

SERVICE OVERVIEW

Managed Detection & Response (MDR)

Uncover hidden risks and threats before they make an impact financially, legally or reputationally



 **AI-powered**
threat detection

 **99% detection rate**—highest in the industry

 **Award winning**
threat intelligence

 **97% alert noise reduction**

OpenText Managed Detection and Response (MDR) pairs best-in-breed technologies alongside security personnel each with 15+ years of experience working breach response investigations and malware analysis engagements. This extensive experience and understanding of threat actors tactics, techniques and procedures (TTP's) leads to faster time to value, identification and remediation of risks. OpenText continuously invests this experience into improving its detection and response capabilities and building advanced algorithms for threat modelling.

Advanced threat detection & analytics

Through the OpenText cloud based Security Operation Center, OpenText MDR provides comprehensive 24x7x365 security monitoring supported by machine learning and MITRE ATT&CK analytics. OpenText's next-gen Security Information and Event Management (SIEM) can ingest any log source and develop correlations between desktops/ laptops, servers, firewall logs, IoT devices, Intrusion Detection System (IDS) logs, proxy logs, etc. using artificial intelligence and advanced workflows. OpenText continuously develops custom content in its SIEM based on

TTPs delivering 99% detection rate and 30-minute mean time to detection (MTTD). Response can be automated based on alert criticality to ensure the fastest path to threat remediation, and the remediation can be controlled in a hands-on fashion—and most importantly the validation of threats. Advanced threat detection and analytics will provide deep insights where threats originate and the overall impact to the business.

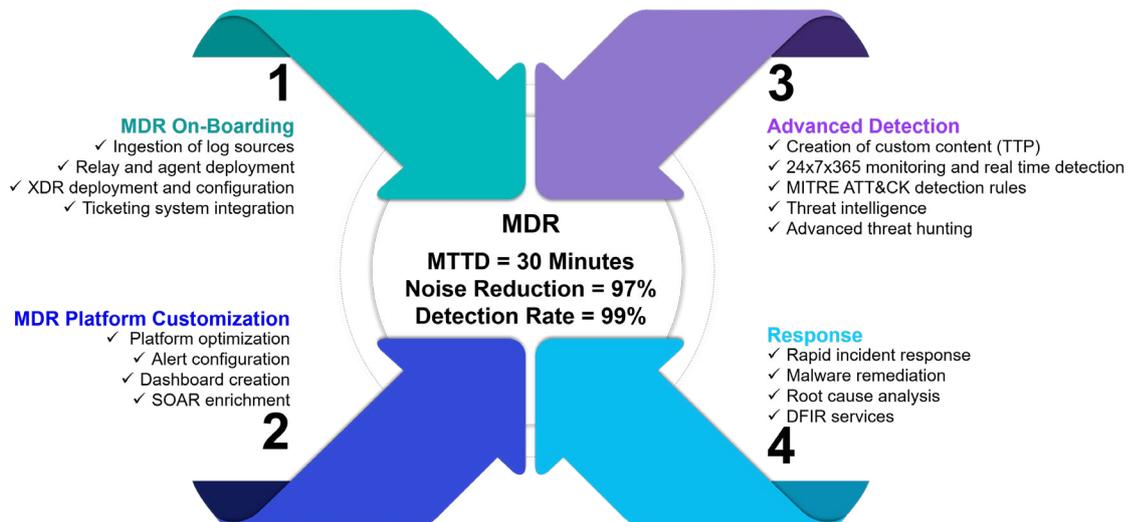
Integrated threat intelligence

OpenText MDR leverages multiple technologies that differentiate OpenText from other providers. One of these technologies, threat intelligence is integrated with OpenText’s next-gen SIEM, helping the business understand the scope and impact of any security event. Threat intelligence also allows the correlation to be drawn between data sets of known malicious files and data points identified from ingested log sources. Having threat intelligence directly integrated allows for immediate threat validation to known malware. In addition endpoint and network technologies are integrated into the solution with people, processes, and procedures in the event of a 0-day or targeted event.

Alert validation & noise reduction

OpenText Security Services workflows are unmatched in the industry and can reduce alert and event noise up to 97% leaving analysts and security personnel more time to focus on patching, upgrades, configurations, etc. OpenText processes and ability to correlate data effectively is a strength that organizations can greatly benefit from. Reduction of event noise and alerts saves analyst time, provides confidence in findings, and increases accuracy on threat identification.

Managed Detection & Response (MDR) by OpenText



Learn more about our complementary security services

[Security Assessment Service](#)

[Security Health Check](#)

[Threat Hunting Service](#)

[Security Services Catalog](#)

OpenText proposes three (3) tiers for organizations to select the MDR Service that meets their needs.

	MDR Essentials	MDR Professional	MDR Enterprise
Next-Gen SIEM			
Log ingestion	✓	✓	✓
24x7x365 monitoring	✓	✓	✓
MITRE ATT&CK detection rules	✓	✓	✓
AI/Machine Learning	✓	✓	✓
Platform access and dashboard	✓	✓	✓
Real-time detection	✓	✓	✓
Real-time alerting	✓	✓	✓
Integrated threat intelligence	✓	✓	✓
Security Services			
Dedicated Security Advisor		✓	✓
Program Manager		✓	✓
Threat hunting		✓	✓
SIEM content development		✓	✓
IOC content sharing			✓
Digital Forensics & Incident Response (DFIR)			
Threat triage support		✓	✓

For more information contact us at securityservices@opentext.com

About OpenText

OpenText, The Information Company, enables organizations to gain insight through market leading information management solutions, on-premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit: opentext.com.

Connect with us:

- [OpenText CEO Mark Barrenechea's blog](#)
- [Twitter](#) | [LinkedIn](#)