OpenText MxDR excels in MITRE ATT&CK® Evaluations

Zero false positives, 100% detection

Sixteen leading cybersecurity providers,[1] including OpenText™, showcased their ability to identify and analyze threats and describe adversary behavior in the first independent MITRE Engenuity ATT&CK® Evaluations for managed security services. The MITRE team simulated attacks by emulating OilRig—a threat actor known for evasion and persistence techniques and complexity.

OpenText Managed Extended Detection & Response delivered:

#1

in avoiding
false positives

The only solution with zero false positives
(mislabeled, non-malicious security alerts)

100%

detection rate

Quickly identified the threat actor and detected every attack tactic within 7 minutes

Why it matters:

94% of organizations either have outsourced XDR or are planning to use managed security

75% spend as much time—or more—on false positives as real threats

85% want to reduce risk by leveraging outside XDR expertise

73% do not have enough skilled IT security personnel

Download the 2022 CyberEdge XDR survey report

[1]Participants in the evaluations included: Atos, Bitdefender, BlackBerry, BlueVoyant, Critical Start, CrowdStrike, Microsoft, NVISO, OpenText, Palo Alto Networks, Rapid7, Red Canary, SentinelOne, Sophos, Trend Micro and WithSecure.

Read more about the MITRE Engenuity ATT&CK Evaluations and results.

opentext™