opentext™

OpenText Threat Hunting Service

Proactively detect threats with speed and efficiency

Detect unknown threats across the cyber kill chain

Enhance existing technology investments with OpenText security expertise

Minimize risks and improve response time

Reduce financial and reputational damage

Cyber attackers are compromising enterprise IT environments with ever more advanced tools and sophisticated tactics. More than one billion malware varieties exist and the average enterprise encounters thousands of alerts every day.[1] Security teams spend most of their time dealing with false alerts while real threats go undetected. Proactively hunting for threats that may have already penetrated requires resources they don't have. It can take more than 200 days to identify and contain a data breach using conventional methods.[2]

Proactive threat detection reduces remediation times exponentially. The OpenText Threat Hunting Service uses AI-powered technologies with behavioral analytics to detect unknown threats based on attackers' tactics, techniques and procedures (TTP) as defined by MITRE ATT&CK® and OpenText research.

Going above and beyond the current industry practice of only using network logs to hunt for threats, OpenText incorporates telemetry information from the endpoint as well as from networks, the cloud and potentially other sources. The OpenText team of experienced threat hunting security analysts and digital forensic investigators leverages deep knowledge and experience to conduct analyses of attack patterns, exploits and vulnerabilities across high value assets.

1 AV-TEST, Malware Statistics & Trends Report.

2 IBM Security, Cost of a Data Breach Report 2022. (2022)

opentext™

> *"The OpenText threat hunting service was extremely effective. We isolated real-world threats and remediated them. We have full visibility into what those issues were and the root cause."*
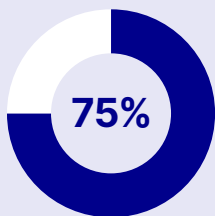
Allen Woolley,
Director of Operations for IT at Webcor

$4.35 M

Cost of a data breach on average (2022)[3]

277

Average number of days to detect a threat[4]

75%

of businesses waste equal time on false positives[5]

💬 Join the conversation

↪ Learn more

OpenText Security Services »
Securing the enterprise with 360° visibility »

Regular threat hunts are critical to identifying unknown threats before they can cause damage and uncovering hidden vulnerabilities missed during regular penetration testing. They are one of the best and fastest ways to detect cyber threats within organizations' environments.

OpenText Threat Hunting Service employs forensic investigators, incident responders, SOC analysts and other cybersecurity experts to uncover advanced persistent threats and unknown attacks. The team leverages OpenText advanced threat intelligence and tools to discover malware and suspicious behavior that, if undetected, can offer months of access to cyber attackers. Comprehensive root cause analysis of events allows incidents to be traced to their origin so that impacts can be quickly understood and remediated.

OpenText experts are well versed in TTPs used by attackers and bring decades of experience to remediation support, offering context on security alerts and recommending next steps and detailed responses. The service can uncover anomalies, such as non-human patterns, spikes of activity outside normal business hours and other red flags that may indicate an attack, insider theft or intentional destruction of data.

OpenText Threat Hunting Service delivers:

- Preventative and proactive identifying or validating of the existence of threats and/or malicious activity across the cyber kill chain.
- Quick identification of patterns, relationships and indicators of compromise.
- Insights to potential zero-day threats, both on premises and in the cloud.
- Threat hunting using anomaly and telemetry data across endpoints, networks and the cloud.
- Remediation recommendations to close gaps in security protocols and policies.
- Comprehensive threat hunting leveraging clients' existing technology stacks. No infrastructure or software install requirements.

To talk to an expert about the OpenText Threat Hunting Service, please contact **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**

---

3 IBM Security, Cost of a Data Breach Report 2022. (2022)

4 Ibid.

5 SRS Networks, 75% of Businesses Waste Just As Much Time on False Positive Security Threats, Study Finds. (2021)

opentext.com/contact