BlackBerry CYLANCE

CASE STUDY HEALTHCARE

Satellite Healthcare Takes on Cybersecurity

INDUSTRY
Healthcare

CHALLENGES
- Identifying and remediating all pre-existing security breaches
- Ensuring uninterrupted access to electronic medical record (EMR) and clinical desktop systems healthcare professionals rely upon to render quality care
- Assessing and baselining the company's overall security posture and risk profile

SOLUTION
- Leveraging the experience and best practices expertise of Blackberry Cylance compromise assessment consultants

SATELLITE HEALTHCARE

The Company

Satellite Healthcare has been among the U.S.'s leading not-for-profit providers of kidney dialysis and related services since 1974. Through its affiliated services, Satellite WellBound, Satellite Dialysis, and Satellite Research, Satellite Healthcare provides unparalleled early patient wellness education, personalized clinical services, and a complete range of dialysis therapy choices. In addition, Satellite Healthcare has a well-recognized, enduring commitment to philanthropy and community service, from funding millions of dollars in research grants to sponsoring kidney programs nationwide. Satellite Healthcare is committed to advancing the standard of chronic kidney disease care so patients can enjoy a better life.

The Situation

When Lokesh Yamasani joined Satellite Healthcare as director of information security in November 2017, his first priority was to ensure that no previous incursion might threaten the firm's ability to render quality care. "Most of our patients are contending with chronic kidney disease," says Lokesh Yamasani. "We can't afford to delay a dialysis treatment because an attack has compromised the confidentiality, integrity, or availability of our EMR and clinical desktop systems. When patients miss appointments, their mortality rates increase. For us, a breach can mean the difference between life and death."

Lokesh Yamasani had heard glowing reports from CISO colleagues about the effectiveness of the BlackBerry Cylance AI Platform™. However, he was not yet aware that the company also offered a portfolio of world-class incident response and forensics consulting services. According to Lokesh Yamasani, "When I met with the technical director for the compromise assessment team, I was immediately impressed by his knowledge and expertise, and by the AI-based methodology and tools his team uses to assess environmental risks, identify indicators of compromise, and trace ongoing threat actor activity. It soon became evident that the compromise assessment was a perfect fit for our needs."

The Process

The compromise assessment (CA) kicked off in mid-February 2018, a scant three months after Lokesh Yamasani took the helm as Satellite Healthcare's cybersecurity lead. Every CA engagement proceeds through three distinct phases, starting with an initial assessment, followed by a targeted assessment, and culminating in a forensic assessment. In the final phase, the consulting team produces a comprehensive report that documents every instance of malware, exfiltration, sabotage, command-and-control activity, user-account exploitation, persistence mechanisms and suspect network, and host-and-application configurations. The CA team also issues risk-prioritized recommendations for preventing further incursions and strengthening the organization's overall security posture. All of these assessments and recommendations begin with a comprehensive data collection exercise.

According to the BlackBerry Cylance CA engagement manager, "In some environments, we install the CylancePROTECT and CylanceOPTICS EDR agent to identify malware and hunt for threats. However, our AI-based methodology doesn't require us to drop hardware or software into an environment to produce actionable results quickly. Instead, we can simply utilize native operating system scripts to collect the raw data we need to identify IOCs and perform forensic analysis. At Satellite Healthcare, these were simple Windows batch files that ran for five to 10 minutes on each target system and then terminated, leaving behind no traces except for the data forwarded to our team for off-site analysis."

In all, the team collected roughly 40,000 hashes from each of the 1,700 Windows hosts in scope for the CA. According to the CA engagement manager, "We hash all of the system locations where malware is most commonly found, including system32, app data, and download folders, as well as scheduled tasks and currently running processes."

With data in hand, the CA team set to work in earnest. One of their first steps was to submit the hashes to CylanceINFINITY™, the highly intelligent data analysis platform BlackBerry Cylance uses to construct the machine learning models that power CylancePROTECT® and CylanceOPTICS™. According to the CA engagement manager, "Within milliseconds, we can determine which threats are present, the categories they belong to, and their degrees of severity. If we find an active IOC, we immediately inform the client and assist with remediation before continuing our analysis. All of the malware and PUPs we identify are prioritized by risk level and listed in an addendum to our final report."

The user activity data collected by the CA team is also subjected to a common machine learning method known as clustering, in which a decision tree algorithm examines hundreds of features of each user account and the environment in which it operates. This enables the team to identify groups of users that exhibit similar behavior patterns and spot anomalies that require further investigation. "For example, we expect to find employees from the IT department in a cluster of accounts utilizing domain administrator privileges," said the CA engagement manager. "However, if one of these cluster members works in accounts payable, we would consider this an anomaly and immediately begin an investigation to determine whether that end-user is an adversary or if their system has been compromised."

According to Lokesh Yamasani, "Some of my colleagues were initially concerned that the CA might disable the fragile medical devices connected to our clinical desktops or impose undue burdens on our IT team. However, we had no system issues whatsoever and my team spent less than 40 hours participating in the three-month assessment. From start to finish, we found the CA process to be both efficient and transparent."

2,000
EMPLOYEES

1,800
ENDPOINTS PROTECTED

240
SERVERS PROTECTED

The Results

The BlackBerry Cylance CA team completed its analysis in mid-May 2018 and formally presented its findings in June. According to Lokesh Yamasani, "The final report was quite comprehensive and included specific recommendations for strengthening our overall security posture. I worried that we'd discover ongoing command-and-control or APT activity, but the CA largely gave us a clean bill of health. We were encouraged to do a better job of patch management and continue educating and motivating end-users to practice good cyber hygiene. However, these are the kinds of security challenges one finds at almost every organization. Frankly, I was pleasantly surprised we had done so well."

Shortly afterwards, Lokesh Yamasani was asked to meet with Satellite Healthcare's board of directors to present his own assessment of the company's cyber risk profile. "Our board is very tech-savvy, which makes my job easier since the members understand the inherent vulnerabilities of our clinical applications and the challenges we face in defending such a large attack surface. Ultimately, however, they want more than a technical dissertation. They expect me to contextualize cyber risks in terms of their potential impact on our patients and our overall mission to provide quality care. The CA gave me the data I needed to provide that assessment with confidence and credibility and to set clear priorities for future investments. I feel very encouraged about where we are now and where we're headed," he concluded.

+1-844-CYLANCE
sales@cylance.com
www.cylance.com

BlackBerry | CYLANCE

20190610-0319