opentext™

Service overview

OpenText Threat Hunting Service

Detect, respond, and remediate threats with speed and efficiency with OpenText Security Services.

Leverage OpenText security experts

Decrease incident response time by outsourcing the detection of threats

Detect unknown threats across the cyber kill chain

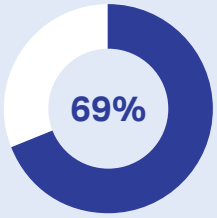
Modern digital adversaries have more access than ever to advanced tools, tactics and procedures, increasing their effectiveness at compromising enterprise networks to steal sensitive data. The average enterprise encounters thousands of alerts per day, while nearly 30 percent reportedly receive more than one million per day.[1] To complicate matters, a recent report from the SANS Institute indicates that security resource limitations are reaching critical mass, citing that a staggering 77.3 percent of security incident response teams are comprised of five members of less.[2]

The OpenText Threat Hunting Service uses the best in breed technologies with custom workflows leveraging machine learning and MITRE ATT&CK framework. Detection is done real time reducing the time to remediate exponentially.

Going above and beyond the industry's current practice of only using network logs as the standard way to hunt for threats, OpenText significantly expands that capability by incorporating telemetry information from the endpoint.

Approximately 350,000 new malicious programs are discovered every day.[3] That's one billion new instances of malware every year. But, which malware is an actual or existential threat? For each organization, it's critical to assess risk and determine which attacks warrant immediate action and which pose a lower threat.

opentext™



69 percent of organizations don't believe threats can be blocked by their anti-virus software.

$4 billion

The Equifax breach cost the company more than $4 billion.[4]

One billion

More than one billion new instances of malware will be discovered in 2019.[5]

2,500%

There is a 2,500 percent increase in instances of new malware over 10 years: from 2010 (47M) to 2019 (1.2B).[6]

Join the conversation

5 critical questions you need to ask about your sensitive data »

About that information leak: It's coming from inside the organization »

How is the enterprise security landscape changing? »

Learn more

360-degree threat detection »

Navigating a breach »

The OpenText Security Services analysts use actionable, visual dashboards to enable them to work more efficiently and focus efforts where it matters most. They prioritize events so incidents can be traced to their origin and impacts can be quickly understood and remediated. They leverage a proprietary library of workflows and automation tools to improve the speed of investigations and remediation by offering context on security alerts, recommending next steps and automating responses.

Reduce costs and risk to reputation

The OpenText Threat Hunting Service delivers advanced threat intelligence to enable quick identification and monitoring of threats and attacks. The OpenText Security Services team use the tools needed to discover malware and suspicious behavior that, if undetected, can offer access to cyber-criminals for months. 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, proactive support that identifies or validates the existence of threats and/or malicious activity within and across the cyber kill chain.
- Quick identification of patterns, relationships and indicators of compromise.
- Insight to potential zero-day threats before they can attack the environment, both on-premises and in the cloud using their Ai & ML tools.
- Threat hunting beyond network logs to cover endpoints and expand security measures.
- Remediation and risk and compliance recommendations to close gaps in security protocols and policies.

Success story

Over several days, executives and members of the senior leadership team at a leading organization received an email demanding payment in Bitcoin, otherwise the bad actor would release damaging videos and photos.

The OpenText Threat Hunting Service team collected network logs to perform threat analysis of potentially compromised endpoints and servers. The team then collected forensics artifacts and snapshot data of identified endpoints, and analytics was used to analyze all collected data to confirm infected machines and identify other unknown threats. OpenText was able to quickly identify and remediate infected endpoints before other machines were infected. The organization has engaged OpenText to evaluate its current security policy and procedures, and to perform monthly threat hunting and quarterly tabletop exercises.

To talk to a security services expert about the OpenText Threat Hunting Service, please contact securityservices@opentext.com

Sources

[1] EMA, InfoBrief: A Day in the Life of a Cyber Security Pro, May 17, 2017.
[2] SANS Institute, Integrated Incident Response: A SANS Survey, August 1, 2019
[3] AV-Test, *Malware Statistics & Trends Report*, 2019.
[4] Money, *Equifax's Massive Data Breach Has Cost the Company $4 Billion So Far*, September 12, 2017.
[5] AV-Test, Malware Statistics & Trends Report, 2019. [6] Ibid.

opentext.com/contact Twitter | LinkedIn