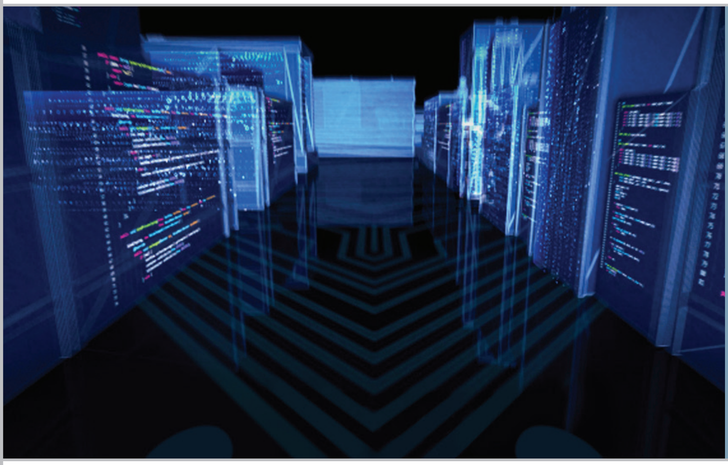
Raytheon

Digital Forensics and Incident Response
(DFIR) Services



Full life-cycle DFIR services include initial development/testing of IR plans-procedures with simulated exercises; incident response; and witness testimony expertise. Other customizable options are 24/7 DFIR coverage/expertise offer remote and onsite full incident response, containment and remediation support services.

Benefits

- 24/7 remote and on-site availability for rapid incident response
- Proactive incident preparation:
  - IR planning services
  - Testing/validation of IR plans and procedures via tabletop exercises and simulation exercises
  - Threat hunting (blue team)
  - IR retainer service
- Gain access to skilled, certified incident responders with industry certifications: GREM,GCFA, EnCE, GCIH, DoD Certifications, MPE, IACIS CFCE, IACIS CEECS
- Only RSA Level 3 ASN worldwide for Incident Response; Recognized vendor by Forrester Research

Your Organization Has Been Compromised. Now What?

Raytheon's Digital Forensics and Incident Response (DFIR) retainer service is a cost-effective measure for dealing with the unexpected effects of a highly-integrated information security environment.

With more than 10 years of experience delivering this service to a broad range of customers, our high-touch, consultative service delivery meets the highest technical and legal standards in the industry and provides:

- Advanced memory and disk analysis capabilities.
- Proactive Threat Hunting though network and log data.
- Incident containment/remediation and initial infection vector analysis.
- Incident management coordination and system recovery coordination.
- Law enforcement, regulatory and corporate communications coordination.
- After action review, playbook development, table top exercises and red/blue team assessment.
- Services that complement the breadth of your IT infrastructure including mobile device platforms.

The DFIR service works in concert with other recommended offerings to ensure that IT operational resilience, continuity and recovery processes effectively support the business objectives of our clients.

Incident Response

We provide quick and thorough containment and remediation assistance for impacted systems and processes to ensure your continued business success.

Why the Details Matter

Our full packet capture and analysis is one key to understanding the full scope of an incident. Observing and correlating available artifacts of network- and host-based systems allows for a quick determination of attribution, malicious code family, and appropriate response. By employing memory analysis of infected systems we identify advanced malicious code that doesn't operate at the disk level, but injects itself across many different processes.

In addition, our host-based artifact analysis allows for discovery of persistence mechanisms and understanding of the initial infection vector.

Incident Response Preparation and Validation

The most successful incident response programs are developed and integrated into business operations well in advance of a security incident. As part of the DFIR retainer service, Raytheon coordinates high-level planning as part of client's "playbook" of expected responses. When a potentially serious security incident is identified, client personnel can immediately call a known and trusted team at Raytheon – without wasting time when it is most critical. We also provide an initial assessment of a client's existing DFIR capabilities, including a focus on people, processes and technologies, and will recommend "quick wins" to adjust or develop new incident response options in the most cost-effective manner.

Incident Response Management Services

Under the DFIR service retainer, our clients receive priority access to Raytheon analysts and subject matter experts. Our service provides defined service level agreement (SLA) providing remote availability of Raytheon resources in four hours or less. Additionally SLAs enable Raytheon to be on site with a full team if that need presents itself:

- 24/7 security incident support from our U.S.-based team
- Telephone remote, and onsite options depending on incident type and severity
- Industry-standard response processes, enhanced by specialized tools and processes
- Remote network system, and application analysis (via VPN or hard drive analysis)
- Audit log analysis
- Forensic analysis of IT infrastructure components and services
- Incident escalation recommendations (internal and external)
- On-site security engineer/analyst engagement as required

When a potential security incident is identified, Raytheon subject matter experts work closely with your designated incident response point of contact (POC) to determine whether the incident is actually malicious or anomalous activity, determine the breadth and depth of the incident, make an initial assessment, and provide a recommended course of action to minimize exploitation of your assets. The Raytheon team analyzes the data provided by the POC and jointly determines the appropriate escalation action (e.g., escalation within Raytheon and client management, external communications management, and engagement of additional resources).

Tiered Engagement Model

Our tiered-engagement model for security incident response with key elements is defined by the size, complexity and potential business impact of each security incident. This engagement model may be adjusted or revised based on actual experience and lessons learned.

Raytheon incident response teams may extend from a single responder for a tactic incident (e.g., analysis of a single memory, device or malware sample) to a field-deployable team for enterprise-level incidents.

The Raytheon digital forensics and incident response team is assembled with surge support in mind. Our staffing model provides surge support to allow more incident responders to assist as the situation dictates. All our highly skilled experts deliver a high level of information security and incident response subject matter expertise, with skill sets in forensics, malware analysis, reverse engineering malware, and memory forensics.

Intrusion Hunting (Blue Team)

Raytheon's intrusion hunting offering will give you the knowledge of what potentially malicious activity is happening on your network by combining network- and host-based hunting techniques to obtain the most complete picture of your network. Our report will arm you with the knowledge to have a realistic conversation about the security posture of your network without the hypothetical scenarios created by penetration testers.

Raytheon believes that by taking a proactive approach to securing your network and actively hunting for signs of intrusion, your network will be far more secure than the historical best practices of watching log events and reacting when alarms trigger. Modern attackers are unlikely to match published signatures, so only by hunting will you detect them in time to prevent them from stealing your organization's information.

Delivery Model

Our DFIR services are offered as part of our V-SOC offering so regardless if you want DFIR by itself or with our managed service, we provide the a comprehensive DFIR practice to our customers with

> The best reaction to an incident is a measured and timely response.

For further information contact
cyber_marketing@raytheon.com

Raytheon Intelligence,
Information and Services
2214 Rock Hill Road
Suite 150
Herndon, VA 20170
703-467-3801

www.raytheoncyber.com/managed-services

EVERY SIDE OF
CYBER

Approved for release. Ref # E17-KDMV. Advanced Media East 06/17 4440732/4436106
This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Raytheon