ISSN: 2583-9888
DOI: doi.org/10.51219/JAIMLD/sabeeruddin-shaik/456

URF PUBLISHERS
connect with research world

Journal of Artificial Intelligence, Machine Learning and Data Science

https://urfpublishers.com/journal/artificial-intelligence

Vol: 3 & Iss: 1

Research Article

Proactive Incident Response Measures - From Threat Hunting to Mitigation

Sabeeruddin Shaik*

Citation: Shaik S. Proactive Incident Response Measures - From Threat Hunting to Mitigation. *J Artif Intell Mach Learn & Data Sci 2025*, 3(1), 2077-2080. DOI: doi.org/10.51219/JAIMLD/sabeeruddin-shaik/456

Received: 02 January, 2025; **Accepted:** 18 January, 2025; **Published:** 20 January, 2025

***Corresponding author:** Sabeeruddin Shaik, Independent Researcher, Portland oregon, USA, E-mail: sksabeer8500@gmail.com

ABSTRACT

Organizations must implement proactive incident response measures to prevent modern cyber threats in the current world Scenario and improve the organization's security Posture. This paper explains the Transition from reactive to proactive Measures like Threat Hunting, Regular Monitoring, conducting Risk Assessments and providing Security Awareness to the employees. In the Reactive Process, the Impact would already happen by the time we react to the incident and perform the recovery. However, by proactive measures, we could analyze and prevent the attacks before they could impact the assets. By analysing the modern challenges and cyber threats, this paper explains the importance of proactive measures that help reduce the impacts of cyber security incidents, Improve Business continuity and stay in a secure place in the digital world. This research paper explains emerging trends and how organizations can improve their defence and response mechanisms to protect their critical assets. By implementing proactive measures, the organizations are protecting their assets and developing Trust with their business stakeholders.

Keywords: Proactive incident response, Threat hunting, Mitigation measures, Cybersecurity, Incident management, Threat intelligence

1. Introduction

Considering the current Modern Evolving world, reactive measures would no longer be a secure option to protect assets. By following reactive measures, we could mitigate the risk only after the attack has occurred. This might end up in loss of data or high impacts on organizations, like reputational damage, Loss of Availability of resources and financial losses. Since the technology has developed, Attackers has also advanced with their attack strategies by Implementing Artificial Intelligence, Machine Learning Algorithms, Automation tools and Social Engineering Techniques, Attackers are taking advantage of the limitations of Traditional Reactive measures were getting succeeded in their attacks. So, the transition to proactive measures has become crucial because Proactive measures Monitor, Detect, Prevent and regularly collect the automated responses and react to them to analyze and mitigate the Risks. Proactive measures focus on protecting assets by performing Threat Analysis, Risk Assessments, Regular Monitoring and implementing Robust Security tools that detect and prevent incidents before they cause potential harm. Along with providing security to the Assets, these measures also reduce the impacts of incidents and the likelihood of incidents. Also, considering the Regulatory Compliance requirements and Industry standards are more emphasizing the Need for Proactive Measures. This Paper provides the Limitations of Reactive measures, explains structured Frameworks of proactive measures and outlines the effectiveness of implementing these measures in organizations. By Examining various advanced Tools, Technologies and frameworks, this research provides the importance of proactive measures in improving organizations' defence security, which will reduce the likelihood of Threats and their Impacts on the organization

2. Main Body

A. Problem statement

Due to the increase in cyber-attacks, such as DDoS attacks, Ransomware attacks, Advanced Persistent attacks (APTs), SQL Injection, cross-site scripting, Ransomware attacks, Insider Threats and many others, the Reactive measures approach is no longer a good secure option. Reactive measures will greatly impact because they require time to detect and respond to incidents. Here are a few key issues that support the limitations of Reactive Measures:

- **Failure to detect the threats:** Even Though Attackers implanted critical malware in the system, we could not detect the vulnerabilities because we followed reactive measures, which will lead to incidents.
- **Amplified impact:** Due to delay in responding to the incidents the threats to disrupt the services which might cause loss of availability to the services and might also result in financial losses.
- **Unpreparedness:** Reactive measures processes will not have preventive measures. These measures could not Analyze or predict the emerging threats which results the systems in vulnerable states easy to exploit vulnerabilities. A few more shortcomings for Reactive measures are due to the Increased latest Cyber Threats.

Here are a few of them:

- **Advanced attacks:** polymorphic malware, zero-day Vulnerabilities and fileless attacks cannot be detected through traditional strategies.
- **Increased attack surfaces:** The Increased adoption of IoT devices, cloud Computing and Hybrid and remote work environments has Increased the attack surface, which is making it harder to protect through Reactive measures.

Traditional Firewalls, Tools and Techniques are harder to detect and respond to promptly, which can lead to financial losses. In Reactive measures, there is a possibility for Human errors in detecting and Responding to a few Incidents. Majorly these issues show the importance of implementing proactive measures.

B. Solutions

2.1. Proactive incident response measures

Threat Hunting- Threat hunting is a proactive approach that involves actively monitoring and scanning the organization's network infrastructure to detect vulnerabilities, malware or any malicious activities that might threaten the asset. In this approach, these threats are detected by robust automated tools. With the combination of Expert teams, Automated Tools and Frameworks, it is possible to collect information on systems and analyze the system security.

2.2. Processes: Here are a few Processes for Threat Hunting

- Hypothesis-Driven Hunting- In this method, Potential Threats are analyzed Using the MITRE Attack framework, which provides the details of TTP Tactics, Techniques and Procedures. By analysing the known patterns and signatures, Threats can be detected.
- Indicator- Driven Hunting-In this method, threats are analyzed based on Forensic analysis of past attacks to find hidden threats.
- Data Driven Hunting - Using Data Analytic techniques, we can analyze the Threats and the Risk appetite. We can also compare various Data sets with information regarding the vulnerabilities and predict the significant Threats.
- Tools and Techniques: SIEM Tools, SOAR Tools, EDR Tools, Velociraptor, OS Query and Suricta to support Threat Hunting and antivirus software are effective in finding threats.

Regular Monitoring: Usage of Advanced Technologies- Implementing AI Tools and utilizing Machine Learning Algorithms makes regular monitoring easy. Tools will perform continuous monitoring and trigger alerts if there are any attack patterns, which helps troubleshoot and mitigate risks.

- **Telemetry data:** Advanced technology software and tools collect Logs regularly, which provide details of traffic flow and help act as surveillance security for early detection of threats.
- **Security operations centre:** By Building a security operations Team to Monitor the network 24*7. Even though we deploy Robust automated tools for regular monitoring, detecting, collecting logs and preventing Threats. But there are also chances for false positives. So, it is essential to involve Human checks for Deep Analysis and Responding to the Alerts.
- **Automated mitigation:** Pre-emptive Playbooks, Automated response not only helps mitigate the issue but also reduces the recovery time. This automated mitigation process helps detect threats and prevents them from occurring, reducing the manual interference needed to resolve attacks.

Challenges in Implementing Proactive Measures-Though by Implementing Proactive measures organizations could improve their security posture, there are some challenges in adopting the proactive incident Response Framework. There is a need for Deploying Robust Security tools for Endpoint security and real-time monitoring to prevent Insider Threats. To deploy these tools, Companies should Invest highly. Since these are advanced tools, companies should recruit highly skilled professionals or provide training to employees and educate them on the usage of these tools.

False Positives- There is a chance of getting False Positives, for which Human intervention is required for deep analysis.

Compatibility issues may arise because a few legacy systems are incompatible with the advanced tools.

Overcoming Challenges: Deploying Managed Detection and Response tools can reduce implementation costs. As per the company budget deploying the tools as per company requirements one after the other.

C. Uses

Proactive Incident Response measures provide a better security posture for organizations. Here are some objectives:

- **Improved detection capabilities:** By following Proactive measures, we could even detect zero-day vulnerabilities and implement security controls before the incident occurs.
- **Faster response:** Reduced Mean time to detect (MTTD) and Mean Time to Respond (MTTR).

Proactive Measures provide Improved security Control mechanisms for the Cloud Environments in Protecting Authentication and Authorization controls. By Implementing Advanced Endpoint security tools, Continuous monitoring and detection of malware through Behaviour patterns. Satisfying the Compliance Regulatory Requirements, these strategies will benefit the Various Industry sectors like Health care, Energy, Government and Financial in Preventing the Organization from Advanced Threats. Improvement in Organization's Resilience - Increased capability to mitigate Disruptions

D. Impact

Here are a few positive impacts of Implementing Proactive measures:

- **Operational Efficiency:** Improved Incidence Response Time. Reduced Mean Time to Detect (MTTD) and Mean Time to Respond, which Improved the Operation efficiency of the industries, making resources available in less time.
- **Decrease in Financial Losses:** Proactive measures improve security and prevent Data Breaches and also Since the Downtime during the Incidents decreased. This saves the companies from Fines or Financial losses. Due to Improved security Posture, the Reputation of the company among stakeholders is boosted.

D. Scope

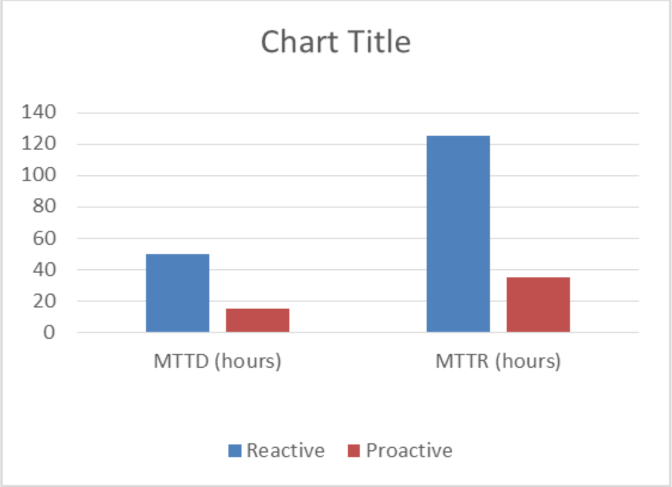
This Research examines applications across various industries:

- Proactive Network Management: Allows smooth Traffic flow by filtering Unwanted traffic or malicious traffic and maintaining network security
- IoT and Cloud security: With Regular monitoring controls, it is possible to detect and mitigate vulnerabilities with the help of Robust security tools.

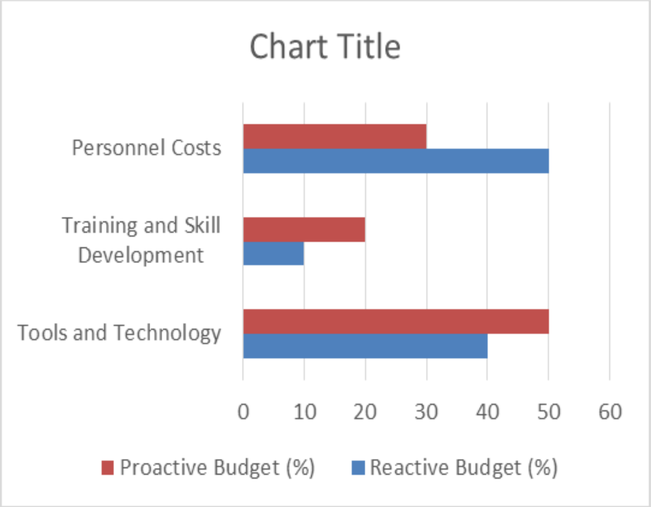
Integrating Proactive measures makes it possible even to mitigate zero-day vulnerabilities.

Future Trends: Enhancing Advanced AI Capabilities reduces Manual intervention, which also reduces response time and Fast recovery processes.

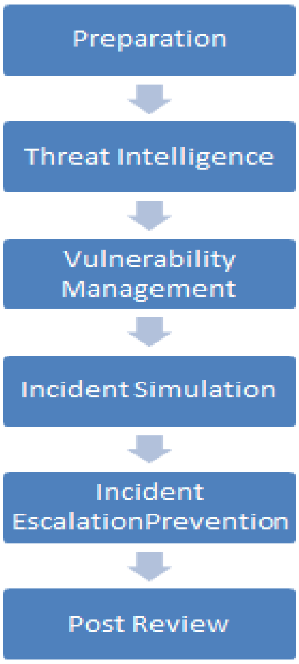
3. Graphs and Flow charts



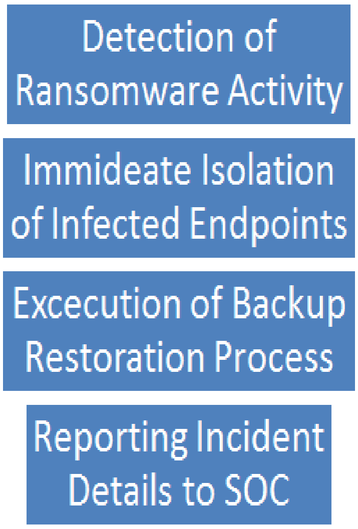
(i) Graph: Comparative analysis of MTTD and MTTR in reactive vs. proactive strategies.



(ii) Budget allocation efficiency for organizations adopting proactive strategies.



(iii) Flowchart: Proactive incident response process from threat detection to mitigation.


Detection of Ransomware Activity
Immideate Isolation of Infected Endpoints
Excecution of Backup Restoration Process
Reporting Incident Details to SOC

(iv) Example of Automated Playbook Workflow

4. Conclusion

The Implementation of Proactive Incident Response Measures in organizations is very necessary. From this case study, we can determine that transitioning from Reactive to Proactive measures would help organizations improve their security posture by Detecting and mitigating vulnerabilities. Performing the Threat Analysis of the critical Assets and Implementing prevention measures reduces the impacts of the incidents. Even in the case of an Incident attack, preparing Business continuity Plans will help the Organization run critical Machines, reducing financial losses and non-availability issues. These measures also improve the Defense mechanisms of the industries and keep the Assets safe. So, Investments in Threat Hunting, Automation tools and Comprehensive Frameworks are crucial to withstand the latest cyber-attack

5. References

1. Smith M. Advanced Persistent Threats: Detection Techniques and Mitigation strategies, Int J Geo-Information systems, 2023.
2. Davis AAT. Enhancing Cybersecurity Resilence Through Threat Hunting and Incident Response Strategies, Academia.edu, 2023.
3. Kumar R. CyberThreat Intelligence as a proactive extension to Incident Response, ISACA Journal, 2021.
4. Brown PAK. Incident Response, Buisness continuity and Disaster Recovery, springer, 2023.
5. T. e. al. A proactive approach to Advanced cyber Threat hunting, IEEE Xplore, 2022.
6. EECMR. Hutchins, Intelligence-driven computer network defense informed by analysis adversary campaigns and intrusion kill chains. Lockheed Martin Corporation, 2011.
7. Gupta M. Proactive cyber security: Threat Hunting and Mitigation strategies, IEEE Transactions on Information Forensics and security, 2020.
8. Smith J. Threat Hunting: An essential approach to cyber defenses., IEEE Security and Provacy, 2020.
9. P. e. a. Ramirez, Mitigation strategies Post-Threat Hunting: comprehensive Approach, IEEE Security and privacy letters, 2021.