IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# A Study On Cybersecurity Incident Response Platform (CIRP)

**Author[1] Pallavi Ramesh Pagar**
Jaihind Institute of Management and Research, Kuran, Pune, Maharashtra (MCA)

**Author[2] Sakshi Bhausaheb Bhor**
Jaihind Institute of Management and Research, Kuran, Pune, Maharashtra (MCA)

**Research Guide- Prof. Shubhangi Pratik Bombale**

**Prof. Dnyaneshwar Balu Lokhande**

## ABSTRACT

The number of cyberattacks is rising annually, and businesses need a quick, well-organized, and efficient solution to handle security issues. Teams may identify, evaluate, and react to cyberthreats in an organized manner with the aid of a Cyber Security Incident Response Platform (CIRP). The concept of CIRP, its elements, features, advantages, difficulties, and future potential are all explained in this research paper in an easy-to-understand manner.

Organizations must have strong and effective incident response capabilities due to the increasing complexity and frequency of cyber attacks. Delays in detection, analysis, and containment are frequently caused by manual procedures and traditional, disjointed security systems, which exacerbate financial and reputational harm. The urgent need for a simplified, automated method of handling security breaches is discussed in this study. In order to improve the efficiency and speed of incident handling, the main goal of this project is to design, build, and assess a complete Cyber Security Incident Response Platform (CIRP) that integrates and coordinates several security solutions. A framework and prototype platform were developed as part of the design science research process, which was then assessed through a case study in an automotive production setting.

## 1. INTRODUCTION

Cyberattacks including ransomware, phishing, malware, and data breaches are becoming more frequent in the digital world. Organizations must act fast to minimize harm when an assault occurs. Security teams can effectively handle these situations with the aid of a system or technology called a Cyber Security Incident Response Platform (CIRP).

Early threat detection, appropriate response, and sensitive data protection are the primary objectives of a CIRP.

A documented, strategic blueprint known as a Cybersecurity Incident Response Plan (CIRP) gives firms a methodical way to identify, address, and recover from security breaches and assaults. Its main goal is to reduce an incident's damage, downtime, and financial and reputational effects while maintaining business continuity and adhering to legal and regulatory obligations.

As part of an incident response program, Introduction to Cyber Incident Management offers helpful advice for effectively and efficiently handling issues. Cyber event detection, analysis, prioritization, and management are key subjects.

## 2. Key Components of CIRP

4.1 Identification of Incidents
This section uses methods such as intrusion detection systems (IDS) to identify possible threats.

4.2 Analysis of Incidents
The platform assists security teams in comprehending:
• How the incident occurred;
• Which systems are impacted; and
• How serious the effect is.

4.3 Reaction Measures
Teams can take actions like blocking suspect IP addresses, isolating compromised devices, removing malware, and resetting user passwords with CIRP.

4.4 Recuperation
The system aids in returning to regular operations:
Rebuilding impacted systems; restoring backups; and confirming that the threat has been eliminated.

4.5 Reporting and Documentation
Every occurrence is documented for the following reasons: legal requirements; future training; and enhancing security protocols.
.

## 3. Features of a Good CIRP

Automation (which minimizes manual labor) and real-time alerts are components of a robust incident response systems.

For collaboration; integration with other security solutions; threat intelligence; monitoring dashboards; and investigative tools.

An organization's ability to swiftly and efficiently identify, evaluate, contain, and recover from cyber disasters is ensured by a robust incident response platform. To lower risk and downtime, a successful CIRP integrates technology, workflows, automation, and intelligence.

## 4. Benefits of CIRP

6.1 Quicker Reaction
Automation enables teams to act right away.

6.2 Improved Coordination
On a single platform, teams may exchange information and communicate.

6.3 Diminished Damage
Financial and operational losses are decreased by prompt response.

6.4 Better Security Procedures
Organizations can develop more robust security measures with the use of reports.

6.5 Savings
stops serious attacks that might cost millions of dollars.

## 5. Challenges of CIRP

Despite its benefits, CIRP has certain challenges.

- Expensive for small businesses
- Needs cybersecurity experts with training
- Problems integrating with outdated systems
- Teams may become overwhelmed by too many alerts.

## 6. Real-World Applications

Banks use CIRP to avoid fraud and data theft; hospitals use it to protect medical data; government agencies use it to prevent cyber espionage; businesses use it to protect intellectual property; and schools and colleges use it to secure student information.

1. Recognizing and Addressing Ransomware and Malware Attacks

The application of CIRP
The CIRP receives alerts from EDR/AV tools.
File hashes, user behavior, and suspicious processes are automatically correlated by the platform.

A playbook initiates the following actions:

Isolating the compromised endpoint
Preventing harmful IP addresses and domains
Obtaining forensic evidence
Eliminating harmful processes

Actual Example:

A ransomware virus similar to LockBit is discovered by a banking company.
CIRP right away:

Retrieves logs from the EDR
Separates the system.
Notifies the SOC team
Initiates a workflow for confinement
Monitors the whole event

Impact: Prevents mass encryption and lateral movement.

## 7. Future Scope of CIRP

Future developments in CIRP will include:

• Machine learning for quicker analysis
• Artificial Intelligence (AI) for autonomous danger prediction
• CIRP on the cloud for increased scalability
• Enhanced zero-touch response automation

Cyber incident response will be quicker, more intelligent, and more precise thanks to these enhancements.

1. Deep Integration of Machine Learning (ML) and Artificial Intelligence (AI)
What is going to change:

- Predictive security will replace reactive security in CIRP.
- Attack patterns will be identified by AI models before they do any harm.
- ML will reduce false positives and identify incidents more accurately.

Prospective Capabilities:

• Estimating the points of ransomware infection
• Business impact-based automated severity scoring
• User risk ranking based on behavior
• Natural language-based summaries of investigations

Impact: Early prevention, intelligent triaging, and quicker discovery.

2. Fully Autonomous Incident Response (Zero-Touch IR)

Self-driving security operations will become the norm for CIRPs.

Examples of totally automatic responses:

• Compromised endpoint auto-isolation
- Auto-revocation of compromised credentials
- Patch auto-deployment
- Auto-rebuilding of infected VM instances

Prospective Trend:

CIRP will function as a cybersecurity "autopilot."

Impact: For most events, there is almost no manual intervention.

## 8. Conclusion

An indispensable tool for contemporary enterprises is a Cyber Security Incident Response Platform (CIRP). It facilitates early threat detection, efficient response, and speedy recovery. CIRP will be essential to safeguarding digital systems and maintaining a safe online environment as cyber threats continue to increase. The future of incident response appears bright and more effective with the development of automation and artificial intelligence.

To safeguard contemporary digital settings, a Cyber Security Incident Response Platform (CIRP) is necessary. It offers an organized method for identifying, evaluating, reacting to, and recovering from cyberattacks. CIRP promotes an organization's overall security, enhances team cooperation, and lessens the effect of incidents. The advantages outweigh the drawbacks, which include expense and complexity. CIRP will continue to

develop with AI, automation, and cloud technology as cyberattacks become more sophisticated.

## 9. References


1. Aleroud, A., Karabatis, G., and Alsmadi, I. (2021). Springer, Cybersecurity Analytics.
2. (Explains threat analysis, incident response, and security monitoring.)

3. Wills, G., and Almubairik, A. (2020). An organized review of the literature on cybersecurity incident response. Information Security International Journal, 19(5), 527-542.
4. (Explains incident response models and CIRP ideas.)

5. (2012) National Institute of Standards and Technology.
6. (Offers a comprehensive incident response architecture that is used globally.)

7. J. Oltsik (2023). The development of platforms for incident response. Group for Enterprise Strategy (ESG).
8. (Explains the characteristics, tools, and industry adoption of contemporary CIRP.)

9. SANS Institute (2022). Cybersecurity Professionals' Incident Response Process (practical instructions for identifying, handling, and recovering from incidents)

10. Symantec Corporation, 2023. Incident Response Report and Cyber Threat Intelligence.
11. (Offers information about actual incidences and reaction tactics.)

12. Trend Micro (2021). The Incident Response Situation in 2021.
13. (Highlights difficulties, typical attacks, and CIRP automation.)