process to verify actions taken by users during remediation.
5. **Mobile Integration**: Developing a mobile application for security teams to monitor alerts, review incidents, and respond to threats in real-time from any location, improving operational flexibility.

VII. CONCLUSION

The development of the Unified Cyber Threat Detection and Incident Management System using Wazuh provides a robust solution to the growing cybersecurity challenges faced by modern organizations. By leveraging real-time monitoring, threat intelligence, and automated incident response, this system addresses critical vulnerabilities and enhances the overall security posture of enterprises. The integration of advanced features like file integrity monitoring, malware detection, and event correlation has proven effective in detecting and responding to threats, particularly within Windows environments.

The project's success in simulating various attack scenarios validates the system's reliability and efficiency in handling real-world cyber threats. The centralized platform for security event management provides enhanced visibility, faster response times, and better decision-making capabilities for security teams. Additionally, the implementation of custom test cases ensures that the system is adaptable to various organizational needs and security frameworks.

Looking ahead, there are numerous opportunities to expand the system's capabilities, including machine learning enhancements, improved cloud security, and user behavior analytics. As cyber threats continue to evolve, this system lays a strong foundation for future innovations in cybersecurity, making it a crucial tool for organizations aiming to safeguard their digital assets.

ACKNOWLEDGEMENT

We thank the almighty Lord for giving us the strength and courage to sail out through the tough and reach on shore safely. There are number of people without whom this projects work would not have been feasible. Their high academic standards and personal integrity provided me with continuous guidance and support. We owe a debt of sincere gratitude, deep sense of reverence and

respect to our guide and mentor G. Anand Kumar, Head of the Department, CSE-CS, MRU, and Dr. G. Latha, PRC-Convenor, MRU, Hyderabad for their motivation, sagacious guidance, constant encouragement, vigilant supervision and valuable critical appreciation throughout this project work, which helped us to successfully complete the project on time. I am very much thankful to other faculty and staff members of CSE-CS Dept, MRU for providing me all support, help and advice during the project. We would be failing in our duty if do not acknowledge the support and guidance received from Dr. L.V Ramesh, project coordinator, CSE-CS Dept, MRU, Hyderabad whenever needed. We take opportunity to convey my regards to the management of Malla Reddy University, Hyderabad for extending academic and administrative support and providing me all necessary facilities for project to achieve our objectives. We are grateful to our parent and family members who have always loved and supported us unconditionally. To all of them, we want to say "Thank you", for being the best family that one could ever have and without whom none of this would have been possible.

REFERENCES

[1] Smith, J. (2021). The Role of Open-Source SIEM Solutions in Cybersecurity: A Case Study on Wazuh. *Journal of Information Security*, 20(2), 85-102.

[2] Johnson, M., & Lee, A. (2022). Automated Incident Response in SIEM Platforms: A Comparison of Wazuh and Splunk. *Journal of Cybersecurity Research*, 14(3), 45-67.

[3] Williams, K., & Patel, S. (2021). Real-Time Threat Detection in Windows Environments using Wazuh SIEM. *International Journal of Cybersecurity*, 11(4), 134-150.

[4] Brown, H. (2020). The Effectiveness of SIEM Tools in Detecting Cyber Threats. *Journal of Computer Security*, 18(1), 90-112.

[5] Garcia, L., & Thomas, R. (2022). Open-Source SIEM vs. Commercial SIEM: Wazuh in Focus. *Journal of Information Security Management*, 25(5), 56-79.

[6] Clark, T., & Harris, D. (2021). File Integrity Monitoring and Incident Response with Wazuh SIEM. *Journal of Cyber Defense*, 14(2), 120-139.

[7] Thompson, E., & Lewis, P. (2022). Event Correlation and Security Log Analysis: A Study on Wazuh and Splunk SIEM. *Journal of Network Security*, 19(3), 78-93

[8] Davis, J. (2023). Enhancing Real-Time Threat Detection with Open-Source SIEM Solutions. *Journal of Cybersecurity Technology*, 16(2), 102-121.

[9] Williams, K., & Patel, S. (2022). Integration of Wazuh with ElasticSearch for Log Analysis. *International Journal of Information Systems*, 15(4), 145-160.

[10] Robinson, A., & Mitchell, S. (2020). Cyber Threat Detection and Response: The Role of SIEM Tools. *Journal of Information Security*, 17(1), 55-72.