



Cyber Protection System

Network defense for organizations across the globe



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

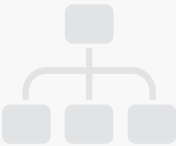
Demonstration operations center provides venues for high-quality demonstrations of cyber services and products offered by Raytheon and our vendor partners

Governance advisory services

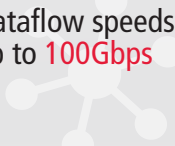
Ensure compliance with standards and regulations

Infrastructure build-out

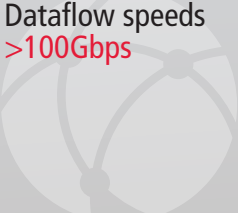
Selection and implementation of IT infrastructure



Primary Response Center
Dataflow speeds up to **20Gbps**



Enterprise Response Center
Dataflow speeds up to **100Gbps**



National Response Center
Dataflow speeds **>100Gbps**

Infrastructure

Physical/Virtual/Appliance/Cloud

- Active Directory
- Patch Management
- Domain Name Service
- Configuration Management

Service Options
Monitor and Response
Incident Response
Forensics Response
Network Assessments
Knowledge Transfer
Executive Training
Practitioner Training
Operators Training
Security Awareness
Standard Operating Procedures (SOPs)
Concept of Operations (CONOPS)
SOC Orchestration
Governance, Risk and Compliance
Advisory Services
Policy and Governance Setup
Risk Management
Infrastructure
Infrastructure Evaluation
Infrastructure Build-out
Collaboration Services
Integration Services
Backup/Restore/Continuity of Operations
Compute and Storage
Operational Staffing

Basic Capabilities (Common Response Center)			
Enterprise Security	Core Defense	Data Analytics	Analysis Lab
Security Information and Event Management (SIEM)	Trouble Ticketing	Network Behavioral Analysis	Incident Response
Full Packet Capture	Knowledge Repository	Threat Intelligence	
Anti-Virus/Anti-Malware	Firewall		
Endpoint Enforcement	Intrusion Detection Services		
Network DLP			

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

Intelligence, Information and Services
 22110 Pacific Blvd.
 Dulles, Virginia
 20166 USA
 iiscommunications@raytheon.com
 www.raytheoncyber.com