

LevelB/ue



LEVELBLUE CONSULTING

SECURITY SERVICES FOR INCIDENT RESPONSE

Have a trusted partner on
standby in the event of a
security breach

Whether or not your organization is prepared, security breaches have become common occurrences. Sometimes, the bad guys win, and security measures occasionally fail to prevent an incident.

LevelBlue has experts in incident response (IR), forensics, and electronic discovery who can support or supplement your team when suspected unauthorized, illegal or malicious activities are detected or you are ready to develop a comprehensive plan so you are prepared in the event of a breach.

IR is an expedited reaction to an adverse event, issue or occurrence. Incident management of a security incident may include: Detection, Triage, Response, Containment, Root Cause Analysis, and a plan to prevent similar events in the future.

Computer forensics is the process of examining and preserving data found in computer systems, digital storage mediums or on networks. This is necessary to determine as much as possible about a security incident including identifying how it occurred, a root cause analysis to determine why it occurred, collection of evidence for suspected misuse, documentation of policy violations, and documentation of potentially unlawful activities or actions.

Incident Response and Forensics Process

Incident Response and Forensics is most often required when adverse or illegal activity is identified within systems and networks.

Our specialists can either spearhead an investigation or supplement your internal security and legal teams. Companies across numerous verticals value the independence of our professionals and turn to our expertise when an adverse event requires an investigation.



Potential benefits

- Respond to security incidents to help stop attacks and mitigate impact
- Assist the safeguarding of information assets by quickly identifying and eradicating incidents
- Help reduce damage by leveraging repeatable and auditable response processes
- Analyze and recover from attacks quickly by using our incident management expertise
- Help improve incident response preparedness

Features

- Incident Response and Forensics Operations Assessment
- Forensics and Electronic Discovery
- The available Retainer Service allows companies to pre-establish terms and conditions for providing services in the event of a breach

* Co-management includes six MSS supported change requests per month



We offer priority IR services for those clients requiring pre-existing service agreements to ensure rapid response by specialized personnel.

Incidence Response Retainer Services

An IR retainer allows a company to establish the terms and conditions for providing services in the event of a suspected or confirmed information security incident. With a retainer in place, an organization has a trusted partner on standby to call in the event of a security breach. This proactive approach can significantly decrease response time and reduce the impact of a security incident, including theft of sensitive data.

This service helps enable you to field a team of information security professionals in response to a security incident or breach, assess the nature and depth of the breach, as well as the remediation of the breach. As part of this service we can gather and validate data that can be shared with law enforcement authorities. This service also provides a programmatic

approach to your IR plan. With regular touch points and scheduled activities we can prepare you to take action should a security incident occur.

As part of the on-boarding process and preparedness exercises, LevelBlue Consultants delivering the service will work with your security staff, legal, and executive teams to create internal and external messaging for use in the event of an incident. Through the program reviews/table top exercises the release of this messaging can be planned so that if an incident occurs, both the timing and the method of the release of this information is reviewed and approved ahead of the incident.

LevelBlue Consulting Services team can provide IR as an expedited service followed immediately with a forensic examination, or can be brought in after an IR effort to conduct the forensic investigation. During the response, we may work with legal, IT, information security, compliance, business unit, and risk managers to provide value to all affected parts of your business. We provide the following services that address the security risks and challenges that organizations face after an incident.

Incident Response

The LevelBlue team is available to assist when suspected unauthorized, illegal, or malicious activities are detected. Our skilled specialists are available to respond to incidents across multiple locations. LevelBlue has worked with Fortune 500 companies on credit card breaches, malware outbreaks, and internal



investigations for many years. LevelBlue is available to support companies responding to various types of incidents, including but not limited to: insider threats, external hackers, malware outbreaks, employee policy violations, and electronic discovery in response to lawsuits.

Incident Response and Forensics Operations Assessment

The Incident Response and Forensics operations assessment service provides a critical review of your current internal processes and procedures for handling events, incidents, and evidence. The results of the review are presented in a gap analysis format referencing industry best practices.

This service includes, but is not limited to, a review of the following: current IR plans; incident responder and handler skill set evaluations; incident responder and handler training evaluations; evidence seizure and storage procedure analysis; electronic data recovery; and litigation support.

Forensics and Electronic Discovery

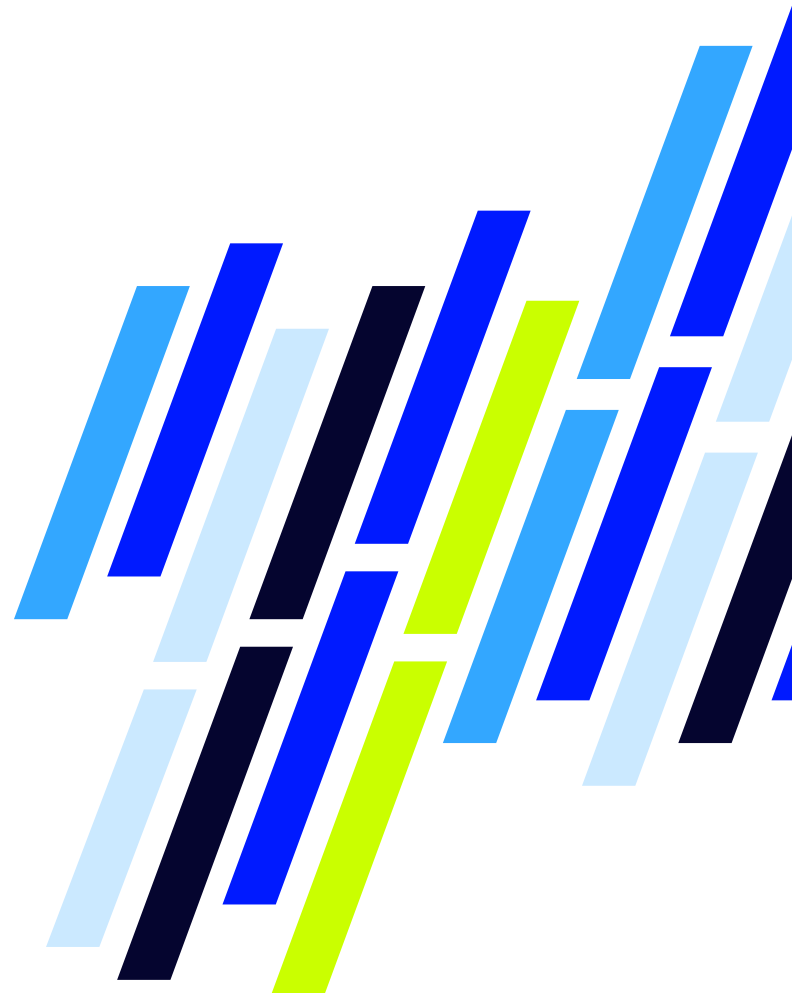
The Forensics and Electronic Discovery offering includes a full spectrum of information system-focused investigative capabilities delivered by professionals experienced in commercial litigation matters and criminal investigative proceedings. The electronic discovery service line includes the capture of computer forensic images of media and reviews of deleted and damaged data. This service provides identification of the data inventories and mappings relevant to in-scope sources and systems, and delivers analytical reviews of e-mail messages and other data sources. LevelBlue supports attorney work products as well as privilege and relevancy reviews of electronically stored data, including creation of production sets like CD, hard copy, and webpages. LevelBlue can also provide affidavits, declarations, expert reports, and related testimony on its electronic discovery activities.

Key Benefits

The LevelBlue Consulting forensics and electronic discovery practice focuses on providing independent and unbiased forensic investigations. We combine in-depth knowledge and use of industry standards, applicable regulatory requirements and our experience in information security management practices within the industry.

Security Solutions: Expertise from a Trusted Provider

LevelBlue provides a unique and world-class portfolio of assessment, compliance, and related security services. Our experience, expertise and commitment to open standards have established us as a strategic and trusted advisor with our customers. 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.



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.

For more information contact a LevelBlue Representative or visit [here](#).