Incident Response & Forensic Services

Modernize security operations with greater speed and visibility

The cost and frequency of data breaches continue to rise as the speed and sophistication of attackers advance to a new level. According to IBM's latest Cost of a Data Breach Report, only one-third of companies discovered a data breach through their own security teams, meaning about 67% of breaches were reported externally by either a benign third party or by the attackers themselves.

Factors such as an increased proliferation and interconnectivity of endpoints and data, coupled with the rise of malicious activities from threat actors, have created a substantial threat to business continuity for organizations and the need for a modernized threat detection and response solution. Traditional methods often fail to detect these threats.

Key findings

66% of breaches were not identified by the organization's internal security teams and tools.

44% of alerts are not investigated and 54% of legitimate alerts are not remediated.

49% of cyber attacks are ransomware (24%) or destructive (25%).

26% who paid the ransom still could not recover the data. The average recovery after a ransomware attack is 23 days.

51% of organizations are planning to increase security investments as a result of a breach.

Source: IBM Cost of a Data Breach Report, 2023

Beat the threat with Incident Response and Forensic Services

Incident response and forensic services provide a comprehensive, proactive approach for detecting, containing, eradicating, and recovering from security incidents, as well as the roles and responsibilities of various stakeholders involved in the process. It fosters a culture of preparedness, protection, and learning, which is crucial in today's rapidly evolving threat landscape. A systematic approach to managing a cyber attack can guide organizations through an otherwise catastrophic event and prevent future attacks.

Outsmart threats with a modern approach

1. **Structured Approach:** Cybersecurity incident response is a structured and systematic approach to managing and mitigating the impact of security breaches, cyberattacks, and data breaches.
2. **Minimize Damage:** Its primary goal is to minimize the damage caused by incidents, reduce recovery time, and ensure business continuity in the face of cyber threats.
3. **Coordinated Actions:** It involves a coordinated set of actions, from identifying the incident and its scope to containing, eradicating, and recovering from the effects of the incident.
4. **Proactive and Reactive:** Incident response combines both proactive measures, like planning and prevention, and reactive measures, like containment and recovery, to address incidents effectively.
5. **Legal and Regulatory Considerations:** It takes into account legal and regulatory obligations, including data breach notification laws, to ensure compliance while handling incidents involving sensitive information.

Call our Security team today.

They'll ask you some preliminary questions about your security environment and schedule a time for a free consultation.

2401 West Monroe Street, Springfield, IL | 217-793-3800 | www.lrssecuritysolutions.com | security@lrs.com

Incident Response & Forensic Services

Transform your business and manage risk

Traditional protection methods fight known threats but are vulnerable to sophisticated and unknown attack techniques. They also don't provide visibility into assets, which is one of the primary impediments to securing these systems. Expert incident response skills are usually only available to the largest or most well-funded organizations. As many attacks are now happening at machine speed with multiple moving parts, security teams are relying on traditional security solutions that can't keep up.

Components of an effective Incident Response plan

- **Rapid Threat Mitigation:** CIR allows organizations to respond quickly to security incidents, reducing the window of vulnerability.
- **Data Protection**: It safeguards sensitive data from theft, unauthorized access, or exposure.
- **Reputation Management:** Effective response helps maintain trust and credibility with customers, partners, and stakeholders.
- **Legal and Regulatory Compliance:** CIR assists in adhering to data protection laws and industry regulations.

Common cyber resiliency challenges

1. → Failure of existing solutions
2. → Limited visibility
3. → Lack of skilled headcount
4. → Alert fatigue
5. → Dormant threats

Take the next steps

Ready to Improve your organization's incident response plan, minimize the impact of a breach and experience rapid response to cybersecurity incidents?

If the answer is yes or if have questions about a security solution that can help achieve your business goals, contact our Security team today!

Call our Security team today.

They'll ask you some preliminary questions about your security environment and schedule a time for a free consultation.

2401 West Monroe Street, Springfield, IL | 217-793-3800 | www.lrssecuritysolutions.com | security@lrs.com