protiviti®
Global Business Consulting

Managed Detect and Respond

Visibility, detection, alerting and action

As companies face an increasing litany of cyber attacks, current 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 machine learning 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 key metrics to monitor and ensure critical corporate assets are protected.

MDR provides piece of mind and validation to your board that your organization is fully prepared 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 integrated situational context, providing end-to-end visibility of your organization's digital infrastructure. The combination of network traffic and endpoint telemetry enables real-time analysis to confirm the severity of an incident and efficiently engage the correct response team members to address each situation appropriately.

Proactive Threat Hunting

We use a proprietary methodology to proactively hunt threats to minimize organizational impact. Our teams can quickly find indicators of compromise and take appropriate remediation actions. MDR 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

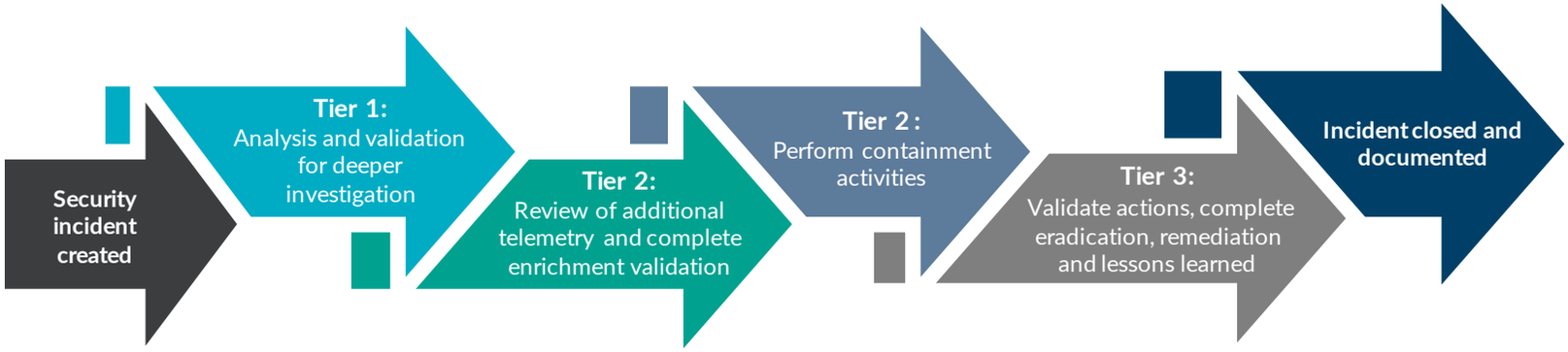
Whether it's through custom-developed response playbooks or automated alert reactions, MDR provides the necessary tools to react swiftly and appropriately to each situation. MDR also enables forensics professionals to quickly and easily navigate through the noise an attack generates. Post-incident forensic investigations require many forms of evidence to be collected from before and during an event and MDR enables you to satisfy these requirements.

Managed SIEM Services

Our skilled team of security experts can assess, advise, implement, operationalize and manage SIEM platforms while also developing custom KPIs, dashboards and reporting. MDR professionals provide integrations with leading EDR, VMS and IDS/IPS services to enable enhanced world-class security awareness for your organization.

Managed Detect and Respond

The Protiviti Managed Detection and Response Incident Methodology



Threat Detection

- Full end-to-end visibility
- SIEM, EDR, cloud and third-party app alerts
- Mapped to standard security frameworks
- Decreases false positives

Threat Intelligence and Hunting

- Integration of known IOC's
- Behavior analysis
- Industry-targeted attacks
- Offensive exercises
- Threat intelligence maturity

Security Monitoring and Response

- Managed SIEM configuration and services
- Pre-built customer validated playbooks
- IP blocks and network segmentation
- Hash banning and process disruption
- Alert-level automation, speeding investigation times

Customized Operations Consulting

- Metrics to visualize SecOps visibility, tool efficacy and efficiency
- Identification of gaps and improved response to threats
- Client specific KPIs/KRIs, dashboards and reporting.

Business Outcomes

- Significantly improved effectiveness of existing tools and technology
- 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

For more information, contact:

Shinoy George
Managing Director
Direct: +1 214-684-6666
Shinoy.George@protiviti.com

TechnologyConsulting@Protiviti.com

Protiviti.com/TechnologyConsulting

protiviti®
Global Business Consulting