MDR ADVANCED
MANAGED DETECTION AND RESPONSE

Features Summary:

- 24x7x365 Eyes-On-Glass by SOC Analysts
- Proactive Threat Hunting by SOC Team
- Proactive Remediation Guidance & Assistance
- Custom & Tuned Alerts and Notifications
- Custom Regulatory Compliance Reports
- Fully Managed SIEM

SIEM Techbology

Log Analytics

24X7 Threat Hunting

Incident Remediation Guidance

Compliance Reporting

Technology Based Service Elements:

- Cloud–Based Cybersecurity Monitoring Platform (includes SIEM Software and Hardware)
- 24x7x365 Automated Real-Time Notifications of *High Severity Incidents* (customizable alert delivery) with 30 Minute Targeted Response from SOC Analyst
- Customized Cybersecurity Detection and Alert Scoring
- Integrated Global Threat Intelligence Feeds
- Event Log Consolidation, Correlation, and Management
- In-Depth Behavioral and Anomalous Activity Monitoring
- Configuration Management Database (CMDB) that builds a Self-Learning Asset Inventory
- Near-Zero False Positives based on Continuous Rule Tuning
- Custom Report Creation and Scheduling / Custom Dashboard

People Based Service Elements:

- 24x7x365 SOC Analysts Providing Eyes-on-Glass
- *Emergency Severity Incidents* (Active or Imminent Threat) Trigger Alert and SOC Engagement with 3-Minutes Target Response Time
- *High Severity Incidents* (Potential Malicious Activity but no Imminent Threat): Manual Investigation, Confirmation, Notification with 30-Minutes Target Response Time
- Proactive Live Incident Remediation Guidance and Assistance
- Post Incident Forensics and Recommendations
- Priority Daily Cybersecurity Reviews with Weighted Triage Score
- Recurring Calls to Review Operations, Variances, and Best- Practice Recommendations
- Audit Support

Compliance Reporting & Automation

- Customized Daily Review of Cybersecurity Status that Satisfies Regulatory Compliance Requirements
- Alerts and Assistance for any Compliance Deviations
- Over 2,500 Pre-Built Compliance and Standards Reports Covering all Commonly Required Standards
- Highlight Supported Standards: *PCI-DSS, GDPR, HIPAA, SOC2, CCPA, SOX, GLBA, FISMA, NIST, SSAE16, COBIT, FedRAMP, NERC CIP, FFIEC*

Book Meeting **Get a Quote**