International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

Smart Cyber Surveillance System for Internal Anomalies and Malicious Domain Identification

M. Vamshi[1], Gundeti Prahasa[2], Bhukya Prabhudas[2], Gugulothu Sriram[2]

[1]Assistant Professor, [2]UG Student, [1,2]Department of Computer Science and Engineering

[1,2]Vaagdevi Engineering College, Bollikunta, Warangal, 506005, Telangana, India.

ABSTRACT

The widespread adoption of internet technologies within organizations has substantially increased exposure to digital security risks, including harmful software, deceptive online schemes, and unsafe web domains. As enterprises increasingly depend on online platforms for daily operations, maintaining secure browsing environments and tracking user access patterns has become essential for safeguarding network integrity. A key challenge lies in the lack of dynamic and immediate detection mechanisms capable of preventing access to dangerous domains before any damage occurs. Traditional security methods, such as predefined blocklists and manual oversight, operate in a reactive manner and fail to adapt to the constantly changing landscape of cyber threats. These conventional techniques are hindered by slow response times, minimal automation, scalability issues, and poor adaptability to newly emerging attack strategies. Consequently, organizations remain at higher risk, with limited visibility and control over user interactions with web resources. To overcome these challenges, there is a demand for a smart, automated, and responsive security framework that can actively identify risks, supervise user activity, and block unsafe web access in real time. Addressing this requirement, the proposed solution presents a web-based system developed using Django, integrated with the Maltiverse threat intelligence an Application Programming Interface (API) for instant domain evaluation. This platform allows administrators to oversee user management, track browsing behavior, record suspicious events, and analyze threat-related data through visual insights. Additionally, it performs domain verification and Internet Protocol (IP) level inspection to prevent access to potentially dangerous websites while maintaining comprehensive logs of user actions.

Key words: Network Security, Django Framework, Threat Intelligence, Real-time Domain Evaluation, Proactive Defense Mechanisms.

1. INTRODUCTION

The frequency and severity of cyber intrusions have escalated significantly in recent years, leading to widespread operational and financial damage across multiple sectors. A well-known illustration is the WannaCry ransomware attack, which compromised over 200,000 computer systems in more than 150 nations [1]. This incident had a particularly severe effect on the National Health Service, where access to vital medical data was disrupted, resulting in postponed treatments, cancelled appointments, and interruptions to critical healthcare services [1]. Statistical analyses further reveal an alarming surge in ransomware activities, including an approximate 435% rise between 2019 and 2020 [1]. Moreover, a significant percentage of industry experts now regard cybersecurity threats as one of the most critical risks to business continuity, with over half of utility-sector organizations reporting direct experiences with cyber incidents [1]. The economic impact of such attacks is equally concerning, as demonstrated by the SolarWinds cyberattack, which is estimated to have caused financial damages reaching up to $100 billion [1].

Received: 28-02-2026 | Accepted: 02-04-2026 | Published: 10-04-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

In response to this rapidly intensifying threat environment, Cyber Threat Intelligence (CTI) has become an essential element in advanced security frameworks. CTI refers to the systematic process of gathering, processing, and interpreting threat-related information to produce actionable insights that support early detection, prevention, and effective mitigation of cyber risks [2]. By enhancing situational awareness and enabling informed decision-making, CTI allows organizations to strengthen their defensive strategies and respond more efficiently to potential incidents. Research findings indicate that enterprises implementing CTI-driven approaches experience notable improvements in threat detection accuracy and response time, with many organizations establishing specialized teams dedicated to intelligence operations and integrating CTI into their daily security workflows [2]. A key aspect of modern CTI implementation is collaborative intelligence exchange, where platforms enable multiple users and organizations to contribute and consume threat data efficiently. The concept of user-driven threat intelligence sharing is illustrated in Figure 1, which demonstrates how information flows between contributors and consumers using MISP [1]. Such systems facilitate structured sharing of threat indicators, enabling faster detection and coordinated defense against cyberattacks.

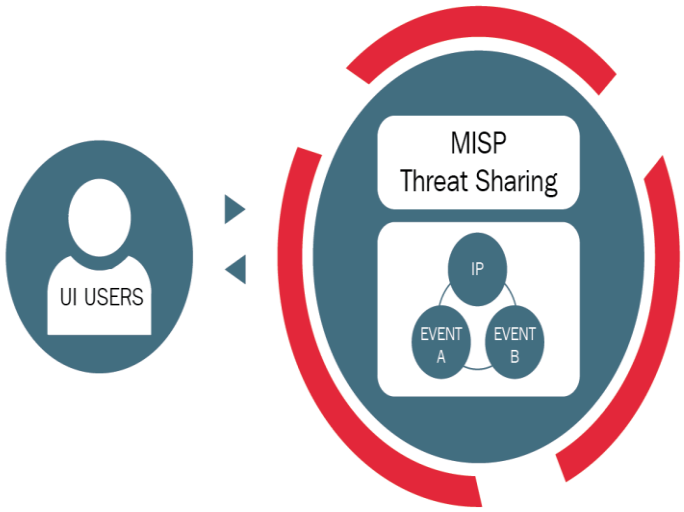


Fig. 1.1 User-Driven Threat Intelligence Sharing with MISP

However, the cybersecurity landscape continues to grow increasingly complex due to rapid technological advancements and the sophistication of modern attack techniques. Conventional security models that primarily focus on identifying system weaknesses or configuration errors are no longer adequate to counter evolving threats [3]. A significant limitation in CTI adoption is the restricted visibility available to individual organizations, as no single entity has access to a complete view of the global threat ecosystem. This constraint underscores the importance of collaborative intelligence sharing across organizations and sectors. By exchanging threat indicators, attack patterns, and contextual insights, organizations can collectively enhance their ability to detect and respond to emerging threats more quickly and effectively. Such cooperation not only reduces operational costs but also strengthens overall resilience against common adversaries. Despite the recognized advantages of information sharing, practical implementation presents several challenges, including concerns related to data confidentiality, trust, and coordination among participating entities [4].

2. LITERATURE SURVEY

Received: 28-02-2026 | Accepted: 02-04-2026 | Published: 10-04-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

Alzahrani et al. [5] proposed a practical implementation of CTI within the Arab region by integrating IoC collection from multiple sources, including security alerts generated through honeypot systems and OSINT. The collected intelligence is stored and managed using MISP, which is an open-source platform specifically designed for creating, sharing, and correlating IoCs. The study emphasized that MISP provides an intuitive interface that supports efficient data analysis, enables accurate threat identification, and facilitates correlation among IoCs, thereby improving the effectiveness of cyber threat detection and analysis. van Haastrecht et al. [6] addressed the challenge of utilizing shared CTI effectively by conducting a systematic review to identify state-of-the-art approaches in this domain. Their study revealed that threat intelligence sharing platforms such as MISP have the capability to meet the requirements of SMEs, provided that the shared intelligence is converted into actionable insights. Based on this observation, they developed a prototype application that automatically processes MISP data, prioritizes cybersecurity threats for SMEs, and provides tailored recommendations based on organizational context. Furthermore, they highlighted that future evaluations in operational environments are necessary to enhance the application and enable SMEs to effectively defend against cyberattacks. Saeed et al. [7] followed a systematic review methodology that involved selecting primary studies based on predefined criteria and conducting a quality assessment of the selected research. As a result of this analysis, they proposed a comprehensive framework for implementing CTI in organizations. The framework consists of multiple components, including a knowledge base for storing intelligence, detection models for identifying threats, and visualization dashboards for presenting insights. The detection layer incorporates behavior-based, signature-based, and anomaly-based detection techniques, ensuring a multi-layered approach to cyber threat detection. Sakellariou et al. [8] focused on the utilization of discussion forums as a source of raw data for CTI processes. Their study analyzed the characteristics of discussion forums and examined their relationship with CTI. They proposed a semantic schema for representing the collected data and applied a systematic methodology to design the SECDFAN reference architecture. This architecture supports the complete CTI lifecycle, including source selection, data extraction, intelligence generation, product sharing, and collaboration among cybersecurity experts. The final outcome of their work is the SECDFAN reference architecture, which enables structured and collaborative CTI generation.

Venckauskas et al. [9] proposed an automated method for assessing CTI data quality by evaluating both the content of the intelligence and the confidence levels of CTI providers. They introduced new quality dimensions to address the requirements of both technical and tactical CTI levels. Their approach utilizes structured data in STIX 2.1 format and includes visualization mechanisms to simplify the interpretation of quality assessment results. Extensive experiments conducted on real datasets demonstrated that their method can efficiently and quantitatively evaluate CTI data quality. Mendez et al. [10] implemented a PoC system aimed at enhancing the security of ISPs, home networks, and home-based IoT devices using blockchain technology. Their approach leverages decentralization to ensure data integrity, improve transparency, and strengthen security across distributed network environments. Pahlevan et al. [11] highlighted that although existing systems facilitate data exchange between different platforms, they fail to address key challenges such as trust, privacy, interoperability, and automation within a single solution. To overcome these limitations, they proposed a secure and efficient CTI sharing system that leverages the TAXII standard along with private blockchain technology. This approach automates the threat sharing process while ensuring privacy, maintaining data integrity, and supporting interoperability across different systems. Demirol et al. [12] proposed an innovative CTI analysis approach by integrating knowledge graphs

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

with a fine-tuned BERT-based model. Their system extracts cyber entities such as threat actors, malware, campaigns, and targets from unstructured threat reports and establishes relationships among these entities using an ontology-driven framework. They also created a dataset for named entity recognition and trained the BERT-based model accordingly. To address class imbalance, they applied oversampling techniques and a focal loss function, achieving an F1-score of 96%, which demonstrates the effectiveness of their approach.

El Amin et al. [13] analyzed existing risk management and threat intelligence frameworks and emphasized the necessity of integrating CTI into cyber risk management processes. Based on this analysis, they proposed a novel risk management framework that incorporates CTI on top of the EBIOS Risk Manager model, thereby enhancing risk assessment and improving organizational decision-making capabilities. Ali et al. [14] proposed that applying CTI technologies is essential for enhancing organizational security and automation. Their work emphasized the importance of detecting, classifying, analyzing, and sharing new cyberattack techniques. They suggested that trusted partner organizations can share newly identified threats to strengthen collective defense mechanisms. Their proposed solution utilizes blockchain smart contracts along with IPFS to enable secure sharing of both historical and real-time cybersecurity data, thereby improving system reliability, automation, and data quality. Cha et al. [15] proposed a blockchain-based CTI system architecture aimed at achieving sustainable computing by addressing challenges such as reliability, privacy, scalability, and sustainability. Their system integrates multiple CTI data feeds, generates reliable datasets, reduces network load, and introduces mechanisms to measure organizational contributions in order to encourage participation. Experimental evaluation using IP data from 10 OSINT-based CTI feeds demonstrated that the proposed model reduces storage consumption by approximately 15% compared to total network resources in a controlled environment.

3. PROPOSED METHODOLOGY

The proposed system architecture as illustrated in Figure 2 is designed as a layered web-based framework that integrates user interaction, backend processing, threat intelligence, and data analytics into a unified platform. It operates on the Django framework, which efficiently handles incoming HTTP requests, maps them to appropriate views, and dynamically renders templates for both admin and employee interfaces. The architecture follows a modular approach where authentication, domain validation, threat classification, data storage, and visualization are structured as interconnected components to ensure scalability, flexibility, and maintainability. A MySQL database, accessed through PyMySQL, is used to store employee credentials and threat activity logs in a structured and reliable manner. When a user submits a domain, the system processes the input by resolving it into an IP address using socket-based domain resolution techniques. The resolved IP address is then validated using IP verification methods to ensure correctness and eliminate malformed or invalid inputs before further processing.

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

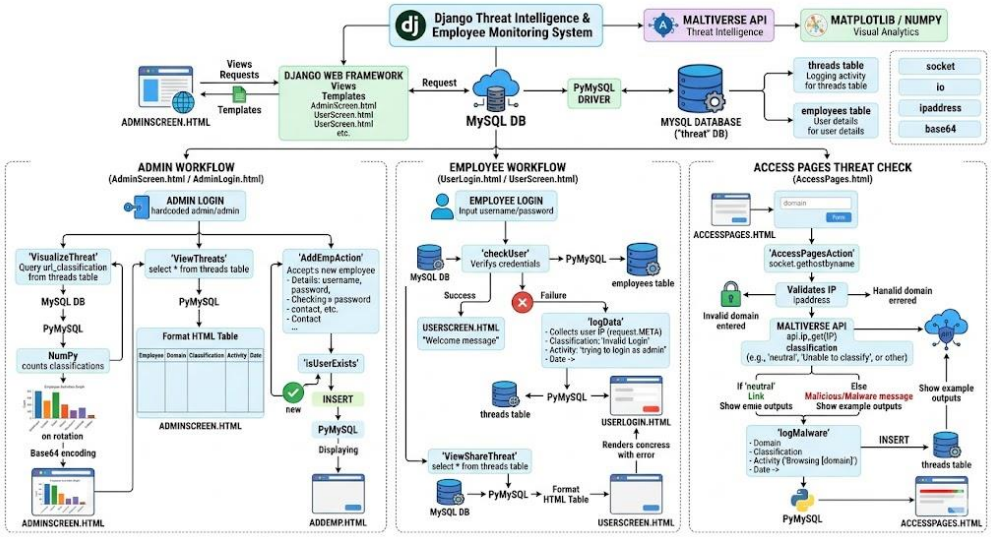


Figure 2: System architecture for threat intelligence sharing platform.

Once validated, the IP address is forwarded to the Maltiverse API, which performs real-time threat intelligence analysis based on IP reputation data. Based on the response received, the system classifies the domain as safe, neutral, or malicious and prepares the result for user display. The system also incorporates robust authentication and access control mechanisms that verify user credentials against stored records and grant role-based access to dashboards. Any failed login attempts are recorded and treated as suspicious activities for monitoring and security analysis. All user interactions, including login events and domain access checks, are logged with timestamps in the database to maintain traceability and support auditing processes. The logging system further helps in identifying behavioral patterns and detecting repeated malicious attempts. Additionally, the architecture includes a data analytics layer where NumPy is utilized for aggregating and analyzing threat-related data efficiently. For visualization, Matplotlib is used to generate graphical insights such as bar charts, which are encoded and displayed on the admin dashboard. These visual representations enable administrators to monitor threat trends and make informed security decisions. The architecture ensures seamless interaction between system components, supports real-time threat detection, enhances data-driven decision-making, and maintains high levels of security and performance.

4. Results description

Figure 3 illustrates the add new employee screen, representing the process of onboarding users into the threat intelligence sharing environment. It depicts how employee information is registered to enable participation in monitoring and secure access workflows. The figure reflects the role of structured employee management in maintaining controlled system access. It demonstrates how administrative inputs contribute to maintaining accurate user records for monitoring purposes.

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

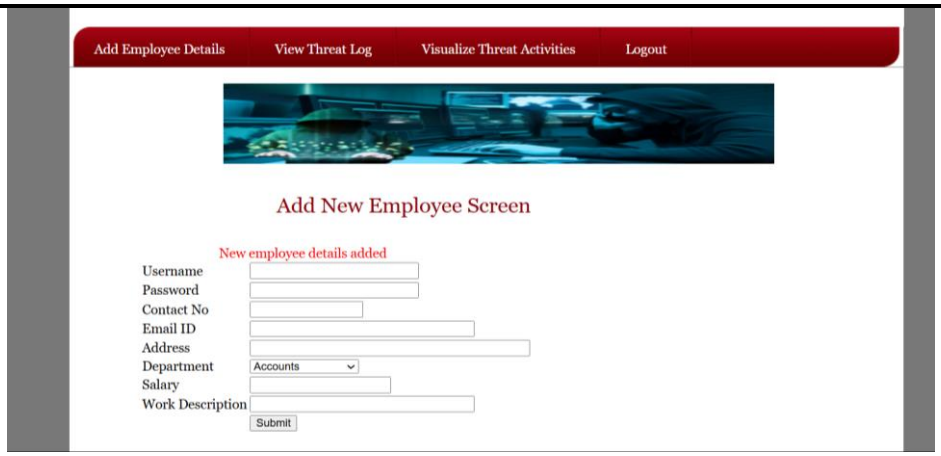


Figure 3: Added new employee screen

Figure 4 illustrates the employee login page, representing the stage where authenticated users successfully enter the system environment after validation. It depicts the transition from authentication to authorized access within the threat intelligence sharing framework. The figure reflects the establishment of user sessions that enable monitoring and activity tracking. It demonstrates how successful authentication allows employees to interact with system resources under security controls.

Figure 5 depicts the employee access web resources screen, representing how users interact with monitored web domains within the platform. It illustrates the evaluation and classification of accessed domains as part of threat monitoring procedures. The figure reflects how browsing activities are analysed to identify potential risks or safe interactions. It demonstrates the system's capability to monitor employee actions while maintaining awareness of security policies.

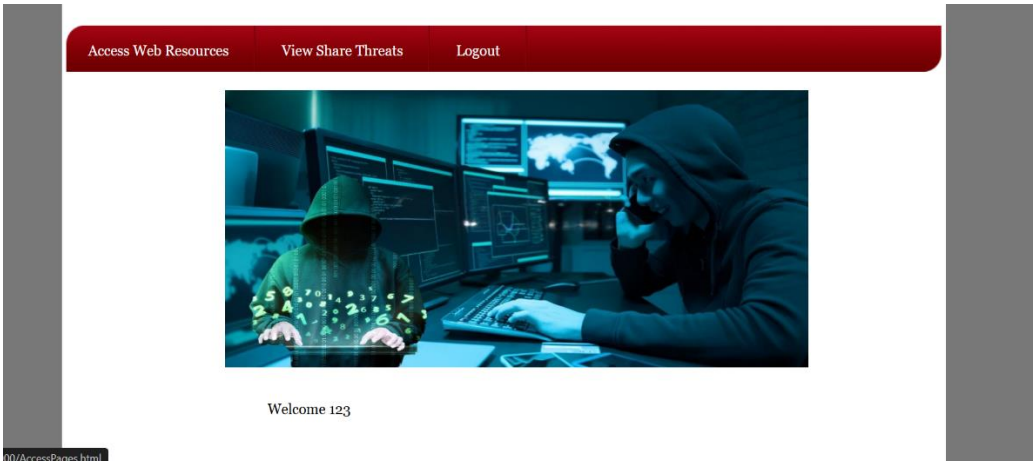


Figure 4: Employee login page

Received: 28-02-2026 | Accepted: 02-04-2026 | Published: 10-04-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

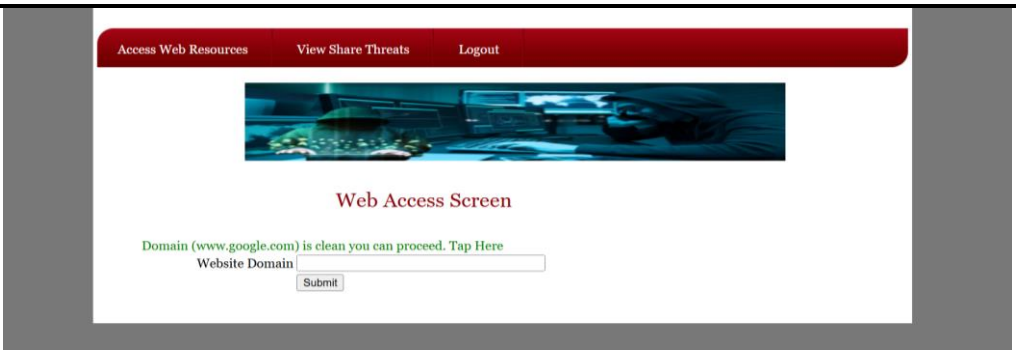


Figure 5: Employee access web resources

Figure 6 illustrates the view share threats screen, representing the interface where employees or administrators review shared threat information. It depicts how intelligence related to suspicious activities or malicious domains is made accessible within the platform. The figure reflects collaborative intelligence sharing that supports improved organizational awareness. It demonstrates how collected threat data contributes to informed decision-making.

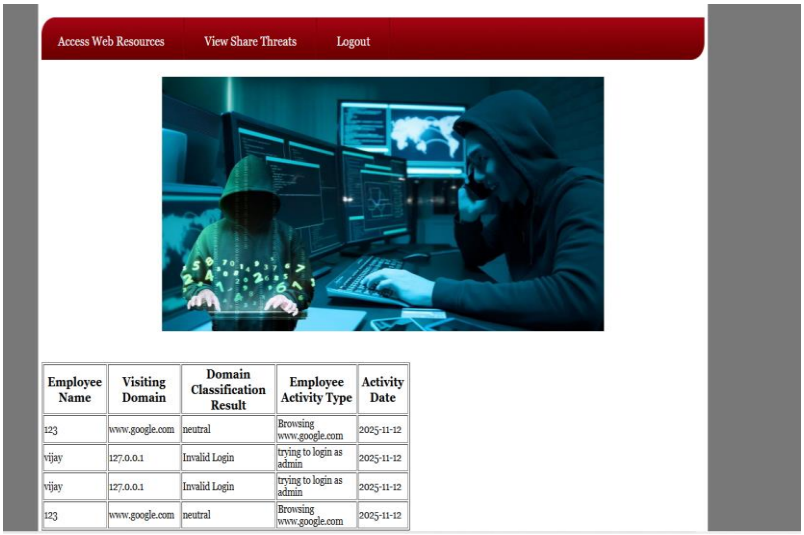
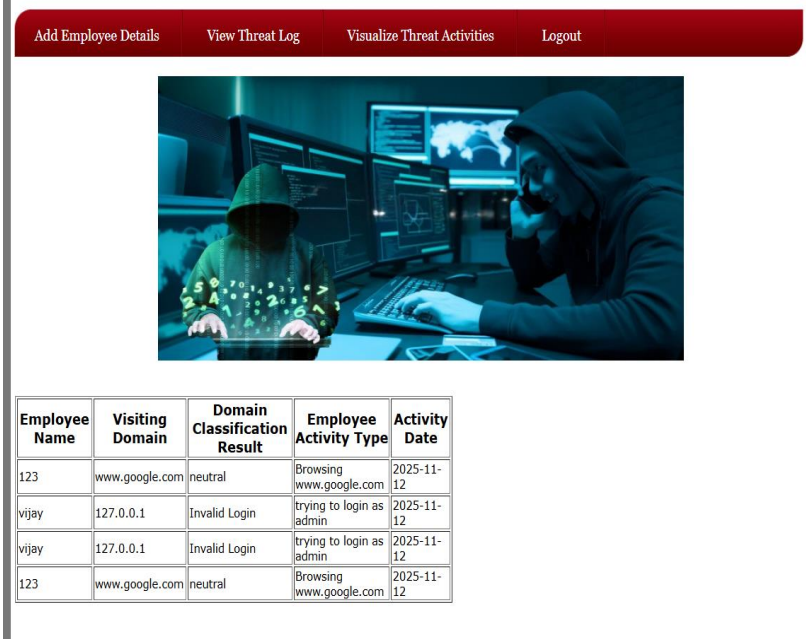


Figure 6: View share threats screen

Figure 7 depicts the admin view threat log screen, representing the detailed record of monitored activities and identified events within the system. It illustrates how activity data such as domain access and classification results are presented for analysis. The figure reflects the importance of maintaining historical logs to support investigation and auditing processes. It demonstrates how administrators track patterns and detect anomalies through structured records.

Figure 8 illustrates the admin visualize threat activities screen, representing graphical analysis of employee behavior and detected threats. It depicts how activity data is transformed into visual representations to improve understanding of trends and patterns. The figure reflects the use of data visualization to support faster decision-making and risk assessment. It demonstrates how graphical insights assist administrators in identifying unusual behaviors or potential security incidents.

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper



Employee Name	Visiting Domain	Domain Classification Result	Employee Activity Type	Activity Date
123	www.google.com	neutral	Browsing www.google.com	2025-11-12
vijay	127.0.0.1	Invalid Login	trying to login as admin	2025-11-12
vijay	127.0.0.1	Invalid Login	trying to login as admin	2025-11-12
123	www.google.com	neutral	Browsing www.google.com	2025-11-12

Figure 7: Admin view threat log screen

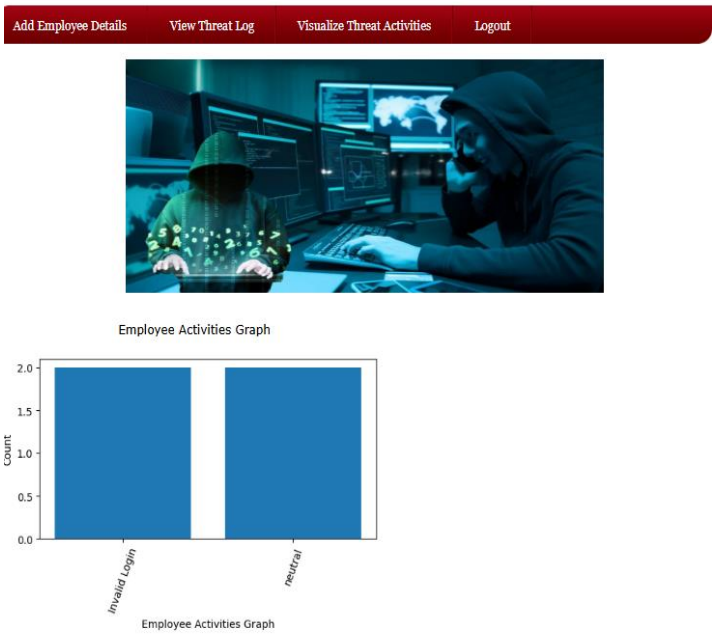


Figure 8: admin visualize threat activities

5. CONCLUSION

This research presents an effective approach for monitoring and sharing web-based threats by addressing the shortcomings of conventional security mechanisms that primarily react after an attack occurs. It actively tracks employee browsing behavior and evaluates accessed domains using integrated threat intelligence, enabling timely identification of potentially harmful or suspicious activities within the network. All events are systematically recorded in a centralized database, ensuring reliable storage, traceability, and ease of auditing for security analysis. The use of the

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

Django framework along with a MySQL database provides a stable and scalable infrastructure capable of handling real-time requests and data operations efficiently. The system also incorporates graphical representations of threat data, allowing administrators to quickly interpret patterns, detect anomalies, and make informed decisions. Furthermore, the controlled sharing of threat information among authorized users enhances collective awareness and supports faster response to emerging risks. By combining automated domain evaluation, structured data management, visual analytics, and collaborative features, the system significantly improves proactive security measures. It minimizes the chances of insider threats and strengthens defense against common web-based attacks such as malware distribution and phishing.

REFERENCES

[1] Collier, R. NHS ransomware attack spreads worldwide. Can. Med. Assoc. J. 2017, 189, E786–E787.

[2] Deep Instinct. 2021 Mid-Year Cyber Threat Landscape Report. Deep Instinct. 2021.

[3] Ponemon, L.; Bissell, K. Ninth Annual Cost of Cybercrime Study. Accenture. 2019.

[4] Siemens and Ponemon Institute. Siemens and Ponemon Institute Study Finds Utility Industry Vulnerabilities. Siemens. 2019.

[5] Alzahrani, I.Y.; Lee, S.; Kim, K. Enhancing Cyber-Threat Intelligence in the Arab World: Leveraging IoC and MISP Integration. Electronics 2024, 13, 2526. https://doi.org/10.3390/electronics13132526

[6] van Haastrecht, M.; Golpur, G.; Tzismadia, G.; Kab, R.; Priboi, C.; David, D.; Răcătăian, A.; Baumgartner, L.; Fricker, S.; Ruiz, J.F.; et al. A Shared Cyber Threat Intelligence Solution for SMEs. Electronics 2021, 10, 2913. https://doi.org/10.3390/electronics10232913

[7] Saeed, S.; Suayyid, S.A.; Al-Ghamdi, M.S.; Al-Muhaisen, H.; Almuhaideb, A.M. A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience. Sensors 2023, 23, 7273. https://doi.org/10.3390/s23167273

[8] Sakellariou, G.; Fouliras, P.; Mavridis, I. SECDFAN: A Cyber Threat Intelligence System for Discussion Forums Utilization. Eng 2023, 4, 615-634. https://doi.org/10.3390/eng4010037

[9] Venckauskas, A.; Jusas, V.; Barisas, D. Quality Dimensions for Automatic Assessment of Structured Cyber Threat Intelligence Data. Appl. Sci. 2025, 15, 4327. https://doi.org/10.3390/app15084327

[10] Mendez Mena, D.; Yang, B. Decentralized Actionable Cyber Threat Intelligence for Networks and the Internet of Things. IoT 2021, 2, 1-16. https://doi.org/10.3390/iot2010001

[11] Pahlevan, M.; Ionita, V. Secure and Efficient Exchange of Threat Information Using Blockchain Technology. Information 2022, 13, 463. https://doi.org/10.3390/info13100463

[12] Demirol, D.; Das, R.; Hanbay, D. A Novel Approach for Cyber Threat Analysis Systems Using BERT Model from Cyber Threat Intelligence Data. Symmetry 2025, 17, 587. https://doi.org/10.3390/sym17040587

[13] El Amin, H.; Samhat, A.E.; Chamoun, M.; Oueidat, L.; Feghali, A. An Integrated Approach to Cyber Risk Management with Cyber Threat Intelligence Framework to Secure Critical Infrastructure. J. Cybersecur. Priv. 2024, 4, 357-381. https://doi.org/10.3390/jcp4020018

[14] Ali, H.; Ahmad, J.; Jaroucheh, Z.; Papadopoulos, P.; Pitropakis, N.; Lo, O.; Abramson, W.; Buchanan, W.J. Trusted Threat Intelligence Sharing in Practice and Performance Benchmarking

through the Hyperledger Fabric Platform. Entropy 2022, 24, 1379. https://doi.org/10.3390/e24101379

[15] Cha, J.; Singh, S.K.; Pan, Y.; Park, J.H. Blockchain-Based Cyber Threat Intelligence System Architecture for Sustainable Computing. Sustainability 2020, 12, 6401. https://doi.org/10.3390/su12166401.