School Systems Rocked by Recent Cyber Attacks.

Here's the Story of One That Decided to Take Action.

At a Glance

- Centennial School District
- 5,900 students, Grades K-12
- Three Elementary Schools, Two Middle Schools, and One High School
- Located in Bucks County, Pennsylvania, the Centennial School District is comprised of Warminster Township, Upper Southampton Township, and Ivyland Borough

Core Agendas

- Evaluate Current Risk and Security Posture
- Elevate Protection Strategies
- Reduce Cybersecurity Workload
- Employ 24x7 Threat Monitoring

CRITICALSTART

Centennial School District, located in Bucks County, Pennsylvania, supports a community that traces its roots back to 1727.

> **But this school system still looks to the future through facilities such as a Planetarium, Special Experience Room and 21ST Century Learning Lab.**

Unfortunately, this type of technology brings with it 21ST century threats through hackers, both foreign and domestic, that are finding even more entry points into school networks as students and teachers move further into a remote learning environment during the COVID-19 pandemic.

Fran Watkins, Network and Systems Administrator for Centennial School District, was solely responsible for protecting the critical technology infrastructure of the district when an abrupt event in a neighboring school system triggered an extensive review of how Centennial protected its network. "A neighboring school district was hit with a **ransomware attack** and it was kind of a shock to us all," he stated. "We knew if it could happen to them, it could happen to anybody, and I was the one with the responsibility to make sure that it didn't happen on my watch. The problem was that I wear many hats and I'm a one-person shop when it comes to security, so I knew we were going to need some help."

The Search Begins...

It was reported that the school system attacked had an "an array of industry standard and reputable firewall and malware protection services to shield against infiltration attempts by cyber criminals." Watkins recognized that it was time to elevate the protection strategies of his school system beyond typical best practices if he really wanted to keep the technology infrastructure of his organization secure.

Finding a Proactive Solution

But the challenge was sifting through all the noise to find a security approach that could really protect such a vulnerable and exposed technology environment. "We were getting bombarded with a bunch of different security vendors coming out with scare tactics around what happened to the other school," shared Watkins. "They were telling us: Don't let this happen to you. But the problem with these vendors was that they had all these requirements for a limited set of security products that they would be willing to work with. When a vendor ultimately came to us that was willing to work with the technology we already had in place, and they could monitor and proactively protect our environment, 24x7, it was a no-brainer for me to go that route."

CRITICALSTART

MDR that Works for the Client, Not the Other Way Around

The vendor, CRITICAL**START**, is a Managed Detection and Response (MDR) provider that was able to deploy a staffed Security Operation Center (SOC) for Centennial School District without forcing the district to use one specific set of endpoint monitoring technology. Their technology agnostic approach to security had a definite appeal for Fran Watkins. "I didn't feel like CRITICAL**START** was pushing me to use one particular product, and I definitely appreciated that," he said. "Without that conflict of interest, I can trust their advice on how to best set up our security portfolio. And since they work with the highest-performing technologies on a regular basis, I feel like they have more leverage than I would in dealing with the vendor of a product if there was ever a problem."

The Critical Importance of Every Alert

But there was another aspect to CRITICAL**START** that's proven highly valuable to the Centennial School District since the organization decided to rely on this unique approach to MDR. CRITICAL**START** believes in a core philosophy that "every alert matters." In many typical MDR processes, critical- or high-priority alerts receive the most attention to focus resources where it's believed they will do the most good. But today's ransomware attacks often generate only a medium- or low-priority alert, opening the door for attackers to be missed entirely by legacy security methods.

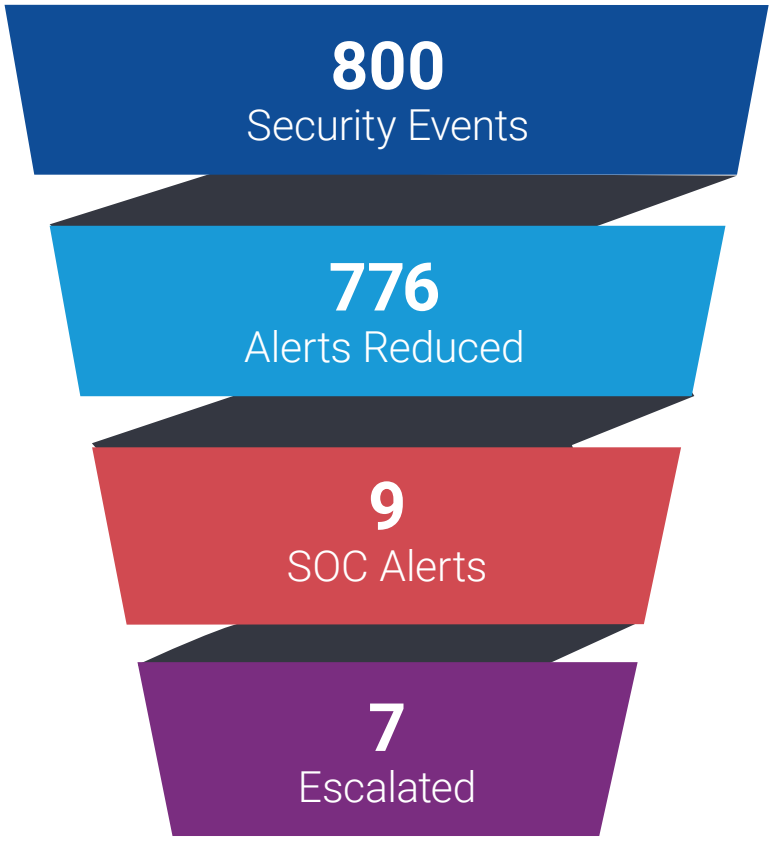
Leaving Nothing to Chance

CRITICAL**START** worked with Centennial School District to develop a trusted registry of alerts so they could identify what's normal and focus identification and remediation efforts on what's not—regardless of the priority status of the alert generated. "It seemed like other vendors would ignore what they considered a minor event, while CRITICAL**START** takes the time to figure out what's going on and respond," Watkins explained. "That was a big plus for me. And between their team and the technology, for the most part it's been hands-off in terms of my involvement when dealing with alerts."

CRITICAL**START**

Defining the Value of Trust

With the MDR team of CRITICAL**START** now identifying, isolating and mitigating any potential security breaches at Centennial School District, Fran Watkins feels that he's gained 2 hours per day that he can now refocus on other tasks for the school system. To be specific, here's what that breakdown looks like from a recent month:



The Key Takeaway

Watkins summed up the importance of this new approach to security this way: "Basically the whole thing with school districts is we don't have a lot of money," he shared. "At most schools there are small shops and the staff is doing multiple things. And for the most part we're not experts in security. With CRITICAL**START,** I now have a resource where security is all they do. I know I can reach out to them if there's a problem, but usually they're the ones coming to me with an alert and a recommended course of action. What I would say to other districts is that the value of this far outweighs any cost. And you really can't put a price on the peace of mind you get from knowing you can rely on this level of expertise."

Want more information on CRITICAL**START?**
To see how we can help, contact us at www.criticalstart.com

CRITICALSTART