
Enterprise Threat Detection

Shagufta Rahil¹, Dr.Asharani Patil²

¹M. Tech Student Dept of DCN at Sharnabasva University Kalaburagi Email: syedshagufarahil@gmail.com

²Prof. Faculty of Engineering & Technology (Exclusively for Women), Sharnabasva University Kalaburagi

Email: asharanispatil@gmail.com

DOI: <https://doi.org/10.5281/zenodo.23000629>

ABSTRACT

Enterprise environments are increasingly exposed to sophisticated cyber threats such as ransomware, phishing attacks, insider threats, Advanced Persistent Threats (APTs), and zero-day vulnerabilities. Conventional signature-based security mechanisms are often inadequate for identifying newly emerging or previously unknown attacks in real time. To address these challenges, this paper proposes an intelligent enterprise threat detection framework that combines machine learning techniques with Security Information and Event Management (SIEM), User and Entity Behavior Analytics (UEBA), and cyber threat intelligence. By correlating data from multiple security sources and analyzing behavioral patterns, the proposed framework enhances threat detection capabilities and improves classification accuracy. Experimental results indicate that the system effectively minimizes false-positive alerts, accelerates threat identification, and strengthens the overall cybersecurity posture of enterprise networks.

Keywords: Enterprise Security, Threat Detection, Artificial Intelligence, Machine Learning, SIEM, UEBA, Intrusion Detection, Cybersecurity.

I. INTRODUCTION

Enterprise Threat Detection has emerged as a critical area of cybersecurity as organizations continue to experience increasingly sophisticated and persistent cyberattacks. Conventional security solutions, including firewalls and signature-based Intrusion Detection Systems (IDS), are primarily designed to identify known attack patterns and often struggle to recognize new or evolving threats. Advanced cyberattacks such as ransomware, Advanced Persistent Threats (APTs), insider attacks, and zero-day vulnerabilities require intelligent detection techniques that leverage Artificial Intelligence (AI), Machine Learning (ML), behavioral analytics, and threat intelligence. Recent studies have focused on developing advanced detection frameworks that improve threat identification accuracy, minimize false-positive alerts, and enable rapid, real-time incident detection and response.

II. LITERATURE SURVEY

Enterprise Threat Detection has evolved significantly over the past few decades, driven by the increasing complexity of cyber threats and the need for proactive security mechanisms. Researchers have proposed various models, frameworks, and intelligent detection techniques to improve the identification and mitigation of cyberattacks.

Denning (1987) introduced one of the earliest and most influential intrusion detection models, establishing the theoretical foundation for modern Intrusion Detection Systems (IDS). The study proposed monitoring system activities through audit records and identifying abnormal behavior by comparing user activities against predefined security profiles. This pioneering work demonstrated that abnormal system behavior could be effectively used to detect unauthorized access and malicious activities, laying the groundwork for both signature-based and anomaly-based detection systems.

Scarfone and Mell (2007) provided a comprehensive guide to Intrusion Detection and Prevention Systems (IDPS) published by the National Institute of Standards and Technology (NIST). The guide describes the architecture, deployment strategies, operational requirements, and management of IDPS in enterprise environments. It highlights the differences between network-based and host-based intrusion detection systems and emphasizes the importance of integrating prevention capabilities with detection mechanisms. The publication remains an important reference for implementing effective enterprise security infrastructures.

Chandola, Banerjee, and Kumar (2009) presented a detailed survey of anomaly detection techniques across multiple domains. The authors classified anomaly detection methods into statistical, distance-based, density-based, clustering, classification, and information-theoretic approaches. Their research demonstrated that anomaly detection plays a crucial role in identifying previously unseen attacks that cannot be detected using traditional signature-based methods. The survey also discussed the challenges associated with high-dimensional data, evolving attack patterns, and evaluation metrics for anomaly detection algorithms.

Sommer and Paxson (2010) critically examined the application of machine learning techniques in network intrusion detection. While machine learning offers promising capabilities for identifying complex attack patterns, the authors argued that real-world deployment presents significant challenges, including feature engineering, data quality, model interpretability, and high false positive rates. They emphasized that machine learning should complement rather than replace traditional security mechanisms and recommended combining automated detection with expert human analysis to improve overall effectiveness.

Buczak and Guven (2016) conducted a comprehensive survey of data mining and machine learning methods used in cybersecurity intrusion detection. Their review covered supervised, unsupervised, and semi-supervised learning algorithms, including Decision Trees, Support Vector Machines, Artificial Neural Networks, Naïve Bayes, Random Forests, and clustering techniques. The authors concluded that machine learning significantly enhances intrusion detection accuracy when combined with feature selection, threat intelligence, and real-time data analysis. They also highlighted the growing importance of big data analytics and artificial intelligence in addressing sophisticated and evolving cyber threats.

III. PROPOSED METHODOLOGY

The proposed **Enterprise Threat Detection (ETD)** system uses an Artificial Intelligence (AI)-based architecture to monitor enterprise network traffic, identify cyber threats, classify their severity, and generate

alerts for security administrators. The system integrates **network monitoring, machine learning, behavioral analysis, and reporting** to provide real-time protection against cyber attacks.

The methodology consists of seven major phases:

Step 1: Data Collection

Security-related information is continuously collected from enterprise endpoints such as:

- Firewalls
- Routers
- Servers
- Workstations
- Network switches
- Cloud services

The collected data includes:

- Network packets
- System logs
- Authentication logs
- DNS records
- Web traffic
- User activities

Step 2: Data Pre-processing

The raw data undergoes preprocessing before analysis.

Tasks include:

- Data cleaning
- Removing duplicate records
- Handling missing values
- Feature extraction
- Feature normalization

The processed data is stored in a SQL/NoSQL database for further analysis.

Step 3: Threat Detection Engine

The detection engine analyzes incoming data using multiple techniques.

Signature-Based Detection

Matches known attack signatures such as:

- Malware
- Virus
- Worms
- Ransomware

Anomaly-Based Detection Uses machine learning to detect abnormal behaviors such as:

- Insider attacks
- Zero-day attacks
- Data exfiltration
- Unauthorized access

Step 4: Machine Learning Classification

The extracted features are processed using supervised learning algorithms such as:

- Random Forest
- Support Vector Machine (SVM)
- XGBoost
- Decision Tree
- Artificial Neural Network (ANN)
- Long Short-Term Memory (LSTM)

The trained model classifies traffic as:

- Normal
- Suspicious
- Malicious

Step 5: Threat Severity Analysis

- Low
- Medium
- High
- Critical

Severity is calculated based on:

- Attack type
- Impact
- Frequency
- Asset value
- Threat intelligence

Step 6: Alert Generation

When malicious activity is detected, the system generates:

- Email notifications
- Dashboard alerts
- Incident reports
- Security logs

Alerts are forwarded to the Security Operations Center (SOC) for immediate response.

Step 7: Reporting and Visualization

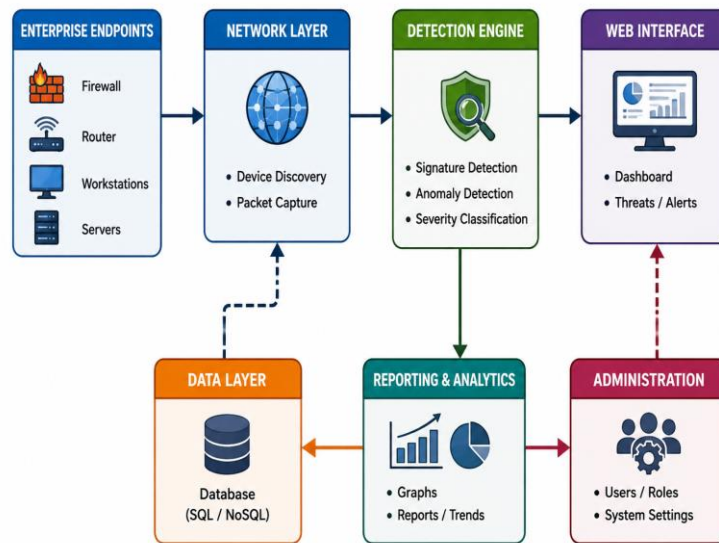
The reporting module generates:

- Threat statistics
- Attack trends
- Network health reports
- User activity reports
- Security dashboards

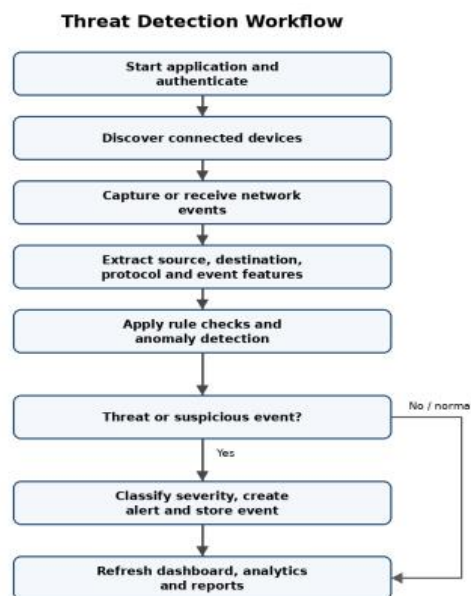
These reports help administrators monitor enterprise security and support informed decision-making.

IV. SYSTEM ARCHITECTURE

ENTERPRISE THREAT DETECTION - SYSTEM ARCHITECTURE



Work flow



ADVANTAGES

- Early attack detection
- Reduced false alarms
- Faster incident response

- Scalable architecture
- Cloud compatibility
- Supports Zero Trust

LIMITATIONS

- Large training dataset required
- High computational cost
- Concept drift
- Encrypted traffic challenges

OUTCOMES

The implementation of enterprise threat detection provides the following overall benefits:

- Early identification of cyberattacks.
- Higher detection accuracy using AI and machine learning.
- Reduced false-positive alerts.
- Real-time monitoring of enterprise environments.
- Faster incident detection and response.
- Protection against sophisticated and zero-day attacks.
- Improved visibility across enterprise networks.
- Enhanced compliance with cybersecurity standards.
- Better utilization of threat intelligence.
- Increased business continuity and organizational resilience.

CONCLUSION

Enterprise Threat Detection plays a vital role in strengthening modern cybersecurity by enabling organizations to identify, analyze, and respond to cyber threats in a proactive manner. The integration of Artificial Intelligence (AI), Machine Learning (ML), behavioral analytics, threat intelligence, and automated response techniques significantly enhances the ability to detect both known and emerging attacks. These advanced technologies improve the efficiency of security operations, reduce false-positive alerts, and shorten

incident response times. Consequently, organizations can achieve a stronger security posture, enhance operational resilience, and better protect critical assets against the continuously evolving cyber threat landscape.

REFERENCES

1. Denning, D. E. (1987). *An Intrusion-Detection Model*. IEEE Transactions on Software Engineering, 13(2), 222–232.
2. Scarfone, K., & Mell, P. (2007). *Guide to Intrusion Detection and Prevention Systems (IDPS)*. NIST Special Publication 800-94.
3. Chandola, V., Banerjee, A., & Kumar, V. (2009). *Anomaly Detection: A Survey*. ACM Computing Surveys, 41(3), Article 15.
4. Sommer, R., & Paxson, V. (2010). *Outside the Closed World: On Using Machine Learning for Network Intrusion Detection*. Proceedings of the IEEE Symposium on Security and Privacy, 305–316.
5. Buczak, A. L., & Guven, E. (2016). *A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection*. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176.
6. Ring, M., Wunderlich, S., Scheuring, D., Landes, D., & Hotho, A. (2019). *A Survey of Network-based Intrusion Detection Data Sets*. Computers & Security, 86, 147–167.
7. National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. NIST CSWP 29.
8. Stallings, W. (2017). *Network Security Essentials: Applications and Standards* (6th ed.). Pearson.
9. Kurose, J. F., & Ross, K. W. (2021). *Computer Networking: A Top-Down Approach* (8th ed.). Pearson.