REDLEGG
INCIDENT RESPONSE & FORENSICS

FORENSICS

RedLegg experts are experienced at preserving relevant digital information and analyzing that data to help you understand the key facts related to a case. Whether investigating employee misconduct, regulatory issues, a security breach, or employment / HR issues, chances are recovery and preservation of available digital evidence is important to the investigation.

RedLegg has extensive experience assisting attorneys and corporate officials with collecting and analyzing digital evidence relevant to a variety of matters:

- Employment matters
- Non-compete agreement violation
- Unauthorized use of trade secrets
- Regulatory compliance & legal response
- Security breach

Discovery services are required for litigation purposes. Federal and other legal rules require organizations to be ready to prove preservation of data integrity during discovery. When a lawsuit is imminent or a litigation hold has been issued, the RedLegg team can assist with issues related to the collection, preservation, and processing of Electronically Stored Information (ESI).

WHAT IS REDLEGG'S INCIDENT RESPONSE?

RedLegg's Incident Response (IR) service utilizes subject matter experts to apply both highly advanced forensics tools and years of experience to the process of locating, preserving, authenticating, and producing electronic evidence. Nearly every incident involving misconduct, diversion of intellectual assets, security breaches, or internal corporate compliance violations contains digital evidence that if uncovered, would prove invaluable in illuminating the event. The digital tracks unknowingly created by wrong-doers can often be found only in electronic form. Even the most sophisticated criminals leave behind digital fingerprints that reveal their actions when scrutinized by a talented computer forensics expert.

SERVICE DESCRIPTIONS

The following is a list of the Incident Response and Forensic Services provided by RedLegg. All Incident response services can be purchased in an à la carte format or by bundled retainer.

INCIDENT RESPONSE ADVISORY SERVICES

- Legal services/Expert witness testimony
- Work with law enforcement
- Development of IR process and plan
- Tabletop exercises
- Breach coaching

FIRST RESPONDER TRAINING

RedLegg will provide key staff members with a first responder training. Suggested attendees include information security staff and other members of the team that have responsibility for responding to security incidents or engaging in internal investigations. The key components of the program will include:

- First Responder "Dos and Don'ts"
- Response Philosophies
- Preserving Electronically Stored Information (ESI) in the early stages of an incident / investigation
- The process for bringing RedLegg into a matter
  - Deployment of RedLegg technologies
- Additional scoped topics

877.811.5040
DOTELL@REDLEGG.COM
REDLEGG.COM

REDLEGG

INCIDENT RESPONSE & FORENSICS

SERVICE DESCRIPTIONS

INCIDENT READINESS ASSESSMENT

- RedLegg documents points of contact, deployment strategies, and environment landscape to better understand the clients IR process
- RedLegg assists client with deployment of EDR and network sensor tools
- RedLegg performs technical audits of the client's environment
    - Network-focused audits through the network sensor
    - Host-focused audits using the EDR tool

INCIDENT RESPONSE

- RedLegg performs technical analysis of the client's environment using EDR and IR sensor technologies. These technologies provide us the ability to scale and analyze many hosts without having to take forensic images.
- RedLegg performs network forensics and monitoring using a deployed network sensor.
- RedLegg provides host forensics using our EDR solution and supplemented by dead box analysis tools on hard drive and/or memory images.
- RedLegg leads the technical investigation process, including forensic analysis, documentation of findings, and reporting to a predefined list of personnel that may include legal counsel.
- We work with security and IT Operations at client the organization to implement remediation plans in response to incidents.

HOST-BASED FORENSICS

- RedLegg provides host forensics using dead box analysis tools on hard drive and or memory images.
- RedLegg will report on any discovered malicious host artifacts.
- Findings will be provided during scheduled updates as well as included in a formal technical report.
- Malware samples and artifacts will be provided upon request for enterprise wide searching.

NETWORK FORENSICS

- RedLegg performs network forensics through the use of SIEM, ATD, firewall/Proxy, domain controller logs, EDR logs, IDS/IPS, network PCAPs and any other aggregated logs to paint a picture of activity.
- Static analysis of any artifacts collected from network traffic.
- Findings will be provided during scheduled updates as well as included in a formal technical report.

877.811.5040
DOTELL@REDLEGG.COM
REDLEGG.COM