opentext™ | Cybersecurity

MDR is here

Uncover hidden threats in minutes

Challenges

Cyber threats keep evolving. As sophisticated attacks rise, so should the methods, defense and response.

Many businesses suffer from:

- Limited internal resources and employee turnover
- Push to drive down costs
- Mandate to increase efficiencies

OpenText Managed Detection and Response (MDR)

OpenText™ Managed Detection and Response (MDR) is built around a 100% remote, cloud-based Virtual Security Operations Center (V-SOC) supported by machine learning and the MITRE ATT&CK framework. OpenText MDR uses the latest tactics, techniques and procedures (TTP) to identify malware and threat actor behaviors. OpenText MDR experts will identify, investigate and prioritize alerts, saving you time and effort and allowing internal teams to focus on business operations.

Outcomes

- **Collection –** OpenText MDR can ingest any log source and develop correlations between desktops, laptops, servers, firewall logs, IoT devices, IDS logs, proxy logs and more.
- **24×7×365 monitoring and detection –** OpenText MDR provides organizations with active monitoring and intelligence-based detection of the latest threats delivering a 30 minute MTTD.
- **Rapid investigation and response –** Once a threat is detected, our team of experts conducts an in-depth investigation to identify the origin of compromise, extent of the breach and intent.

Why OpenText MDR?

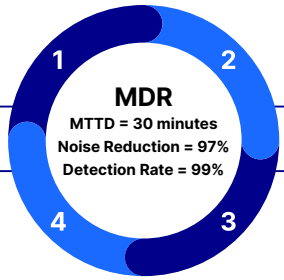
- AI-powered threat detection
- Integrated award-winning threat intelligence
- Noise reduction and alert validation
- Digital forensic investigation expertise
- Behavioral analytics
- Intuitive user experience

MDR On-Boarding

- Ingestion of log sources
- Relay and agent deployment
- XDR deployment and configuration
- Ticketing system integration

MDR Platform Customization

- Platform optimization
- Alert configuration
- Dashboard creation
- SOAR enrichment



Response

- Rapid incident response
- Malware remediation
- Root cause analysis
- DFIR services

Advanced Protection

- Creation of custon content (TTP)
- 24×7×365 monitoring and real-time detection
- MITRE ATTACK detection rules
- Threat intelligence
- Advanced threat hunting

Ready to get started? Please contact your dedicated OpenText Cybersecurity partner account manager