CASE STUDY

Simcoe County District School Board Relies on Cygilant Security-as-a-Service

Simcoe County District School Board

Industry

- Education

Challenge

- Protect proprietary information within educational institutions
- Avoid school business disruption

Solution

- Cygilant Managed Detection and Response
- Cygilant Unified Vulnerability and Patch Management

Result

- Single view of log activity and Cygilant experts' prioritization of issues for SCDSB staff to address
- Assess servers and identify any security holes including missing patches
- Immediate visibility into system weaknesses, enabling SCDSB to address concerns quickly versus waiting for an annual or bi-annual test to identify potential issues

One of Ontario's largest public education systems, the Simcoe County District School Board (SCDSB) has schools and learning centers dotted throughout 4,800 beautiful square kilometers in Simcoe County.

Simcoe County District School Board (SCDSB) relies on Cygilant Managed Detection and Response and Cygilant Unified Vulnerability & Patch Management to help defend against today's volatile cyber-threat landscape.

SCDSB uses Cygilant Managed Detection and Response to collect and monitor log activities, such as Active Directory user and group changes, multiple log on failures, privilege escalation, and unusual traffic. All activities can be viewed by both Cygilant Cybersecurity Advisors and SCDSB IT staff in a single location within the Cygilant SOCVue Portal. If there is an incident that requires SCDSB's attention, Cygilant's SOC team will alert the SCDSB IT staff, so they can address the issue immediately.

Cygilant Unified Vulnerability and Patch Management provides SCDSB with the ability to assess servers and identify any security holes. This includes finding missing security patches not just for the operating system, but also for installed applications. Cygilant provides SCDSB's IT staff with regular insight into issues that servers may have. This service provides a historical trail of all possible issues regarding the SCDSB network through real-time reporting available in the portal.

"Log monitoring and security intelligence allows us to see logical network changes that could be a symptom of an attack," said Christine Evitt, Chief Information Officer, Simcoe County District School Board. "Additionally, the ongoing vulnerability testing means we have immediate visibility into system weaknesses, enabling us to address concerns quickly versus waiting for an annual or bi-annual test to identify potential issues."

It's important to protect proprietary information within educational institutions. Suffering from a data breach would significantly disrupt school board business activities and take resources away from what really matters – serving students' needs. With Cygilant, SCDSB can rest assured knowing it has experts devoted to monitoring its network around the clock to improve its security posture.

Managed Detection and Response (MDR)

24/7/365 threat detection, compliance monitoring and SIEM and Log Management through a cloud-based SOC-as-a-Service. Customers get curated actionable alerts which we've investigated, and we provide remediation guidance.

Learn More

Managed Vulnerability and Patch Management

Continuous vulnerability scans, risk prioritization and auditable patch management to reduce security vulnerabilities and enforce change control across servers, desktops and laptops on, or off, a network.

Learn More

About Cygilant

Cygilant Inc. delivers Cybersecurity-as-a-Service to mid-sized organizations that have limited IT resources yet require 24x7x365 protection. Through its SOC and dedicated Cybersecurity Advisors that extend a customer's IT team, Cygilant provides affordable cloud-based security monitoring that hunts for threats, responds to incidents, patches systems and supplies audit artifacts for compliance mandates.

AICPA SOC

Cygilant, Inc.
60 State Street, Boston, MA 02109
www.cygilant.com