Incident Response & Data Forensics Services

EMAGINED SECURITY®

Overview

Emagined Security has a well-respected role in ethical security practices, helping to guide clients through data loss, security breach incidents, and forensic investigations. The several individual and combined services that comprise the Emagined Security service portfolio are shown in the matrix below.

Incident Response / Data Forensics Service-Level Matrix

Service Level	Platinum	Gold	Silver	OnDemand
Brief Description	Highest-Level Service Contract	High-Level	Core Business Hour	T&M / Bulk Hour
Hotline Availability	24/7	24/7	8/5	8/5
Guaranteed Response Time	Within 2 hrs	Within 4 hrs	Within 1 business day	Best Effort
Guaranteed Deployment Time	Within 24 hours	Within 3 days	Within 1 week	Best Effort
Digital Forensic Evidence / Data Storage Retention	12 months	3 months	1 month	Duration of engagement
Incident Response Management	●	●	●	●
Incident Response	●	●	●	●
Incident Monitoring	●	●		●
Digital Forensics (basic)	●	●	●	●
Digital Forensics Data Recovery	●			●
Digital Forensics Data Discovery & Capture	●			●
eDiscovery Support	●			●
Incident Recovery Services	●			●
Neutral Party Services	●			●
Litigation Support	●			●
Minimum Retainer Size	$50,000	$25,000	$15,000	N/A

EMAGINED SECURITY®

Service Descriptions

Each item in the Emagined Security service portfolio matrix can be described more fully. The following table is a more detailed description of each service.

Hotline Availability	A phone hotline is available for use by those under a service contract, with a guaranteed response time.
Guaranteed Response Time	An Incident Response Manager will contact you within the agreed upon timelines to begin discussing your potential incident and help if additional support is needed and deployment is required.
Guaranteed Deployment Time	When investigators and/or consultants need to be deployed the guaranteed deployment time is the amount of time that can be guaranteed for an Emagined Security deployment or response to a reported incident.
Digital Forensic Evidence / Data Storage Retention	Any digital forensic evidence or data is stored and retained in a non-descript, secure, environmentally controlled facility for a minimum amount of time, after which the evidence or data is either returned or destroyed by contractual agreement
Incident Response Management	An executive-level, methodical approach to managing an internal, proactive and effectively reactive response program to security breaches and attacks (a specific instance of which is known as an incident, or case). This typically used the following stages: Monitor, Investigate, Isolate & Secure
Incident Response	A methodical approach to managing the aftermath of, in particular, a cyber-security breach or attack (known as an incident, or case). This typically requires these three steps: Investigate, Triage and Evidence Preservation
Incident Monitoring	An approach of monitoring an incident that is actively in process in order to gather evidence or Isolate and Secure.
Digital Forensics (basic)	A methodical approach to developing, preserving and analyzing evidence relating to computer and digital storage media, especially for use in civil or criminal court proceedings.
Digital Forensics Data Recovery	Building upon basic Digital Forensics techniques the Investigation Team can attempt to recover data that has been lost for a multitude of reasons.
Digital Forensics Data Discovery & Capture	Building upon basic Digital Forensics techniques the Investigation Team can attempt to identify and acquire investigative data that can be used to manage and guide the investigation.
eDiscovery Support	A discovery, usually involving the use of digital forensics, to recover evidence in exchanges of information in electronic formats, a.k.a. electronically stored information (ESI), and which is identified as relevant by legal representation by attorneys.
Incident Recovery Services	A recovery from either a security breach or incident, or a recovery of other digital forensic data of relevance.
Neutral Party Services	A forensics accounting of evidence can be gathered to determine the who, what and when of an incident.
Litigation Support	A forensic accounting practitioner acting on behalf of a litigant or the Court such as acting as an Expert Witness.