IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 11, November 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.625

© 2024 IJIRCCE | Volume 12, Issue 11, November 2024| DOI: 10.15680/IJIRCCE.2024.1211026

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Enhancing Threat Detection and Incident Response

A .Suraj Kumar[1], Ch.Deepika[2], M.SaiKrishna[3], T.SaiBhavani[4], V.Rakesh[5], V.PavanSriram[6]

Assistant Professor, Department of CSE (Data Science), NSRIT, Visakhapatnam, India[1]

Student, Department of CSE(Data Science), NSRIT ,Visakhapatnam, India[2,3,4,5,6]

ABSTRACT: In the evolving landscape of cyber security, the effectiveness of threat detection and incident response is critical for safeguarding organizational assets and data. This paper addresses the limitations of current threat detection systems and incident response protocols by proposing a novel framework that integrates advanced machine learning techniques and automated response mechanisms. We introduce an enhanced threat detection model that leverages real-time data analytics and behavioural analysis to improve accuracy and reduce false positives. Additionally, our incident response system employs orchestration and automation to streamline and accelerate response times. Through a comprehensive evaluation involving simulated cyber-attacks and real-world case studies, we demonstrate significant improvements in detection rates and response efficiency. Our findings highlight the potential for these advanced methods to transform cyber security practices, offering actionable insights and practical recommendations for implementing these enhancements in diverse organizational environments.

KEYWORDS: Cyber security, Threat detection, Behavioural analysis, Incident Response, Machine Learning, Data Analytics, Digital Forensics

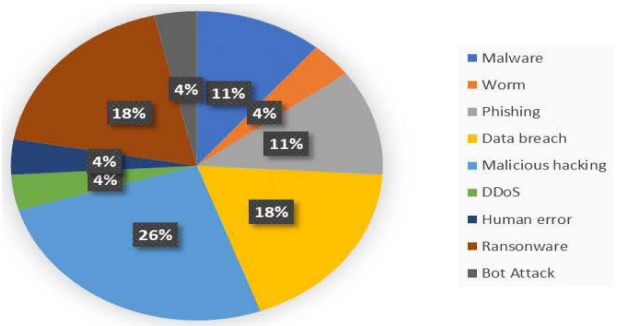
I. INTRODUCTION

In today's digital era, organizations are increasingly vulnerable to advanced and fast-evolving cyber threats that exploit complex vulnerabilities. As cyberattacks become more sophisticated, it is crucial for organizations to implement effective cybersecurity measures to mitigate risks. At the core of these measures are two critical components: **threat detection** and **incident response**.

Threat detection focuses on identifying potential security breaches or malicious activities within a system or network. Traditional methods, such as **signature-based detection** and **static rule sets**, are often inadequate in addressing modern threats, which evolve rapidly and can bypass these conventional defences. These methods also suffer from high false positive rates, overwhelming security teams with unnecessary alerts, and slow detection times, which delay the response to real threats.

Incident response, on the other hand, involves the steps taken to manage and mitigate the impact of a detected security incident. However, traditional response strategies rely heavily on manual, reactive measures, which can be slow and inefficient. The longer it takes to respond to an incident, the more potential damage occurs, including data breaches, financial losses, and reputational harm.

Types of cyber attacks



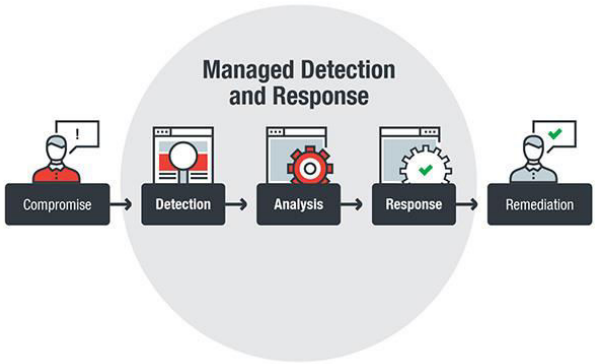
www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

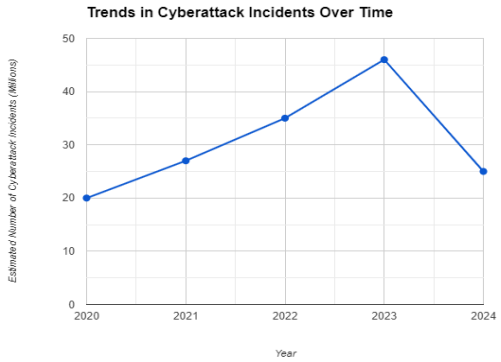
International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

To overcome these challenges, there is a growing need for more advanced and adaptive solutions that integrate modern technologies like **machine learning** and **automation**. Machine learning enables real-time analysis of vast data, identifying both known and unknown threats more accurately, while automated response systems ensure faster and more effective actions, minimizing the impact of incidents.

This paper introduces a novel approach that combines **machine learning-driven threat detection** with **automated incident response** to create a more efficient and proactive security framework. Through this integration, organizations can improve their ability to detect, respond to, and mitigate threats in real-time. The paper also evaluates the effectiveness of this framework through **empirical testing** and **case studies**, providing actionable insights for enhancing organizational cybersecurity against the constantly evolving threat landscape.





II. METHODOLOGY

To enhance threat detection and incident response, we propose a multi-faceted approach that integrates advanced machine learning techniques and automated response systems. Our methodology consists of the following key components:

1. Threat Detection Enhancement

1.1. Data Collection and Integration:

Sources: Aggregate data from diverse sources, including network traffic logs, system event logs, and threat intelligence feeds.

Pre-processing: Clean and pre-process data to ensure quality and consistency, handling missing values and normalizing data formats.

1.2. Machine Learning Model Development:

Feature Engineering: Extract relevant features from the pre-processed data that are indicative of potential threats, such as network anomalies and user behaviour patterns.

Model Selection: Develop and train machine learning models, including supervised (e.g., Random Forest, Support Vector Machines) and unsupervised (e.g., Anomaly Detection, Clustering) techniques.

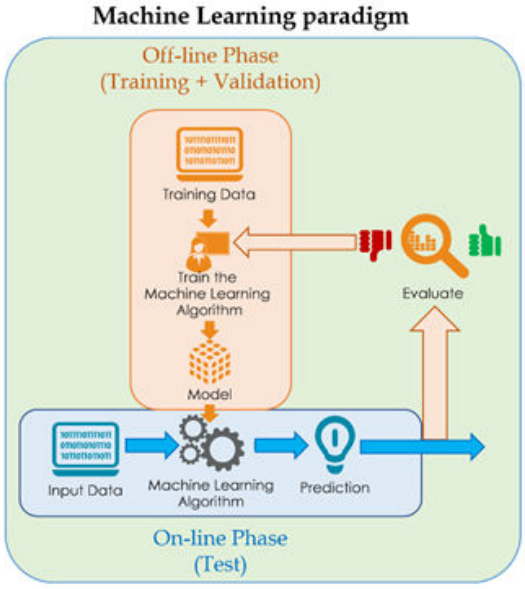
Training and Validation: Utilize historical attack data to train models and validate their performance using cross-validation techniques to prevent over-fitting and ensure generalizability.

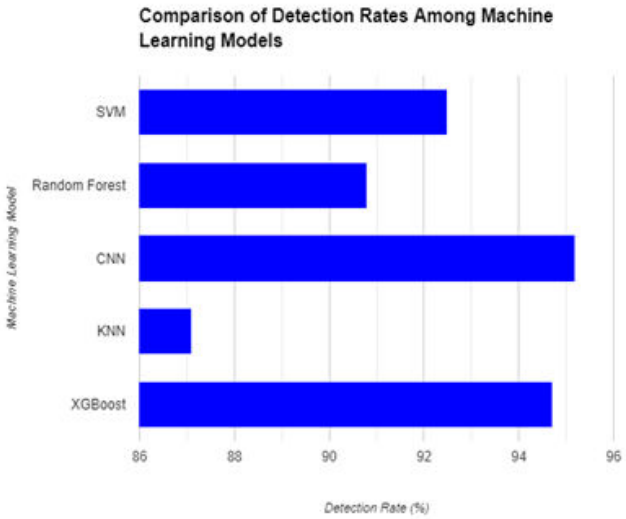
Evaluation Metrics: Assess model performance using metrics such as accuracy, precision, recall, and F1-score to evaluate detection capability and minimize false positives.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)





2. Incident Response Optimization

2.1. Automation and Orchestration:

Response Playbooks: Develop automated response playbooks that define specific actions to be taken based on detected threats, such as isolating affected systems or blocking malicious IP addresses.

Integration: Integrate automation tools with existing Security Information and Event Management (SIEM) systems to enable real-time orchestration of incident response actions.

2.2. Real-Time Incident Handling:

Alerting System: Implement a real-time alerting mechanism that triggers automated responses and notifies security personnel of critical incidents.

Dynamic Response: Use machine learning insights to adapt response strategies dynamically, based on the evolving nature of the threat and its impact.

3. Evaluation and Testing

3.1. Simulation and Testing:

Test Environment: Create a controlled test environment to simulate various cyber-attack scenarios and evaluate the performance of the enhanced detection and response system.

Metrics Assessment: Measure the system's effectiveness in detecting threats, reducing false positives, and responding to incidents, using metrics such as detection time, response time, and recovery time.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Evaluation and Testing Framework for Cybersecurity Systems

3.2. Case Studies:

3.2.1.Real-World Application:

Conduct case studies with selected organizations to apply the proposed framework in real-world scenarios. Collect feedback and performance data to assess the practical benefits and areas for improvement.

4.Analysis and Refinement

4.1.Data Analysis:

Analyse results from simulations and case studies to identify strengths and weaknesses of the proposed system.

4.2.Refinement:

Refine the machine learning models and automated response strategies based on feedback and performance data to enhance overall effectiveness.

Key Arguments

1. Need for a Holistic Approach

Organizations should adopt a comprehensive security framework that combines people, processes, and technology to enhance threat detection and incident response capabilities.

2. Continuous Improvement and Adaptation

Cyber threats evolve rapidly; organizations must continually assess and update their detection and response strategies. Regular training and simulations can prepare teams for real-world incidents and improve overall resilience.

3. Investment in Tools and Technologies

Allocating resources toward advanced detection tools (e.g., SIEM, EDR) is essential for maintaining an effective security posture.

Investment in skilled personnel and on-going education is equally critical to leverage these technologies effectively.

4. Importance of Incident Response Planning

Developing and regularly updating an incident response plan is crucial for minimizing damage during an attack.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Clear roles and communication protocols enhance coordination and effectiveness during incidents.

5. Legal and Compliance Considerations

Organizations must navigate various regulations regarding data protection and incident reporting, emphasizing the need for robust compliance strategies.

Scenario: Ransom ware Attack

Step 1: Threat Detection

1. Initial Alert:

- An employee reports encrypted files and a ransom note demanding, prompting an investigation.

2. **Security Monitoring:**

- The Security Operation Centre (SOC) receives alerts from endpoint detection tools about unusual file encryption across devices.
- Network analysis identifies abnormal outbound traffic to a known malicious IP.

3. User Reports:

- SOC reviews logs and finds multiple failed login attempts from an external IP, indicating a possible compromise.

Step 2: Incident Response

A. Containment

1. Isolate Systems:

- Affected systems are disconnected from the network to prevent further spread, and access to shared drives is restricted.

2. Block Malicious IPs:

- Firewalls are updated to block connections to the identified malicious IP.

B. Investigation

1. Forensic Analysis:

- The team analyses affected machines to find the entry point (e.g., phishing, vulnerabilities) and reviews the ransom note for clues.

2. Log Review:

- Security logs are examined for unauthorized access and unusual behaviour before the attack.

C. Eradication

1. Remove Ransom ware :

- The team employs decryption tools (if available) or wipes infected systems, restoring them from clean backups.

2. Patch Vulnerabilities:

- Any exploited vulnerabilities are patched, software is updated, and unnecessary services are disabled.

D. Recovery

1. Restore Data:

- Data is restored from backups, ensuring they are unaffected, and systems are reconfigured before reconnecting to the network.

2. Monitoring:

- Continuous monitoring is implemented to detect any signs of reinfection.

E. Post-Incident Review

1. Debriefing:

- The incident response team evaluates the response, identifying strengths and areas for improvement.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

2. Employee Training:
- Additional training sessions are held to educate employees on phishing and safe browsing.

3. Policy Updates:
- Security policies are revised based on lessons learned, including stricter access controls and multi-factor authentication.

4. Simulation Exercises:
- Regular drills are scheduled to prepare the team for future incidents.

III. CONCLUSION

This structured response illustrates how organizations can detect, contain, and eradicate ransom ware threats while enhancing future resilience. Each step is crucial for minimizing damage and ensuring a quicker recovery.

REFERENCES

1. SANS Institute(2018) Incident Handler's Handbook. Retrieved from [SANS website](https://www.sans.org/white-papers/37016/).
2. National Institute of Standards and Technology (NIST)(2018) Framework for Improving critical Infrastructure Cyber Security.Retrieved from [NIST wwebsite](https://www.nist.gov/cyberframework).
3. Symantec Corporation(2021) Internet Security Threat Report. Retrieved from [Symantecwebsite](https://www.broadcom.com/company/newsroom/ Press releases filter =2021).
4. Carson, S., & John, A(2019) Incident Response: A Strategic Guide to Handling Cyber security Incidents Wiley.
5. Verizon(2022) Data Breach Investigations Report. Retrieved from [Verizon website](https://enterprise.verizon.com/resources/reports/dbir/).

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details