School district adds MDR to enhance security after ransomware attack

INDUSTRY
Education

LOCATION
Indiana

EMPLOYEES
51-250

ENDPOINTS
1,500

"Having a team of security experts to help prevent this from happening again and teach us how to protect against it is invaluable."

— Network administrator & Coalition MDR customer

The network administrator of an Indiana school district received a seemingly routine call over a holiday weekend. An employee was unable to access the district's system through the virtual private network (VPN). He didn't think much of it — until he arrived at work the next day and couldn't log into his own computer.

Students and teachers were similarly locked out of their devices and software applications. The cafeteria was unable to process payments normally. Printers were completely down. Without access to vital technology, education within the school district came to a standstill.

Eventually, the administrator discovered a ransomware note and notified his superintendent, who immediately called Coalition.[1] The district promptly began working with Coalition Incident Response (CIR)[2] to initiate a forensic investigation. CIR instructed the admin to shut down physical servers and remove hard drives for analysis. "Within hours, we were making progress," the administrator said. "CIR was adamant about ensuring we were returning our system to a point where it would be operational again."

CIR deployed SentinelOne endpoint detection and response (EDR) to monitor the district's endpoints for further intrusion while restoring data from backups. CIR provided daily updates as all of the district's servers were brought back online. "The communication with CIR was spot on," said the administrator. "They answered any questions we had, helped us through the initial rebuild, and also carried out the detective work."

Following the attack, the network administrator acknowledged that managing 1,500 devices across seven locations was too much for his two-person team. To enhance its security, the school district decided to purchase Coalition Managed Detection and Response (MDR).[3] "Who can help protect us better than Coalition? We moved from incident response to MDR, and it was hands-off for us," said the admin. "Having a team of security experts to help prevent this from happening again and teach us how to protect against it is invaluable."

Since adopting Coalition MDR, the school district has already benefitted from our security team identifying suspicious activity on a laptop, which was quickly resolved. "Coalition MDR is like having security experts install a surveillance system at your house — and they watch it full-time."

1. The claim scenarios described here are intended to show the types of situations that may result in claims. These scenarios should not be compared to any other claim. Whether or to what extent a particular loss is covered depends on the facts and circumstances of the loss, the terms and conditions of the policy as issued and applicable law.

2. Breach response included the engagement of an incident response firm; the insured selected Coalition Incident Response, Inc., an affiliate of Coalition..

3. Coalition MDR services are provided by Coalition Incident Response, Inc.