protiviti®
Global Business Consulting

Managed Detect and Respond

Visibility, Detection, Alerting and Action

As companies face an increasing litany of cyber-attacks, conventional Managed Security Services (MSS) and response capabilities that rely on static security monitoring tools are insufficient. The future of MSS uses next generation advanced security analytics, deeper detection capabilities, threat intelligence, and AI/ML to investigate, auto-contain threats and orchestrate effective responses.

Protiviti's Managed Detect and Respond (MDR) solution provides a world-class, unified, scalable service that establishes the foundation to continuously strengthen your security posture. MDR optimizes the delivery of high-quality security incident response and investigations through expert analysis and automation, applying prescriptive and customized response actions and producing an output of key metrics to monitor and ensure critical corporate assets are protected.

Managed Detect and Respond provides piece of mind and validation to your board that your organization possesses the means to prepare, identify, contain, eradicate and recover from modern day threats.

MDR – The Foundation of a Robust Security Posture

Threat Intelligence and Detection

Our teams combine multiple sources of relevant threat intelligence feeds with integrate situational context, providing end-to-end visibility of your organization's digital infrastructure for leading threat detection capabilities. The combination of network traffic and endpoint telemetry enables real-time analysis to confirm the severity of an incident, providing the confidence to efficiently engage the correct response team members and address each situation appropriately.

Proactive Threat Hunting

Protiviti utilizes a proprietary methodology to proactively hunt threats to minimize organizational impact. Our teams can quickly find indicators of compromise and take appropriate remediation actions. Our MDR solution supports the foundation for reliable threat hunting, attack simulations and purple teaming actions to strengthen an organization's overall security program.

Security Monitoring and Response

Whether it's through custom-developed response playbooks or automated alert reactions, Protiviti's MDR experts provide the necessary tools to react swiftly and appropriately to each situation. Additionally, MDR enables forensics professionals to quickly and easily navigate through the plethora of noise that an attack bears. Post-incident forensic investigations require many forms of evidence to be collected before and during an event and our team can enable you to satisfy these requirements.

Managed Cyber Defense

Our skilled team of security experts are equipped to assess, advise, implement, operationalize and manage threat defense platforms while also developing custom KPIs, dashboards and reporting. Protiviti's team can integrate with leading SIEM, EDR, Email Security, and VMS platforms to enable enhanced world class security awareness for the organization.

Managed Detect and Respond

The Protiviti Managed Detection and Response Incident Process

Monitoring & Triage		Investigation & Response		Remediation & Recovery	
Security Incident Created	Analysis & validation for deeper investigation	Complete review of additional telemetry and enrichment validation	Perform containment activities	Validate actions, complete eradication, remediation and examine lessons learned	**Incident closed and documented**

The Protiviti MDR Methodology

Threat Detection

- Full end-to-end visibility across platforms.
- SIEM, EDR, Cloud, and 3rd Party application integration for comprehensive alerts.
- Aligned strategies by mapping to standard security frameworks.
- Techniques to decrease false positives.

Security Monitoring & Response

- Pre-built playbooks and strategies for various threat scenarios.
- Proactive and reactive containment and mitigation actions to reduce threats.
- Streamlined processes for efficient threat detection and resolution

Threat Intelligence & Hunting

- Integration of relevant threat data sources for holistic view
- Continuous assessment of threat behaviors and patterns
- Proactive threat simulation exercises
- Regular evaluation of intelligence capabilities

Customized Operations Consulting

- Metrics to visualize SecOps visibility, tool efficacy and efficiency
- Gap evaluation of security posture to identify enhancement opportunities
- Customized dashboard, metrics, and reports to align with client goals

Business Outcomes

- Significantly improved effectiveness of the tools and technology you already own
- Validation of security controls through continuous and ad hoc attack simulation testing
- Decreased destruction of data or loss of intellectual property
- Decreased mean time to respond with streamlined, coordinated threat response

Schedule a Technology Assessment today by contacting us at TechnologyConsulting@Protiviti.com.

Protiviti.com/TechnologyConsulting

TechnologyConsulting@Protiviti.com

TCblog.Protiviti.com

Robert Half® Talent Solutions

protiviti® Global Business Consulting