LevelBlue

SOLUTION BRIEF / MAY 2024

# LevelBlue Consulting

## Incident Readiness and Response Services

It's no longer if an incident will happen, it's when.

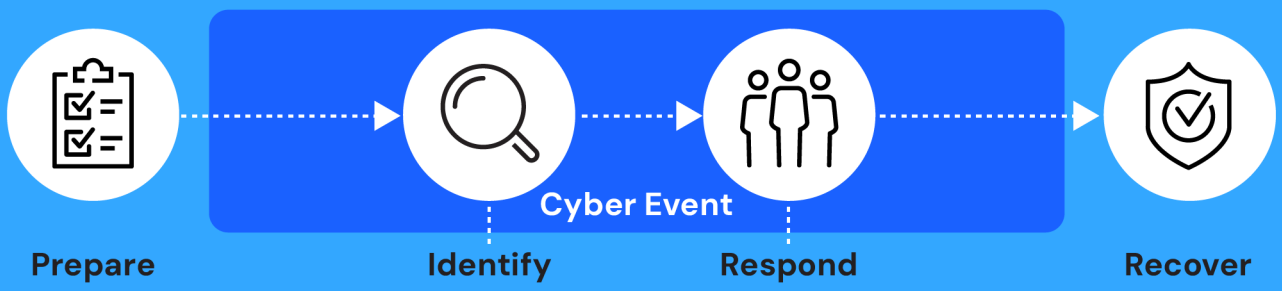
## The importance of having an Incident Readiness and Response (IRR) service in place for organizations cannot be overstated.

In today's digital landscape, it's no longer if an incident will happen, it's when. Cyber threats are constantly evolving, and organizations of all sizes are vulnerable to attacks that can lead to data breaches, financial loss, reputational damage, and legal consequences. Defending your organization and having a plan for what to do if an incident occurs is more critical than ever.

A well-prepared IRR plan enables the ability to prepare, identify, and respond to security incidents rapidly, reducing the potential damage caused by cyber threats. The benefits can become quantifiable. According to a recent survey Forrester published, global security decision makers reported that their organization paid an average of $3 million in total during a breach and averaged 63 days to recover from the breach[1].

LevelBlue Cybersecurity Consulting offers a holistic approach to help organizations strengthen their security defenses, providing IRR services that address potential threats both before and after a security breach.

## LevelBlue Incident Readiness and Response can help Mature Incident Management Program




### Pre-Breach

A cyber attack can happen at any time and take any number of forms. By taking proactive actions companies can advance preventative security measures such as improved asset discovery and visibility across their attack surface, centralized configuration, policy management, and faster mitigation. If organizations know their security gaps and close them, they can better prepare and respond to a potential breach.

We help organizations understand their strengths, identify opportunities for gap closure in their security program, and improve operational readiness for security events through a mix of the following activities:

- Malware Risk Assessment
- Incident Response Plan Creation and Review
- Playbook Creation and Review
- Tabletop and Cyber Range Exercises for Technologies and Executives
- Red Team Exercises
- Dark Web Monitoring
- SOC Optimization
- Architecture and Deployment of Preventive and Detective Controls
- Incident Response Retainer
- Threat Briefings

## Post-Breach

In the event of an incident, having IRR services is paramount to help organizations recover by providing rapid response, expert guidance, and a structured approach to incident management. LevelBlue's IRR services can help your organization respond swiftly and effectively to security breaches and mitigate their impact. Our skilled incident response and forensic specialists are available to provide support during incidents, including insider threats, external hackers, malware outbreaks, and employee policy violations. Our incident response and digital forensics services can provide:

- External or Internal Breach Response
- Incident Triage and Management
- Malware Containment and Eradication
- Image Aquisition and Disk Analysis
- Rapid Deployment of Investigative Tools (EDR/XDR)
- Log Analysis Correlation
- Remeditation Support
- Communication and Reporting Support

*Each activity would need to be scoped based on the size and complexity of the customer organization under review.

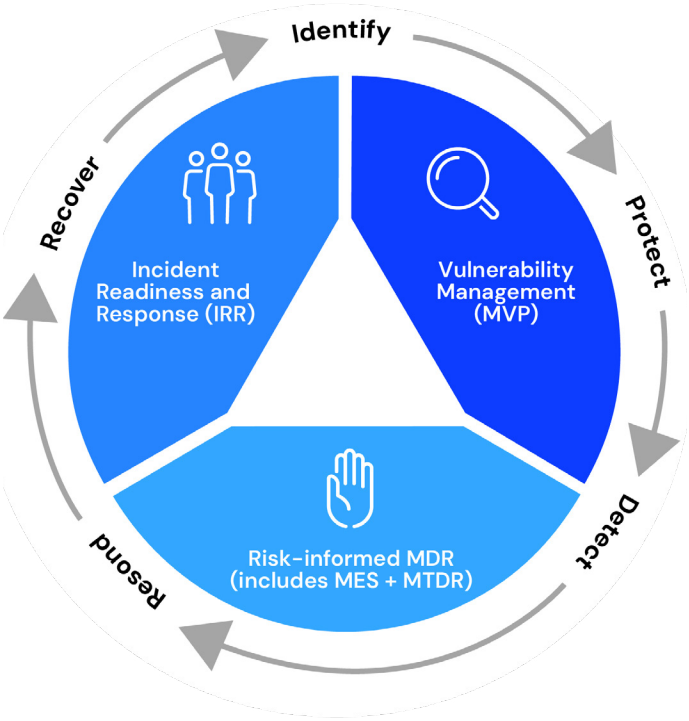
In conclusion, IRR services are vital for organizations to protect their assets, maintain customer trust, and comply with regulatory requirements. In the event of an incident, a well-structured response plan can help organizations quickly identify, contain, and resolve incidents, minimizing the potential impact. This plan can further help organizations to learn from past incidents, identify areas for improvement, and implement necessary changes to strengthen their overall security posture.

LevelBlue Cybersecurity Consulting has a team of highly skilled and experienced professionals who specialize in cybersecurity, ensuring that your organization receives top-notch guidance and support. We focus on proactive measures to help prevent cyber incidents and minimize their impact should they occur. Our consultants take a complete approach to incident readiness and response, addressing everything from risk assessments and vulnerability management to incident response planning and breach investigations, tailoring services to meet the unique needs of each organization, and ensuring that your security posture is strengthened in the most effective and efficient manner possible. By leveraging LevelBlue, you can expect best-in-breed solutions, a global network of proven technology, and a cost-effective program-based approach to meet your security and compliance needs.

**LevelBlue Cybersecurity Consulting offers a holistic approach to help organizations strengthen their security defenses, providing IRR services that address potential threats both before and after a security breach.**

**Extended security combining LevelBlue Incident Readiness and Response Services with LevelBlue Managed Detection and Response.**

LeveBlue's IRR services along with LevelBlue's Managed Detection and Response (MDR) services work together to provide a comprehensive approach to cybersecurity, covering the entire spectrum from threat detection and prevention to incident response and continuous improvement. Combining the two services provides organizations with a more efficient response to cyber threats with quicker identification, containment, and remediation of threats. Our MDR services continuously monitor across the attack surface for potential threats, while our IRR services provide a structured approach to plan and respond to any incidents that may arise.




**Potential Benefits of having LevelBlue IRR services paired with LevelBlue MDR:**

- Improve threat intelligence
- Enhance visibility into the network, endpoints, cloud environments
- Enhance incident response preparedness
- Minimize disruption caused by security events
- Mitigate the impact of security incidents
- Control data leakage
- Uncover application vulnerabilities
- Have a trusted partner on standby in the event of a breach
- Help lead or supplement the customer's internal cybersecurity team with an investigation to quickly respond to attacks and restore the integrity of their environment
- Protect sensitive data and maintain customer trust
- Regulatory compliance ensuring that organizations can promptly address incidents and remain compliant with such regulations
- Mitigate reputational damage
- Cost savings, reducing the overall costs associated with an incident response such as legal fees, fines, and potential loss of revenue

LevelBlue

# About LevelBlue

We simplify cybersecurity through award-winning managed security services, experienced strategic consulting, threat intelligence and renowned research. Our team is a seamless extension of yours, providing transparency and visibility into security posture and continuously working to strengthen it.

We harness security data from numerous sources and enrich it with artificial intelligence to deliver real-time threat intelligence. This enables more accurate and precise decision making. With a large, always-on global presence, LevelBlue sets the standard for cybersecurity today and tomorrow. We easily and effectively manage risk, so you can focus on your business.

**Cybersecurity. Simplified.**

**To learn more, contact your LevelBlue representative or visit LevelBlue.com.**