CASE STUDY:

REVENUE CYCLE MANAGEMENT COMPANY_

INDUSTRY:

Hospital Revenue Cycle Management

OUTCOME

- Decreased the learning curve for junior analysts new to security
- Junior analysts could detect and remediate threats in six weeks
- Added value to the company's existing security stack

EXECUTIVE SUMMARY

A hospital revenue cycle management company's perimeter defense tools weren't providing it with enough endpoint visibility. The company wanted total visibility and an easy-to-use interface that made its junior security analysts more efficient and effective. Additionally, the tool needed to work with the company's security stack.

THE CHALLENGE

Like many companies, this organization was handling the security talent shortage by hiring people with IT backgrounds and then teaching them security. Since many of the junior analysts were new to security, the EDR tool needed to be intuitive to use. Ideally, the tool would decrease the analysts' security learning curve by automating detection and showing the complete attack story in a user-friendly interface.

The tool also had to provide deep endpoint visibility and augment the company's other security products, which included antivirus software and an intrusion detection system. While these products were essential to the company's layered approach to security, they didn't provide enough information on malicious endpoint activity.

The organization needed an EDR tool that:

- **Was easy to use for junior analysts who were new to security**
- **Helped junior analysts quickly detect and remediate threats**
- **Offered greater endpoint visibility and worked with its existing security tools**

THE SOLUTION

Six weeks after using Cybereason, junior analysts were able to detect and remediate threats using the tool's interface, which presented them with an entire attack story. By seeing what machines were infected, if the attacker moved laterally to other computers and if there was communication to command-and-control servers, among other information, they were able to take immediate action.

> "Cybereason makes it very easy to know what you're looking for. When it comes to remediation, blacklisting and whitelisting, you can do it all in seconds. The ability to protect yourself in seconds makes a difference."

ANALYST
WORKED IN COMPUTER NETWORKING

Cybereason's ease of use helped less experienced analysts swiftly handle the fallout after hackers placed a backdoor in CCleaner, a popular maintenance and file cleanup program. This incident occurred 10 weeks after two analysts with IT experience joined the security team.

"The first thing I did was grab the hashes and put them in Cybereason. We were able to catch a lot that day," said the analyst.

Additionally, junior analysts used Cybereason to get more value from the other security tools they used. For example, when another security product triggered an alarm, they used Cybereason to investigate the machine's history.

"It's a fantastic complementary tool as well as a stand-alone tool. I like to use it for hunting queries. It's really pretty amazing how you can get so much visibility in your environment," said the analyst.

THE OUTCOME

The organization reduced the amount of time spent teaching new analysts about security while gaining deeper endpoint visibility. In less than two months, security team members with IT backgrounds were using Cybereason to quickly detect and stop threats, including handling a major security incident. Plus, Cybereason provided additional value to the company's security stack.

> "There isn't any application but Cybereason that allows me to have visibility like this. You get the how, the what and the when."

JUNIOR ANALYST