Raytheon

Virtual Security Operations Center (V-SOC)

Our V-SOC service is designed for client organizations that need an advanced hunting capability to detect threats at the packet level that traditional security controls cannot provide.

Benefits

- Proprietary ATIP technology
- Advanced detection and threat hunting
- Extensive expertise in best-of-breed tool sets
- Focuses on advanced threats and TTPs
- Secure, isolated VDIs ensure data remains within client's environment
- Leverages client's current security toolset
- Maintains client control over sensitive security data
- Provides immediate return on investment

The traditional Managed Security Services (MSS) model uses signature-based network security tools such as intrusion detection and prevention systems (IDS/IPS) and security events (antivirus alerts, firewall denies, etc.) to detect attacks based on known patterns and attack vectors. Raytheon's V-SOC service takes a new approach to managed security by automating much of the traditional MSS model through its Automated Threat Intelligence Platform (ATIP) and allowing analysts to spend their time conducting advanced network hunting for threats that can circumvent traditional security controls.

Our V-SOC service is designed for client organizations that need an advanced hunting capability to detect threats that traditional security controls and MSSPs (standard managed service providers) cannot provide. V-SOC places the focus on advanced threats and tracking attacker tactics, techniques, and procedures (TTPs) versus simple alert response. As a result, V-SOC provides immediate return on investment by quickly identifying existing network or host compromises, zero day exploits, data exfiltration, network anomalies, emerging advanced threats, suspicious insider behavior, use of insecure ports/protocols and misconfigured devices.

Key Differentiators

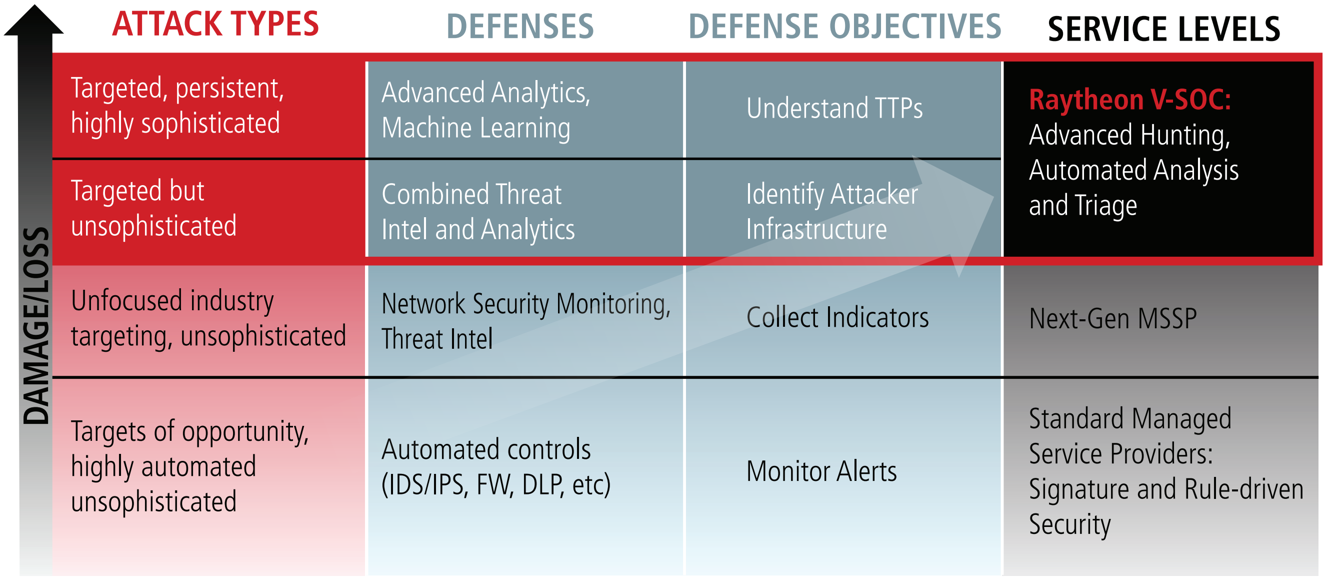
- **All data stays within the customer environment.** V-SOC leverages secure, isolated virtual desktop interfaces (VDIs) for each customer that are logically separated from all other client organizations and wiped on disconnect. Through this infrastructure our service ensures that all data stays within the client's environment. By leveraging the client's current security toolset—rather than requiring our proprietary security devices or forwarding all logs/events from the client enterprise—we ensure that client organizations maintains control over their most sensitive security data.
- **Advanced analytics.** Our proprietary ATIP technology uses advanced analytics and machine learning to improve over time based on human guidance and feedback.
- **Vendor agnostic.** We support and have extensive expertise in best-of-breed tool sets including RSA Security Analytics, ArcSight, Splunk, FireEye, QRadar, Solara, McAfee and others.
- **Our service supports and integrates into our client's processes, playbooks and requirements.** We consider our service a collaborative security service, meaning that our automation in playbooks, reporting, and process allows us to align with each client's reporting requirements, processes, and playbooks completely and efficiently. All of this is identified and integrated into the service during the activation phase.

- **We provide active advanced detection and threat "hunting."** We hunt on a 24x7x365 basis through a combination of our ATIP, automation, and human analysis "eyes on glass" approach.

	Focused	Monitored	Managed
24/7 Coverage		✓	✓
Traditional Monitoring		✓	✓
Automated Threat Intel	✓	✓	✓
Active Hunting	✓	✓	✓
Forensics and Malware Analysis			✓
NSM/SIEM Management			✓
Enterprise Security Management			✓

Our V-SOC Offerings

Our V-SOC offerings are characterized by breadth of coverage, scope of monitoring and our engagement levels. As a collaborative security service, Raytheon's V-SOC offering is designed to complement client support and operations teams from both an analytic and incident response perspective and an engineering perspective. We can offer part-time analysis and escalation support—for example, on nights, weekends, and holidays to compliment business hour coverage by client staff—full time monitoring and management support, or a long-term phased approach in which the V-SOC scope changes over time along with the maturity and operational capabilities of the customer team.



ATTACK TYPES	DEFENSES	DEFENSE OBJECTIVES	SERVICE LEVELS
Targeted, persistent, highly sophisticated	Advanced Analytics, Machine Learning	Understand TTPs	**Raytheon V-SOC:** Advanced Hunting, Automated Analysis and Triage
Targeted but unsophisticated	Combined Threat Intel and Analytics	Identify Attacker Infrastructure	
Unfocused industry targeting, unsophisticated	Network Security Monitoring, Threat Intel	Collect Indicators	Next-Gen MSSP
Targets of opportunity, highly automated unsophisticated	Automated controls (IDS/IPS, FW, DLP, etc)	Monitor Alerts	Standard Managed Service Providers: Signature and Rule-driven Security

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

Raytheon