opentext™

SERVICE OVERVIEW

65/24/7
realtime defense

7 m mean
time to respond

false positives

The 2022 MITRE Engenuity ATT&CK® Evaluations for Managed Services recognized OpenText next-level Managed Detection and Response offerings for quick detection of real incidents and a 99-percent detection rate for all attack tactics.

Read the r r for details.

r y

From the OpenText virtual Security Operation Center (VSOC), OpenText MxDR provides comprehensive 24×7×365 security monitoring supported by machine learning and MITRE ATT&CK® behavioral analytics and detection. OpenText's cloud-based security information and event management (SIEM) can ingest any log source and develop correlations from telemetry collected on desktops, laptops, servers, firewall, email servers, active directory, IoT devices, intrusion detection systems, proxy and other telemetry sources using artificial intelligence and advanced workflows.

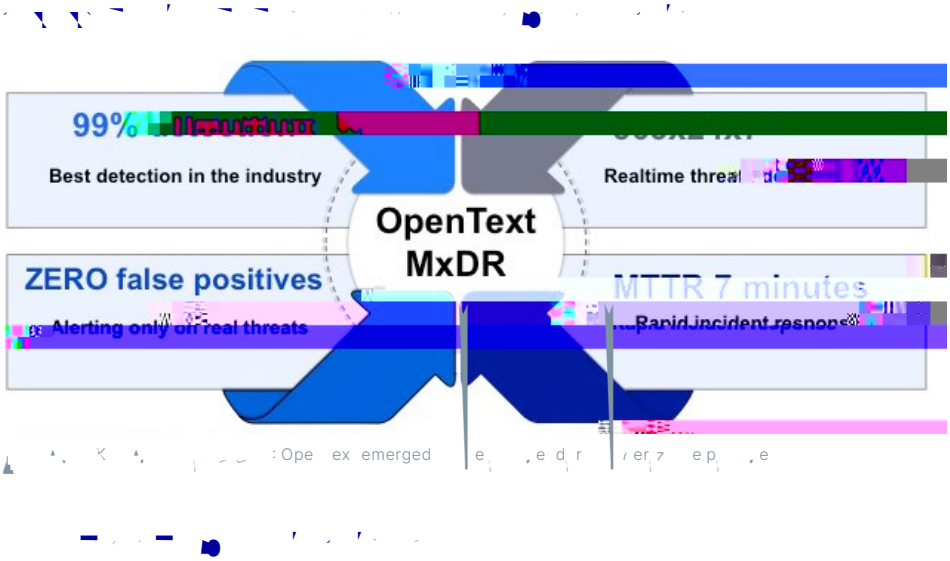
OpenText continuously develops behavioral detections in its SIEM, based on its threat research, with a seven-minute mean time to respond (MTTR). Response can be automated based on alert criticality to ensure the fastest path to threat remediation, and the remediation can be controlled in a hands-on fashion—and most importantly the validation of threats. Advanced threat detection and analytics will provide deep insights into where threats originate and the overall impact to the business.

r r

OpenText MxDR leverages multiple technologies that differentiate it from other providers. One of these technologies, threat intelligence is integrated with OpenText's SIEM, helping the business understand the scope and impact of any security event. BrightCloud 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.

r r

OpenText workflows are unmatched in the industry and can eliminate alert and event noise with zero false positives, leaving analysts and security personnel with more time to focus on actual threats and business priorities. Organizations benefit from OpenText's ability to correlate data effectively, while eliminating event noise and false positive alerts saves analysts' time, provides confidence in findings and increases accuracy of threat identification.



OpenText MxDR services are designed to provide confidence in detecting unknown risks and threats, before they can do damage to a business. It provides:

- Behavioral analytics based on MITRE ATT&CK® framework and artificial intelligence delivering a 99% detection rate with mean-time-to-respond (MTTR) within 7 minutes.
- Security workflows that eliminate event noise with zero false positives.
- Threat correlation and root-cause analysis.
- Daily automated reporting.
- Advanced workflows and 500+ TTPs detections.
- Powered with SIEM and integrated with BrightCloud Threat Intelligence.
- Behavior-based threat detection across endpoints, networks, ceieh h

o ente t™