REPORT ON

INDIAN COMPUTER EMERGENCY RESPONSE TEAM (CERT-In)

Prepared by:
Abishek Devanand
Engineering Student – Computer Science and Engineering(Cyber Security)
Email: [abishek07d@gmail.com]
Contact: [8072356214]

Submitted to:

Sagar Sakalley

Founder & Director

MacroEdtech

Date: 01st December 2025

INDIAN COMPUTER EMERGENCY RESPONSE TEAM (CERT-In)

1. Introduction to CERT-In

The **Indian Computer Emergency Response Team (CERT-In)** is the national agency dedicated to cybersecurity incident management and digital threat intelligence in India. Established in **2004** under the **Ministry of Electronics and Information Technology (MeitY)**, CERT-In acts as the country's frontline defence against cyber incidents, vulnerabilities, and emerging threats. It serves as the nodal point for coordinating cybersecurity efforts across government departments, public institutions, private organisations, and critical infrastructure sectors.

As India rapidly digitizes through initiatives such as Digital India, UPI, online governance, and nationwide digital public infrastructure, the number of cyber threats has grown significantly. Cyberattacks today include advanced malware, ransomware, phishing campaigns, DDoS attacks, and targeted intrusions on sectors like banking, telecom, healthcare, defence, and power grids. In this landscape, CERT-In plays an essential role by issuing timely alerts, identifying vulnerabilities, providing defensive measures, and guiding organisations to strengthen their cybersecurity posture.

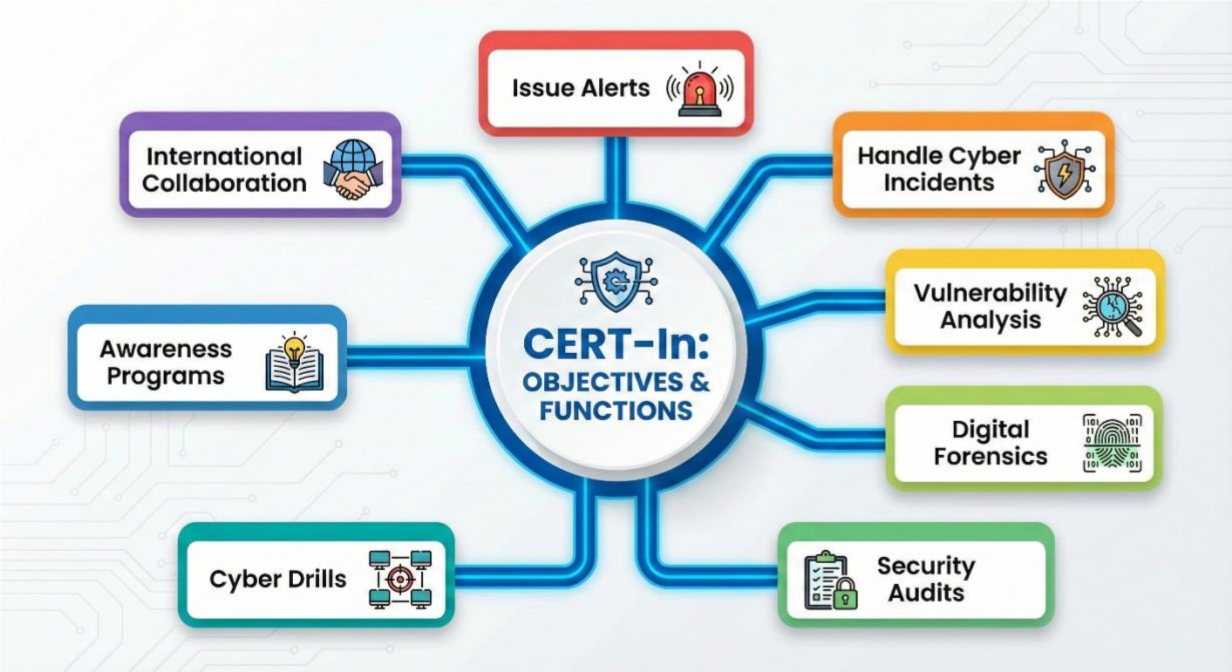
CERT-In also acts as the central coordinator for cyber incident response in India. When a cyberattack occurs, CERT-In collaborates with affected organisations, conducts technical analysis, mitigates vulnerabilities, and supports restoration of services. The agency works closely with law enforcement, digital forensics teams, and sectoral CERTs to ensure effective containment and investigation of cyber incidents. Through continuous monitoring and threat intelligence systems, CERT-In helps detect early warning signs of cyberattacks and prevents major disruptions.

Beyond incident response, CERT-In focuses heavily on strengthening national cyber awareness and skills. It regularly conducts cybersecurity drills, training programs, workshops, and simulation exercises for government, industry, and academic institutions. By encouraging best practices, promoting security standards, and collaborating with global cybersecurity bodies, CERT-In plays a crucial role in shaping a secure digital ecosystem for India. As cyber threats evolve in complexity, CERT-In remains a cornerstone of India's national cybersecurity framework, ensuring resilience, safety, and trust in the digital space.

2. Objectives & Functions of CERT-In

Objectives

- To enhance the security of India’s cyber infrastructure.
- To provide timely responses to cybersecurity threats and attacks.
- To coordinate national cyber incident handling.
- To promote awareness of cybersecurity best practices.
- To issue guidelines and advisories to prevent cyber incidents.
- To strengthen India’s cyber defence ecosystem through collaboration.



Functions

CERT-In performs a wide range of functions, including:

- **Monitoring cybersecurity incidents** across India’s networks.
- **Issuing alerts, advisories, and guidelines** to prevent cyberattacks.
- **Coordinating incident response** during large-scale attacks.
- **Analyzing vulnerabilities** in software, networks, and critical infrastructure.
- **Digital forensics** support and assistance to law enforcement agencies.

- **Conducting cybersecurity training, workshops, and drills** for organisations.
- **Promoting cybersecurity research**, standards, and best practices.
- **Collaborating with international cybersecurity agencies** to share intelligence.

---

3. Organizational Structure of CERT-In

CERT-In operates under the **Ministry of Electronics and Information Technology (MeitY)** and follows a structured, hierarchical model designed to ensure smooth coordination, rapid response, and strong cybersecurity governance across the country. The organization is led by senior cybersecurity experts and is divided into multiple specialized divisions, each focusing on a crucial functional area. This structure enables CERT-In to perform large-scale monitoring, incident handling, and policy implementation efficiently.

Its structure includes:

a. Director General / Chief Executive

Leads the organization, oversees policy formulation, and ensures execution of national cybersecurity strategies.

b. Cyber Incident Response Division

Handles real-time monitoring, threat analysis, and response coordination.

c. Vulnerability Assessment & Threat Intelligence Division

Identifies software/hardware vulnerabilities, tracks global cyber threats, and distributes intelligence.

d. Digital Forensics & Malware Research Division

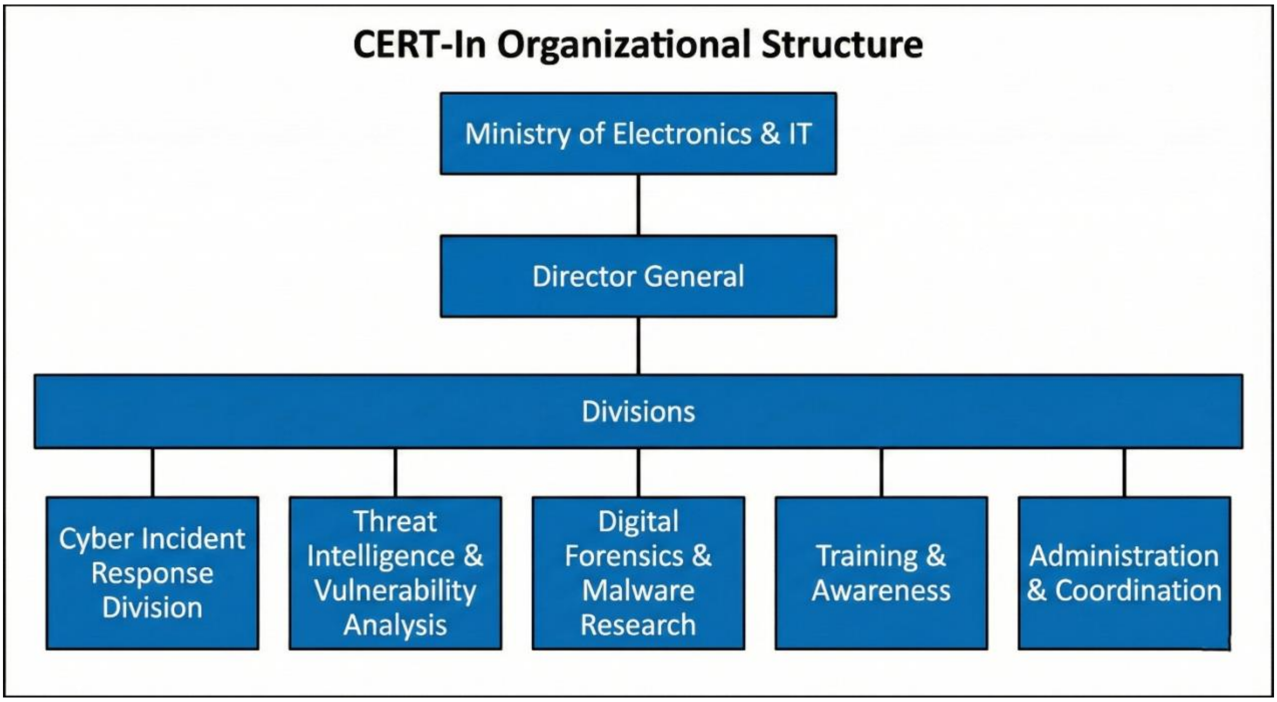
Investigates malware, analyzes cyberattacks, and provides forensic support.

e. Training & Awareness Division

Conducts certification programs, workshops, and awareness initiatives for government, industry, and academia.

f. Administration & Coordination Wing

Handles public communication, partnerships, and routine administrative functions.


CERT-In Organizational Structure
Ministry of Electronics & IT
Director General
Divisions
Cyber Incident Response Division
Threat Intelligence & Vulnerability Analysis
Digital Forensics & Malware Research
Training & Awareness
Administration & Coordination

4. Major Activities of CERT-In

CERT-In performs several key activities essential to national cyber safety:

1. Issuing Alerts & Advisories

Regularly warns organizations about cyber threats, vulnerabilities, malware attacks, and security patches.

2. Cyber Incident Response

Coordinates real-time responses to cyberattacks such as ransomware, phishing, website defacements, and network intrusions.

3. Security Audits & Compliance

Enforces cybersecurity standards for government organisations, critical infrastructure, and service providers.

4. Cybersecurity Awareness Programs

Conducts nation-wide training, webinars, and certification programs to enhance cyber hygiene practices.

5. National Cyber Drills

Organizes simulation-based cybersecurity drills to test readiness of government and industry sectors.

6. Digital Forensics Support

Assists law enforcement agencies in cybercrime investigation.

7. International Collaboration

Works with foreign CERTs and global cybersecurity organisations for threat intelligence sharing.

---

5. Types of Cyber Incidents Handled by CERT-In

CERT-In handles a wide variety of cyber incidents, including:

1. Malware Attacks

Viruses, worms, ransomware (like WannaCry), spyware, trojans.

2. Phishing & Social Engineering

Fake emails, fraudulent messages, impersonation attacks targeting individuals and companies.

3. Ransomware

Data encryption attacks demanding ransom payments.

4. Distributed Denial of Service (DDoS)

Flooding systems/networks with excessive traffic to disrupt services.

5. Website Defacement

Unauthorized modification of public or private websites.

6. Data Breaches

Unauthorized access or leakage of sensitive data.

7. Network Intrusions

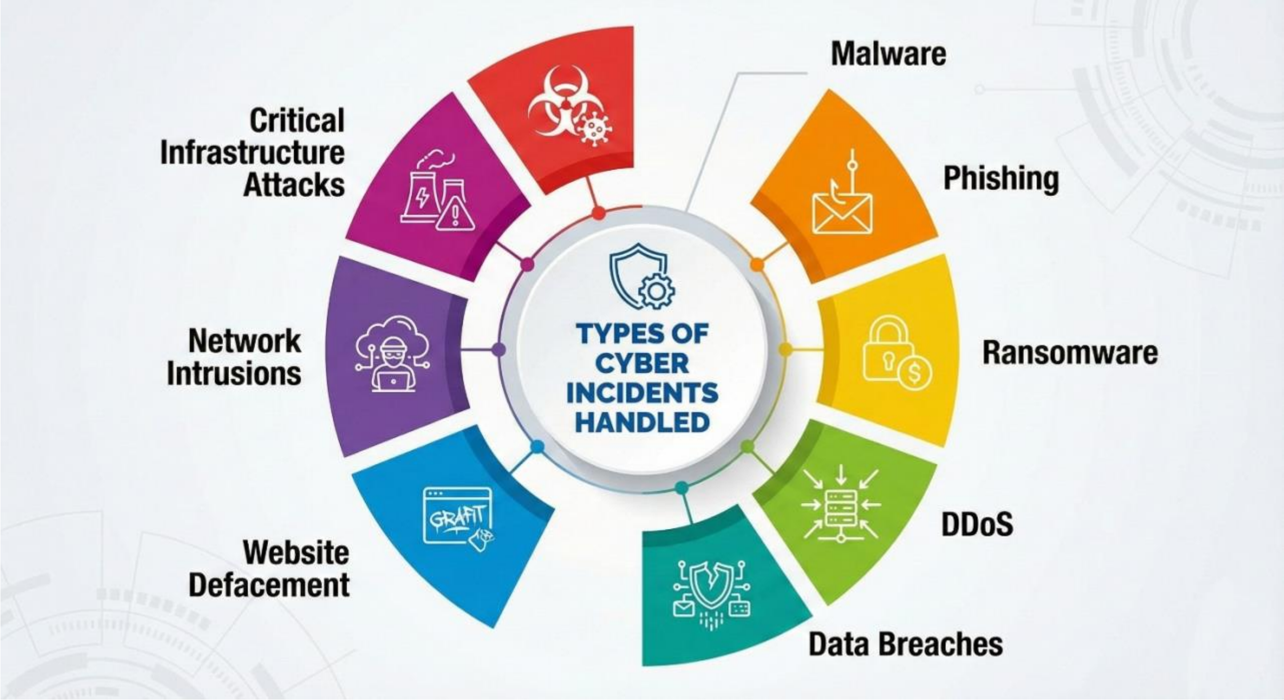
Exploitation of vulnerabilities to gain unauthorized access.

8. Vulnerability Exploits

Zero-day vulnerabilities, software bugs exploited by attackers.

9. Critical Infrastructure Attacks

Cyberattacks on banking, power grids, telecom, healthcare, or government services.



6. Case Studies

Below are notable examples of incidents where CERT-In played a major role:

Case Study 1: 2020 Indian Power Grid Cyberattack Attempt

A suspected foreign threat group targeted India's power grid network. CERT-In issued alerts, coordinated with state electricity boards, and quickly blocked malicious IPs, preventing major disruption.

Case Study 2: 2021 COVID-19 Vaccine Cyber Threats

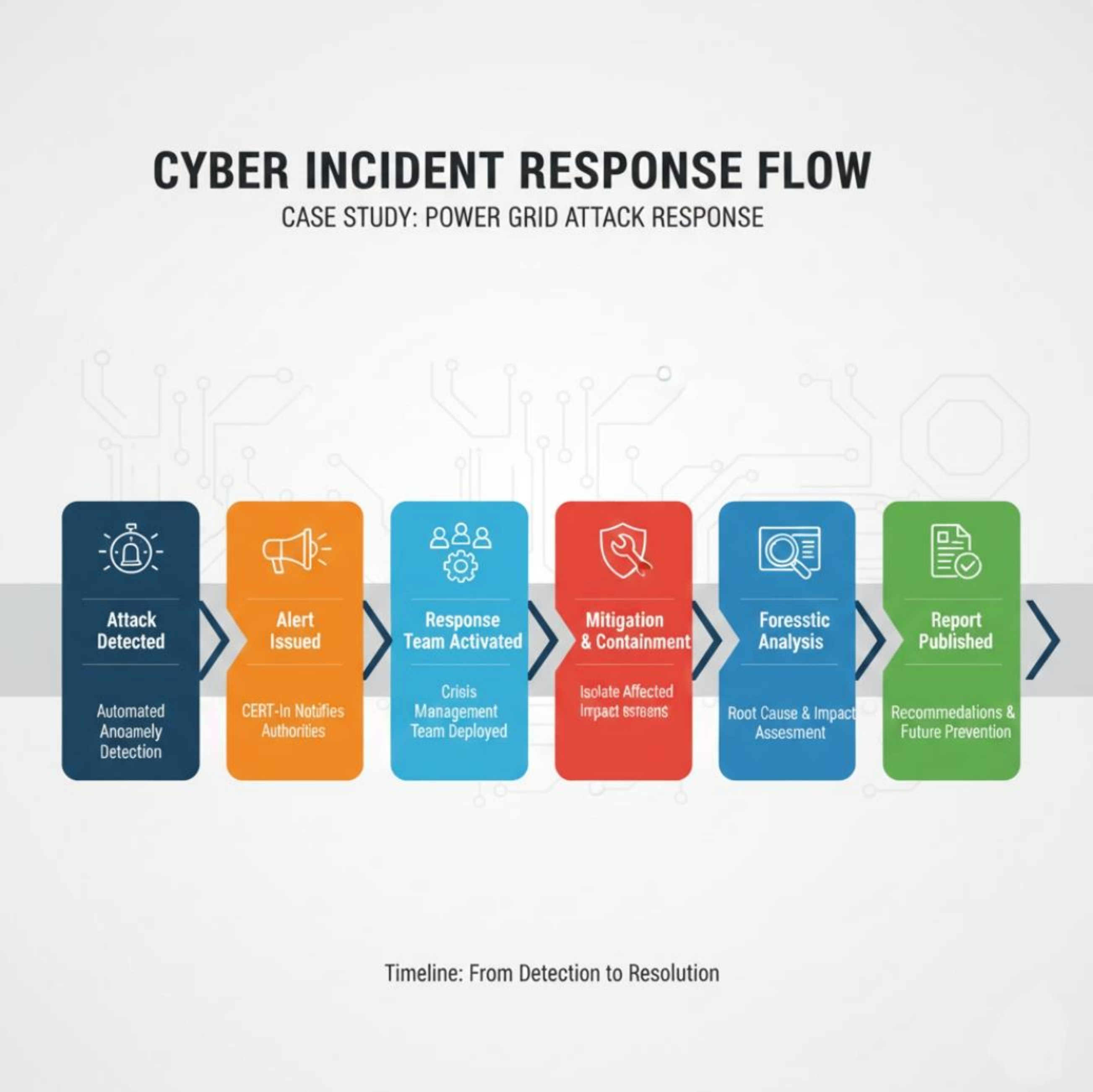
Attackers attempted to target India's healthcare and vaccine distribution systems. CERT-In notified authorities, secured servers, and provided security hardening guidelines.

Case Study 3: Financial Sector Phishing Attacks

CERT-In detected large-scale phishing campaigns targeting banking customers. It issued nationwide warnings, enabling banks to implement additional security layers.

Case Study 4: Ransomware Alerts (WannaCry, Petya, Locky)

CERT-In coordinated responses, distributed patches, and helped secure affected government and private systems.



CYBER INCIDENT RESPONSE FLOW

CASE STUDY: POWER GRID ATTACK RESPONSE

Attack Detected
Automated Anoamely Detection

Alert Issued
CERT-In Notifies Authorities

Response Team Activated
Crisis Management Team Deployed

Mitigation & Containment
Isolate Affected Impact esraens

Foresstic Analysis
Root Cause & Impact Assesment

Report Published
Recommedations & Future Prevention

Timeline: From Detection to Resolution

7. Importance of CERT-In for India’s Cybersecurity

CERT-In is vital for ensuring the cybersecurity and digital safety of India’s critical sectors. Its importance includes:

- **National Cyber Protection:** Shields government networks, defence systems, and critical infrastructure.
- **Threat Intelligence & Early Warning:** Provides timely alerts about global cyber threats.
- **Improved Cyber Readiness:** National drills enhance emergency response capability.
- **Protection of Digital Economy:** Safeguards banking, online payments, and financial transactions.
- **Public Awareness:** Educates millions on cyber hygiene, safe browsing, and security practices.
- **International Collaboration:** Enhances India’s position in global cybersecurity partnerships.

As India transitions into a digital-first economy, CERT-In remains one of the most important agencies ensuring the nation’s cyber resilience.

---

8. Conclusion

CERT-In plays a critical role in defending India against growing cyber threats. Through incident response, cybersecurity standards, advisories, digital forensics, and national drills, it strengthens national cyber resilience. With cyberattacks becoming more sophisticated and frequent, CERT-In continues to lead India’s cybersecurity efforts by ensuring preparedness, protection, and coordinated action across all sectors.

References

1. CERT-In Annual Reports, Ministry of Electronics & IT
2. “National Cyber Security Policy – Overview” by Government of India
3. Publications of Indian Computer Emergency Response Team
4. “Cybersecurity Frameworks and Best Practices” – National Informatics Centre
5. Indian Cybercrime Coordination Centre (I4C) Documents
6. “Cyber Incident Response Guidelines for India” – Government Cybersecurity Division
7. Journal of Cyber Security and Digital Forensics (India)