LevelBlue

SERVICE BRIEF

LevelBlue Incident Readiness and Response

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

The importance of having incident readiness and response (IRR) services 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].

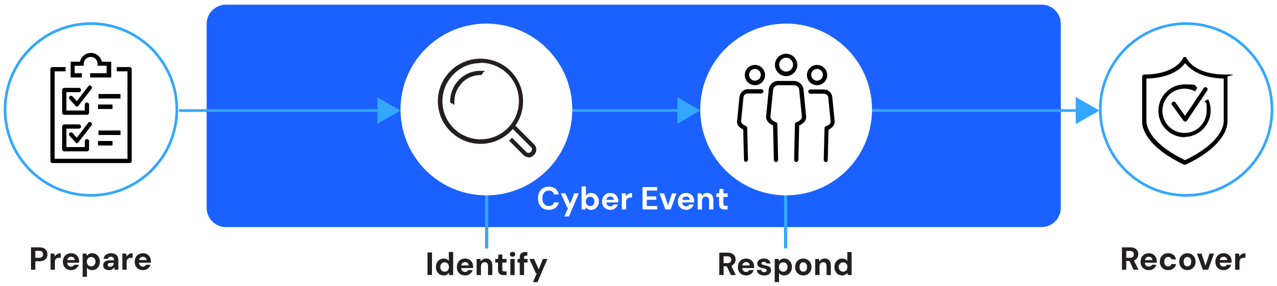
LevelBlue offers a holistic approach to help organizations strengthen their security defenses, providing IRR services that address potential threats both before and after a security breach.

[1] The State of Incident Readiness and Response, 2022 | Forrester

© 2025 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 467SB 04-2025

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

© 2025 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 467SB 04-2025

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.

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 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 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.

© 2025 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 467SB 04-2025

Service Tiers

LevelBlue offers customers service and price flexibility through three Incident Readiness and Response service tiers: Essentials, Advanced, and Premium. The Essentials tier builds a strong foundation for incident management through a thorough readiness assessment and 20 annual hours of response support. These annual hours can also be utilized for tabletop tests, playbook development, and malware risk assessments. The Advanced tier offers enhanced incident response support with 40 annual hours and monthly threat review briefings to help you stay ahead of emerging threats. With Premium IRR, customers receive the highest tier of support for incidents and can choose between a thorough incident response plan review or tabletop test. The chart below outlines the three service tiers and their component services:

LevelBlue Incident Readiness and Response

	ESSENTIALS	ADVANCED	PREMIUM
Onboarding and Readiness Review	Included	Included	Included
Monthly Threat Review Call		Included	Included
Incident Response Plan Review or Tabletop Test			Included
Phone Response Callback within specified time	24 hrs	16 hrs	12 hrs
Resources on Route Time to dispatch personnel to customer site		48 hrs	24 hrs
Annual Service Hours Customers can purchase additional hours in 20-hr increments	20 hrs	40 hrs	120 hrs

Note: Additional hours can be used for tabletop tests, paybook creation, and malware risk assessments. These are available for up front (annual) customers only.

LevelBlue IRR Service Components

Onboarding and Readiness Review: LevelBlue consultants identify gaps in people, processes, and technology, and recommend targeted improvements. Readiness is assessed through documentation review, staff interviews, and evaluation of current incident response plans, procedures, and tools. The customer receives an Incident Response Plan Assessment and Development Report with findings and recommendations, as well as a tailored incident response plan that includes key operational processes.

Monthly Threat Review Call: LevelBlue delivers monthly updates on cyber threats, including recent trends, new vulnerabilities, incident insights, risk mitigation strategies, threat actor tactics, and proactive security measures for organizations to take.

Incident Response Plan Review: LevelBlue consultants review and update the organization's incident response plan for detecting, responding to, and recovering from security incidents. This involves clearly defining and updating roles, objectives, and communication protocol and procedures.

© 2025 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 467SB 04-2025

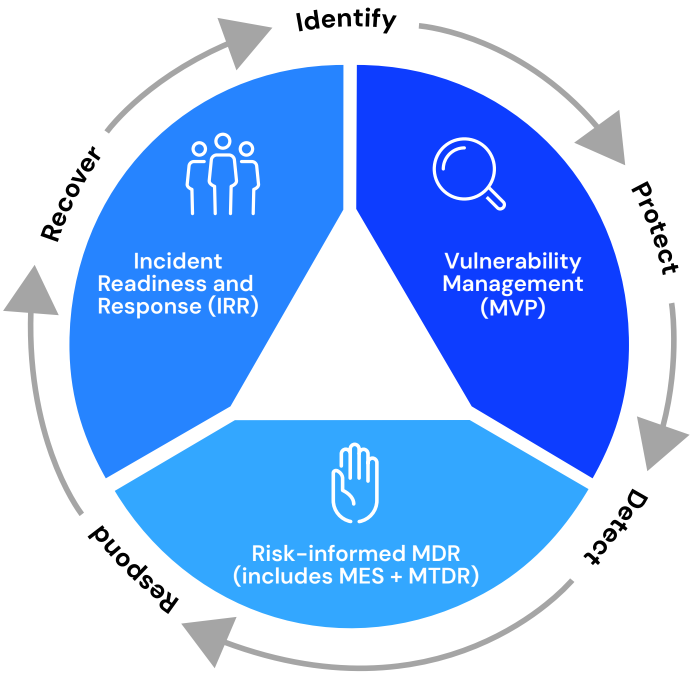
Tabletop Test: LevelBlue consultants engage in a discussion-based simulation with the customer to practice responses to hypothetical security incidents, improving coordination, decision-making, and incident response effectiveness. Participants should include a cross-functional group covering both technical and leadership roles, including cybersecurity and business leaders. Customers receive a Tabletop Exercises and After-Action Recommendation Report, which includes lessons learned, root-cause analysis, and specific recommendations to improve their incident response plan.

Playbook Review or Creation: LevelBlue Consulting provides guidance on scenario-specific procedures with step-by-step actions for different types of incidents, providing precise, actionable steps for mitigation. Playbook creation is customized based on an in-depth assessment of the customer's environment, industry, and incident response maturity. Customers receive documentation of general workflows, process diagrams, detailed procedures, and quick reference guides.

Malware Risk Assessment: LevelBlue consultants evaluate internal and external threats and share an analysis of findings and recommendations for remediation through multiple risk assessment activities and tools. Customers receive a Malware Risk Assessment Report tailored to their specific environment and industry. This includes an endpoint assessment, as well as network segmentation, patch management, and multi-factor authentication reviews, a backup and restoration controls review, and a remote connectivity assessment.

Extended Security Combining LevelBlue IRR and MDR

Organizations can combine LevelBlue IRR services with LevelBlue's portfolio of managed detection and response (MDR) services for a more comprehensive approach to cybersecurity. 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. Combining the two services provides organizations with a more efficient response to cyber threats with quicker identification, containment, and remediation of threats.


Identify
Protect
Detect
Respond
Recover
Incident Readiness and Response (IRR)
Vulnerability Management (MVP)
Risk-informed MDR (includes MES + MTDR)

© 2025 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 467SB 04-2025

Benefits of having LevelBlue IRR services paired with LevelBlue MDR:

- 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
- Protect sensitive data and maintain customer trust
- Regulatory compliance ensuring that organizations can promptly address incidents and remain compliant with such regulations
- Cost savings, reducing the overall costs associated with an incident response such as legal fees, fines, and potential loss of revenue
- Centralized visibility across customer environment
- 24/7 threat monitoring and management from the LevelBlue MDR SOC
- In-depth investigations
- Guided response and remediation – 10 hours of courtesy IR per customer, per incident
- Proactive threat hunting
- Continuously updated threat intelligence from LevelBlue Labs powered by in-product machine learning

© 2025 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 467SB 04-2025

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.

© 2025 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 467SB 04-2025