Real-Time Cyber Incident Tracker

MR.NOORAHAMED J M.C.A., M.Phil

Assistant professor(SG), Department of Computer Applications,
Nehru College of Management, Coimbatore,
Tamilnadu, India
jnamca@gmail.com

CLEMENTSIJO L

II MCADepartment of Computer Applications,
NehruCollege of Management, Coimbatore,
Tamilnadu,India
clementsijo@gmail.com

ABSTRACT

Cyber threats are becoming more frequent and complicated, putting people and businesses at serious danger all around the world. It is difficult for traditional security monitoring systems to offer real-time insights into new dangers. In order to depict worldwide cyber occurrences, this project suggests a Real-Time Cyber Incident Tracker that makes use of the MERN (MongoDB, Express.js, React.js, Node.js) stack, Leaflet.js, Socket.io, and external Threat Intelligence APIs. The system retrieves, analyzes, and presents real-time cyberattack data on an interactive global map. Through interactive charts and reports, users can keep an eye on malware varieties, impacted regions, and attack trends. By offering historical data analysis, real-time threat updates, and an admin interface for manual incident tracking, the suggested system improves cyber awareness.

Keywords: Live Attack Map, Data Analytics, Malware Tracking, Rate Limiting, Real-Time Threat Tracking, and Incident Reporting

INTRODUCTION

Cyber risks have increased globally as a result of the rise of digital transformation. Cybercriminals target businesses, financial institutions, and vital infrastructure using sophisticated assault methods. Cybersecurity teams find it difficult to identify and eliminate attacks in the absence of real-time monitoring and immediate threat intelligence. Conventional security systems are less successful in stopping changing cyberthreats because they concentrate on post-attack analysis.
The Real-Time Cyber Incident Tracker, a cutting-edge web-based tool that continually monitors, tracks, and visualizes cyber occurrences worldwide, is introduced in this project. The

solution offers real-time updates, data filtering, and analytics to improve cybersecurity monitoring by utilizing Threat Intelligence APIs, WebSockets, and interactive geospatial visualization. This platform allows enterprises and security experts to proactively respond to cyber attacks, evaluate attack trends, and find vulnerabilities.

Key features:

1. Real-Time Cyber Threat Map: This interactive global map displays real-time cyber occurrences using Leaflet.js.
2. WebSocket-Based Live Updates: Uses Socket.io to deliver attack data in real time.
3. Integration of Threat Intelligence APIs: Gathers international cyberthreats from outside sources.
4. Using role-based access and JWT-based authentication, user authentication provides secure access.
5. Authorized users can manually log and manage incidents using the Admin Panel.
6. Security & Rate Limiting Middleware: Guards against misuse and illegal access.
7. Data Storage & Analytics: Stores previous attack data for trend analysis and analytics using MongoDB.
8. Responsive UI: Tailwind CSS was used to create a streamlined, mobile-friendly interface.

METHODOLOGY

In order to guarantee effective real-time data processing and precise threat portrayal, the Real-Time Cyber Incident Tracker was developed using a modular and structured methodology, integrating essential technologies and security measures. The following are included in the methodology:

1. Gathering data:
   - obtaining real-time cyber threat intelligence from outside APIs.
   - Determining the type, target, virus, attack source, and industries impacted.
2. Processing and Storing Data
   - For accuracy, removing redundant and out-of-date data.
   - Keeping track of cyber occurrences for later investigation in a MongoDB database.
3. Real-Time Data Streaming:
   - WebSockets (Socket.io) are used to provide users with real-time attack updates.
   - Making it possible to track in real time without refreshing the website.
4. Visualization of Cyber Threats:
   - Using Leaflet.js to show assault sites on an interactive global map.
   - Using assault path animation to show the movements of cyberwarfare in real time.
5. Role management and user authentication:
   - Using JWT-based authentication to provide safe user access.
   - Granting administrator access for system administration and manual threat logging.

6. Analytics & Data Filtering
    - Offering location, attack type, and severity filtering options that can be customized.
    - Visualizing attack trends and statistics with Chart.js and Recharts.
7. Optimization & Security
    - Rate restriction is being used to stop excessive API queries.
    - Improving system dependability through the use of error handling middleware.

MODULES

The several components that make up the Real-Time Cyber Incident Tracker each carry out distinct tasks to improve system functionality and performance:

1. Module for User Authentication
    - Role-based access and login combined with secure JWT-based authentication.
    - Prevents unauthorized users from taking sensitive system actions.
2. Real-Time Cyber Threat Visualization
    - It shows real-time cyberattacks on an interactive global map.
    - To dynamically depict cyberattacks, animated attack pathways are used.
3. WebSocket Communication Module:
    - This module streams cyber threat data in real time via Socket.io.
    - Guarantees that users get real-time updates without having to reload the website.
4. Data Fetching & Storage:
    - It retrieves real-time cyber threat intelligence from APIs.
    - Uses MongoDB to store past attack data for analysis.
5. Admin Panel Module:
    - Enables manual cyber incident management and logging.
    - Facilitates the search, filtering, and editing of historical data.
6. The Analytics & Reporting Module
    - It creates assault trend graphs using Chart.js and Recharts.
    - Shows the most often attacked areas, malware kinds, and attack frequencies.
7. Security & Rate Limiting Module:
    - Prevents excessive requests by implementing API rate limiting.
    - To improve system stability, error handling middleware is

LITERATURE REVIEW

Modern digital defense depends on cybersecurity threat intelligence, which enables businesses to monitor and assess cyber occurrences instantly. Although they offer a wealth of threat knowledge, traditional platforms such as IBM X-Force and Check Point Threat Map are frequently costly and lack dynamic filtering and real-time interaction. Real-time data streaming has been enhanced by recent developments in WebSockets, which allow for immediate cyber threat tracking and faster reaction times. Furthermore, interactive visualization tools such as Leaflet.js improve users' capacity to efficiently assess attack patterns. Many current systems lack the capability to manually log localized hazards for improved situational awareness, instead depending only on automated detection. While open-source cybersecurity programs try to fill these shortcomings, the majority don't have a thorough real-time tracking system that combines several data sources. An interactive cyberattack map, WebSockets for real-time updates, and Threat Intelligence APIs are all combined in the suggested Real-Time Cyber Incident Tracker to create an affordable, scalable, and engaging cybersecurity monitoring system. It is a vital resource for security experts, businesses, and academics since it fills the gap between easily accessible real-time tracking tools and enterprise-level intelligence platforms.

EXISTING SYSTEM Existing cybersecurity monitoring solutions are less successful at stopping new threats since they mostly concentrate on post-attack analysis and aggregated data representation. Although they offer enterprise-level threat intelligence, platforms such as Check Point Threat Map, IBM X-Force, and FireEye are expensive, inaccessible, and do not offer real-time interaction. Instead of using live data streaming, many systems rely on static dashboards that are updated periodically, which lessens their ability to mitigate threats in real time.

Security teams are also unable to track localized or organization-specific cyber incidents because the majority of current systems do not include human incident logging. For real-time updates, WebSockets are more efficient than HTTP polling, which is frequently used by traditional cybersecurity technologies. Organizations' capacity to properly assess and address cyberthreats is further restricted by the lack of interactive attack visualization and sophisticated filtering tools.

Key Points:

1. Absence of Real-Time Monitoring: Instead of tracking threats in real time, many systems rely on delayed data updates.
2. Limited Interactive Visualization: Attack maps frequently lack user engagement and are static.
3. No Live Data Streaming: Traditional HTTP polling, which is slower and less effective

than WebSockets, is used by the majority of platforms.

4. High Cost & Limited Accessibility: Smaller businesses and individual researchers may find it difficult to obtain enterprise solutions due to their high cost.
5. No Manual Incident Logging: Security teams' situational awareness is limited by the inability of current systems to log localized threats.
6. Absence of Data Filtering & Analytics: There aren't many ways to filter cyberthreats by nation, attack type, sector, or virus type.
7. Weak User Access Control: Role-based authentication is either nonexistent or very limited, which raises the possibility of unwanted access.

PROPOSED SYSTEM

A real-time, interactive, and data-driven cybersecurity monitoring system is what the Real-Time Cyber Incident Tracker is intended to offer. This system tracks, visualizes, and analyzes cyber risks as they occur, in contrast to standard cybersecurity solutions that concentrate on post-attack analysis. Instant updates, attack trend analysis, and proactive threat mitigation are made possible by combining Threat Intelligence APIs, WebSockets, and interactive geospatial visualization.

The proposed system offers the following key features:

Key Points:

1. Monitoring of Threats in Real Time uses WebSockets to display real-time cyber events with real-time updates.
2. . Interactive Cyber Attack Map: This dynamic visualization of attack origins, destinations, and trends makes use of Leaflet.js.
3. Integration of Threat Intelligence API retrieves current cyber threat information from outside threat intelligence sources that use artificial intelligence.
4. Real-time Data Transmission replaces conventional HTTP polling with WebSockets (Socket.io) for real-time updates.
5. Incident Logging & Manual Reporting: This feature enables security analysts to manually record and monitor localized cyber occurrences.
6. . Analytics & Data Filtering offers filters according on malware categories, industry, attack type, and country.
7. Access Based on Roles and User Authentication
   guarantees safe access control for various user roles (viewer, analyst, and administrator).
8. Data Visualization & Charts displays attack trends, top-targeted nations, and malware kinds using Chart.js or Recharts.
9. Tailwind CSS was used in the design of the scalable and responsive user interface to provide a completely responsive and intuitive experience

CONCLUSION

For keeping an eye on worldwide cyberthreats, the Real-Time Cybersecurity Incident Tracker provides a strong and expandable solution. This solution improves cybersecurity awareness and reaction capabilities by utilizing WebSockets, real-time APIs, and interactive visualization. It is a useful tool for cybersecurity experts and businesses since it combines analytics, live threat mapping, and automated data fetching. Deeper integration with security frameworks and AI-based threat prediction models are possible future improvements.

REFERENCES

1. Stouffer, K., Lightman, S., Abrams, M., & Hahn, A. (2015). *Guide to Industrial Control Systems (ICS) Security (NIST Special Publication 800-82)*. National Institute of Standards and Technology.
2. Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice.* Pearson Education.
3. Check Point Threat Intelligence. (2024). *Cyber Threat Map.* Retrieved from https://threatmap.checkpoint.com
4. Open Web Application Security Project (OWASP). (2024). *Web Security Standards.* Retrieved from https://owasp.org
5. Rajaraman, V. (2018). *Fundamentals of Cyber Security.* McGraw-Hill Education.
6. YouTube. (2023). Web Development Tutorials. Retrieved from YouTube
7. OpenAI. (2023). ChatGPT. Retrieved from OpenAI