

Cybersecurity Additional Services



PENETRATION TESTING

Using a three-phase approach, BlueVoyant helps test your systems and network to find and verify security vulnerabilities that could be exploited by a threat actor. All discoveries are documented in a report that will specifically identify deficiencies and recommend improvements.

Includes:

- *Penetration testing for up to 20 IPs*
- *Detailed report of findings with priorities vulnerability and remediation recommendations*
- *Meets regulators recommendations for insider threat monitoring*



CYBERSECURITY CONSULTING

Cybersecurity Consulting provides a bank of hours available for use to address your cybersecurity initiatives.

Hours may be used for security awareness training, development and management of security policies, and other cyber-related intelligence.

Includes:

- *15 hours (max: 10 hours/week)*
- *Immediate access to cybersecurity experts to get technical and strategic advice across a broad range of cybersecurity topics*
- *Security policy templates*



INCIDENT RESPONSE RETAINER

The first 72 hours following the discovery of a data breach are critical. The decisions made carry legal, regulatory, investigatory, and public relations repercussions. During this short time period, every decision is critical, and even the most prepared organizations can quickly become overwhelmed.

From forensic collection to the witness stand, BlueVoyant will provide you the answers you need, paired with a superior investigative perspective.

Includes:

- *Retainer agreement tailored to your specific needs*
- *Pre-negotiated terms and conditions to reduce response time*
- *Pre-arranged, rapid response SLA's to minimize breach impact*
- *Meetings regulators recommendations for incident response preparedness**