Cost-effective cybersecurity response centers, with supporting services, scale and deploy rapidly to ensure information systems and critical infrastructure remain operational.

**Benefits**

- Response centers are tailorable and scalable to customers’ unique requirements
- Customizable options and services provide the building blocks to meet specific needs and evolving mission requirements
- Match customer mission to the right set of preintegrated, preconfigured products and services at scope and scale
- Consultative approach guides customers through the process to ease implementation
- Ensure information systems and critical infrastructure remain operational

The spread of cyber threats today means systems need constant vigilance to keep them operational in a contested cyber environment. The ability to grow and integrate new capabilities into a secure infrastructure as the threat landscape evolves is critical. Raytheon delivers highly scalable and extensible cyber response centers and services in pre-integrated and configurable capability sets. A robust set of optional capabilities form a layered defense approach.

**Three Tiers of Response Centers**

**Primary Response Center**
Provides fundamental monitoring and incident response capability as an extension of existing infrastructure: scalable to handle up to 20Gbps for each connection

**Enterprise Response Center**
Extends the primary response center capability to scale to speeds up to 100Gbps for each connection: incorporates analysis labs for malicious code, incident response and forensics

**National Response Center**
Extends the enterprise response center capability to scale to speeds greater than 100Gbps for each connection with additional features to ensure national-level monitoring and response

**Additional Optional Services**

- **System assessments**
  Evaluate customer systems to identify vulnerabilities for data-driven risk management
- **Cyber test ranges**
  Live-fire cyber ranges to test the cyber resilience of hardware, software, networks and enterprise maintenance and security operations
- **Mobile testing**
  Fly-Away Kits for penetration testing, malware analysis and forensic evaluation travel to remote facilities to complete testing away from the center
- **Lab environments**
  Analyze malware, perform penetration testing and conduct forensics so analysts can determine the best way to manage them
- **Knowledge transfer and training**
  Courses and practical-skills training for executives and practitioners
- **Real-time analytics**
  Identify cyber threats by connecting the dots in seemingly unrelated data
- **Adding cyber to C4ISR**
  Add the cyber element to command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) systems
- **Global Cyber Solutions Center**
  Demonstration operations center provides venues for high-quality demonstrations of cyber services and products offered by Raytheon and our vendor partners
- **Governance advisory services**
  Ensure compliance with standards and regulations
- **Infrastructure build-out**
  Selection and implementation of IT infrastructure
Cyber Protection System

**Service Options**
- Monitor and Response
  - Incident Response
  - Forensics Response
  - Network Assessments

**Knowledge Transfer**
- Executive Training
- Practitioner Training
- Operators Training
- Security Awareness

**Infrastructure**
- Physical/Virtual/Appliance/Cloud
  - Active Directory
  - Domain Name Service
  - Patch Management
  - Configuration Management

**Basic Capabilities (Common Response Center)**

<table>
<thead>
<tr>
<th>Enterprise Security</th>
<th>Core Defense</th>
<th>Data Analytics</th>
<th>Analysis Lab</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Information and Event Management (SIEM)</td>
<td>Trouble Ticketing</td>
<td>Network Behavioral Analysis</td>
<td>Incident Response</td>
</tr>
<tr>
<td>Full Packet Capture</td>
<td>Knowledge Repository</td>
<td>Threat Intelligence</td>
<td></td>
</tr>
<tr>
<td>Anti-Virus/Anti-Malware</td>
<td>Firewall</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Endpoint Enforcement</td>
<td>Intrusion Detection Services</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network DLP</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Capability Options**

<table>
<thead>
<tr>
<th>Enterprise Security</th>
<th>Core Defense</th>
<th>Data Analytics</th>
<th>Analysis Lab</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perimeter Defense</td>
<td>Information Sharing</td>
<td>User Entity and Behavioral Analysis (UEBA)</td>
<td>Digital Forensics and Incident Response (DFIR)</td>
</tr>
<tr>
<td>Defense In Depth</td>
<td>Intrusion Prevention Services (IPS)</td>
<td>Data Integration</td>
<td>Vulnerability Analysis</td>
</tr>
<tr>
<td>Secure DNS</td>
<td>CSOC</td>
<td>Social Media Monitoring</td>
<td>Forensics—Host, Network, Device</td>
</tr>
<tr>
<td>Secure Communications</td>
<td>Cross-Domain Sharing</td>
<td>Lawful Intercept</td>
<td>Malware Analysis</td>
</tr>
<tr>
<td>Endpoint DLP</td>
<td>Identity and Access Management (IdAM)</td>
<td>Insider Threat</td>
<td>Fly-Away Kits</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CERT</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cyber Range</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>National Response Center</th>
<th>Enterprise Response Center</th>
<th>Dataflow speeds</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Response Center</td>
<td></td>
<td>Dataflow speeds up to 20Gbps</td>
</tr>
<tr>
<td>Enterprise Response Center</td>
<td></td>
<td>Dataflow speeds &gt;100Gbps</td>
</tr>
</tbody>
</table>

Intelligence, Information and Services
22110 Pacific Blvd.
Dulles, Virginia
20116 USA
iiscommunications@raytheon.com
www.raytheoncyber.com