



## Proactive Threat Hunting

Combining the use of threat intelligence, analytics and automated security tools with human smarts



### Benefits

- Detect attempts to compromise your IT environment by sophisticated cyber attackers
- Mitigation and remediation
- Improve confidence in your network integrity and data confidentiality
- Obtain guidance on your information security architecture and related security controls to improve the resiliency and security of your overall IT environment
- Obtain advice and recommendations on what actions to take to respond to and eradicate cyberthreat

Raytheon understands the key components necessary to build a successful threat detection and response capability while delivering it in a packaged Managed Detection and Response (MDR) service. By combining the right tools, training, skills, analytics, visibility and intelligence, we help customers proactively hunt down bad actors and malicious activity within their networks and rapidly respond to eradicate any threats before they can harm business operations.

### Problem:

Organizations of all sizes, across all industries, are fighting asymmetric cyberbattles. Every day, they're faced with attacks from a wide range of adversaries using tactics, techniques and procedures that differ significantly from one another. Unlike the "script kiddies" of the past, these modern day advanced cyber adversaries are typically highly skilled, well-funded, elusive, polymorphic and able to bypass legacy security controls and

**Raytheon**

# Proactive Threat Hunting



exfiltrate critical data from even the most closely monitored enterprises. To compound the problem, most organizations are understaffed, overwhelmed with alerts and lack the visibility, skills and information they need to detect and investigate these advanced cyberthreats.

#### **Solution:**

Armed with our patented automated threat detection and analytics technology, superior threat intelligence, and our unique proactive threat hunting methodology, Raytheon's MDR services provide you with expert security analysts who perform ongoing deep inspection of your environment to identify threat indicators, previously undetected vulnerabilities, suspicious insider

behavior and other malicious activity on your network. We identify weaknesses in your security architecture and detect a wide range of threats that typically evade traditional security controls such as: advanced malware, zero-day vulnerabilities, lateral movement, and advanced persistent threats (APTs).

#### **Questions to Consider:**

- Do you hunt within your environment to identify the presence of known and unknown vulnerabilities, compromises and threat actors?
- Is implementing a solution for improving your security threat detection and response capabilities an ongoing challenge?

#### **Raytheon Is Here To Help**

Proactive Threat Hunting is the process of proactively searching through networks or datasets to detect and respond to advanced cyberthreats that evade traditional rule- or signature-based security controls. Threat hunting combines the use of threat intelligence, analytics, and automated security tools with human intelligence, experience and skills.

#### **Superior Technology, Intelligence and Skills**

Our patented automated threat detection and analytics technology, combined with our superior threat intelligence and highly skilled staff of security analysts enables us to deliver defense-grade MDR services that focus on advanced threat identification and validation through proactive analyst-driven threat hunting.

For further information contact  
[cyber\\_marketing@raytheon.com](mailto:cyber_marketing@raytheon.com)

#### **Raytheon Intelligence, Information and Services**

2214 Rock Hill Road  
Suite 150  
Herndon, Virginia  
20170 USA  
+1 703-467-3801

[www.raytheoncyber.com/managed-services](http://www.raytheoncyber.com/managed-services)



EVERY SIDE OF  
**CYBER**