Solution Brief

Digital Forensics and Incident Response (DFIR) Retainer

A new breed of retainer that provides always-on access to an expert technical team ready to respond

Why is an Incident Response Retainer important, and why trust BlueVoyant?

A cyber incident can cause business disruption, loss of sensitive data and create liability for your organization. To mitigate this risk, most organizations invest heavily into cybersecurity software, training and even Managed Security Services. While these products and services go a long way to protect your network, they can't fully protect you from insider threats, successful phishing campaigns, or external threat actors that are developing new ways to compromise your environment. Breaches are inevitable.

A general Incident Response retainer allows you to respond quickly with a team of experts who can get moving right away without having to negotiate terms and conditions during a crisis. But is this enough?

BlueVoyant Digital Forensics and Incident Response (DFIR) Retainer not only offers rapid response, but we also partner with you to thoroughly investigate incidents, as well as perform digital forensics to investigate smaller events to help prevent them from becoming larger incidents.

Through hundreds of data breach investigations, we have observed that **most large-scale breaches could have been avoided had the initial indicators of unauthorized access been fully investigated and appreciated at the time of occurrence.**

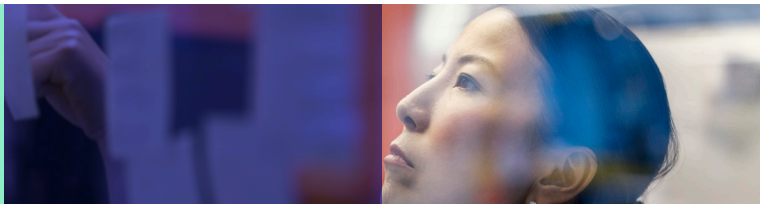
Experience has shown that almost all catastrophic breaches start as something much smaller - a missed or underappreciated A/V alert, repeated "failed" attempts into critical devices or a mistaken belief that the threat was caught "in the nick of time" only to realize weeks later that the threat had already gained persistence. The window of opportunity to stop a large-scale attack had been missed even though additional deep dive forensics would have revealed the true plot.

Key Differentiators

- Partnering with BlueVoyant helps protect you from large scale breach events by encouraging investigation of small, but high-risk incidents before they grow.
- Up to 50% of DFIR retainer unused hours can be rolled over upon renewal.
- Dedicated team of Incident Response (IR) professionals with experience handling hundreds of full scope DFIR investigations involving ransomware attacks; insider threat; malware-based data breaches, etc.
- Trusted by more than 20 cyber insurance companies to perform IR and digital forensic services for their insured clients.
- Unmatched expertise from seasoned forensic examiners with FBI Cyber, Fortune 100, legal and other private sector backgrounds.
- Highly experienced, dedicated "Incident Commanders" guide your C-Suite through post breach forensics and legal challenges.

To help clients avoid having small incidents become catastrophic ones, BlueVoyant's DFIR Retainer encourages clients to utilize retainer hours for forensic investigative related matters to help stop these attacks before they grow into larger ones by digging deeper. In the process, the client builds invaluable experience and muscle memory in the event a large-scale breach occurs, better preparing them for future attacks

BlueVoyant



Features

Rapid Incident Response

Pre-negotiated terms and conditions, and rapid response SLA to minimize breach impact and expedite response. BlueVoyant's predefined chain-of-command, processes, pre-authorization with client's internal IT or third-party suppliers and service providers, communication methods, intervention scope, and monitoring of technologies/ security perimeter will also expedite incident response.

Comprehensive Investigations

Modern forensic investigations performed by an experienced and dedicated incident response team to include dead box forensics, containment efforts, root cause analysis, and data exfiltration determinations. Expert investigators capable of leading the overall crisis management strategy from scoping call to potential litigation, including expert testimony.

Compromise Assessment

BlueVoyant will utilize and deploy sensors to aggressively hunt and triage all high-risk devices in your computing environment for malicious activity and to uncover attack history and breach exposure, enabling you to identify or confirm compromised data and initiate proper response.

IR Readiness Engagement

Exercise that discusses Incident Response investigation components (e.g., immediate actions, engaging legal counsel, exfiltration, data mining, notifications, etc.) to enable your organization to assess internal IR preparedness and relevant next steps.

Data Discovery & Validation Engagement

BlueVoyant DFIR team engages your IT resources to identify and produce evidence that will be requested should an actual incident occur. Data will be reviewed to ensure proper format, delivery, and usefulness.

Quarterly Common Vulnerabilities & Exposure (CVE) Assessment

Investigation that provides domain-wide visibility into emerging security concerns by identifying both successful and unsuccessful exploitation attempts involving recently released and critical CVEs on high value targets.

Dedicated IR Team

During onboarding, each IR retainer client is assigned a dedicated forensic investigator who will act as your incident lead and direct point of contact. Also, a dedicated IR Team (Commander, Intel, Ransomware/Negotiation Specialist) will augment your internal response staff during periods of high demand, such as forensic root cause analysis, log review, and O365/Azure auditing.

Unused Hours Rollover

For North American clients, we offer the ability to rollover up to 50% of unused hours into a retainer renewal.

Incident Response Gap Analysis

For EMEA clients, we will perform a high-level Incident Response Gap Analysis, such as a review of the incident response plan, policy, and playbook as part of the onboarding process.

BlueVoyant

Features	Standard DFIR Retainer	BlueVoyant DFIR Retainer
Rapid incident response	√	√
Comprehensive investigations	√	√
Compromise Assessment		√
IR Readiness Engagement		√
Data Discovery & Validation Engagement		√
Quarterly Common Vulnerabilities & Exposure (CVE) Assessment		√
Dedicated IR Team		√
Unused Hours Rollover (only for North America clients)		√

Ready to get started? Learn more.

About BlueVoyant
BlueVoyant combines internal and external cyber defense capabilities into an outcomes-based cloud-native platform by continuously monitoring your network, endpoints, attack surface, and supply chain, as well as the clear, deep, and dark web for threats. The full-spectrum cyber defense platform illuminates, validates, and quickly remediates threats to protect your enterprise. BlueVoyant leverages both machine-learning-driven automation and human-led expertise to deliver industry-leading cybersecurity to more than 900 clients across the globe.

BlueVoyant