CASE STUDY:

CONNECTICUT WATER_

ConnecticutWater

COMPANY:

Connecticut Water

INDUSTRY:

Utilities

NUMBER OF ENDPOINTS:

500

USE CASE:

Critical Infrastructure

THE CHALLENGES

- Lack of endpoint visibility
- Inability to detect signature-less threats with behavioral analysis
- Needed an EDR tool that was easy to use

OUTCOME

- Increased endpoint visibility, especially in the machines controlling the industrial control system environment
- More efficient threat hunting program by using automated hunting
- Ability to detect threats that don't have signatures by using behavioral analysis
- Faster remediation time

EXECUTIVE SUMMARY

Connecticut Water provides life-sustaining water to more than 360,000 people in 59 communities in Connecticut and Maine. This critical infrastructure provider needed greater visibility into its 500 endpoints, including the ones in its corporate network and industrial control systems environment. Carbon Black and Cylance couldn't provide the ability to detect fileless malware nor the forensic capabilities offered by Cybereason. Also, Connecticut Water required an easy-to-use endpoint detection and response (EDR) tool to increase the efficiency and effectiveness of a small security team.

THE CHALLENGE

Connecticut Water needed greater visibility into malicious activity occurring on its Windows machines. Connecticut Water's security stack included a firewall and antivirus software, but neither tool could tell the utility provider if it was under attack. For example, neither tool offered behavioral-based detection of signature-less threats. These threats include fileless malware attacks, which use PowerShell to carry out malicious activities.

"We had zero visibility into any attacks from how they began to how they ended. We didn't have a forensics program in the endpoint space," said Will Perez, cybersecurity lead at Connecticut Water.

The EDR platform that Connecticut Water purchased had to be easy to use. "Forensic analysis shouldn't be a cumbersome process", said Perez, who found that other solutions he tested "gave him the runaround" when he used them to examine endpoint activity.

THE SOLUTION

After testing Cybereason against Carbon Black and Cylance, Connecticut Water deployed Cybereason across 500 endpoints. Compared to the competitors, Cybereason proved to be easier to use, provided greater forensic capabilities, and responded to threats faster.

"If you want an EDR product that lets you respond to threats without getting frustrated over how to use it, go with Cybereason. With Cybereason, you've found your issue in 30 minutes as opposed to two hours," Perez said.

Connecticut Water has a hybrid deployment of Cybereason. A cloud instance protects the computers and servers on the utility provider's corporate network while an on-premise deployment protects the computers that operate the industrial control systems.

"[Cybereason] is protecting the computers that control the machinery and the chemicals that treat the water. If any of those computers get infected, we're in a world of hurt. As the company name implies, we supply life sustaining water," he said.

Using Cybereason also helped Connecticut Water make its threat hunting program more efficient. Before Cybereason, threat hunting was predominantly done manually. With Cybereason, the security team has been able to automate threat hunting, which has "paid huge dividends by letting us be proactive with protecting our network as opposed to being reactive," Perez said.

THE OUTCOME

Connecticut Water used Cybereason to gain greater visibility and to protect the endpoints that help provide water to nearly 400,000 people. Unlike competing products, Cybereason presented forensic information in an easy-to-use interface, allowing analysts to respond to incidents in minutes instead of hours. Cybereason presents the full attack story, providing analysts with information including the infection vector and lateral movement activity.

With Cybereason, Connecticut Water's security team is better equipped to detect signature-less threats, which can't be detected by antivirus software and firewalls. Finally, the utility provider's threat hunting program is more efficient since Cybereason allows the security team to automate hunts.

"People think that forensics is this huge activity and means getting logs from firewalls and other security appliances. But it doesn't have to be that way. With Cybereason, it isn't like that. Cybereason makes it easy to see what's going on at the endpoint," Perez said.

> "If you want an EDR product that lets you respond to threats without getting frustrated over how to use it, go with Cybereason. With Cybereason, you've found your issue in 30 minutes as opposed to two hours."

WILL PEREZ
CYBERSECURITY LEAD
CONNECTICUT WATER