CASE STUDY

South Carolina Public Charter School District Selects Cygilant for Cyber Defense Program

Industry

Education

Challenge

Confidently reduce the risk of data breaches

More efficiently monitor for threats

Solution

Cygilant Managed Incident Detection & Response

Result

Greater network visibility into its extensive network to improve its security posture and mitigate the risk of data breaches.

Greater consistency and thoroughness to threat monitoring

Significant reduction in time and money spent reviewing logs

Expertise in delivering security best practices

Background

The South Carolina Public Charter School District's (SCPCSD) mission is to improve student learning and increase learning opportunities in South Carolina through the creation and implementation of innovative, high-quality charter schools. It strives to assist the state in achieving and maintaining academic excellence. The district has 32 schools, with a student population of more than 18,500.

For SCPCSD, it is critical for reliable security measures to be in place and that systems are properly monitored, allowing the District to be made aware of any potential issues, according to William James, Director of Technology Services, South Carolina Public Charter School District.

"As one of the fastest-growing school districts in the country with roughly 42,000 student records, we naturally have a lot of data to monitor," said James. "If that information gets into the wrong hands, it can lead to identity theft and other similar issues."

Monitoring the district's servers allows SCPCSD to spot evidence of attempted breaches before they've occurred to prevent them from happening and to block future possible cyber attacks from the same source or method. "If we catch an unknown IP address attempting to access our server and we note that it's from China, we can block that address, as well as others in that region and elsewhere globally." The problem is, explains James, "I was spending a considerable amount of time – more than five hours per week – monitoring upwards of 800 app and IP address logs."

Finding the Right Solution

The SCPCSD technology team agreed that it made sense to bring in an outside party to handle the IT security systems. They wanted a vendor to provide effective and cost-efficient cybersecurity services.

The team learned about Cygilant, a pioneer in Security-as-a-Service. Cygilant offers Cygilant Managed Incident Detection & Response, a comprehensive yet simple service for identifying threats and mitigating risks. It offered SCPCSD continuous monitoring and advanced security intelligence to meet its unique security needs. Cygilant combines best-of-breed log management and SIEM with 24x7 management and monitoring for real-time threat detection, analysis and notification, remediation guidance, and compliance auditing.

Results

Cygilant helps the SCPCSD reduce the risk of breaches by providing a continuous security monitoring program that can aggregate and correlate information across its networked systems.

"We needed a system that worked to monitor and consolidate all our logs and Cygilant delivers that function," James said. Cygilant allows the SCPCSD to collect, correlate, and analyze its vast array of network, host, application, security, and system event logs.

James explained that Cygilant was set apart from other vendors because of its unique balance of people, process, and technology to deliver an effective cyber defense managed service.

Cygilant's solution is built around the framework of Critical Security Controls, as recommended by SANS/CIS, and other compliance regulations. Cygilant provides the technology to collect and correlate raw data to assess threats in real-time. The service includes Cygilant's security experts who monitor SCPCSD's environment and provide guidance on observed incidents before a successful breach occurs. In this way, Cygilant's security experts have become an extension SCPCSD's IT team and add expert cybersecurity capabilities to the School District.

As James explains it, working with Cygilant has proven to be an excellent decision. "Given all the time I spent monitoring and assessing all our logs, it has proven to be much less costly to have Cygilant handle these important security functions. The process is more consistent and thorough than my handling it manually."

The customer service that the SCPCSD receives from Cygilant is an important added value, cites James. "Our Cygilant SOC analysts have been very helpful in providing support, including giving us reminders as needed for security best practices and answering all our questions. Overall, we're extremely pleased."

"Given all the time I spent monitoring and assessing all our logs, it has proven to be much less costly to have Cygilant handle these important security functions."

AICPA SOC
aicpa.org/soc4so

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