CUSTOMER STORY

RAPID7

Clatterbridge Cancer Center

Trusts Rapid7's SIEM to Keep Patient Records Secure

Products

InsightIDR

InsightConnect

Industry

Healthcare

Overview

The Company

The Clatterbridge Cancer Center is one of the UK's leading cancer centers providing highly specialized cancer care to more than 2.4 million people in Northwest England. The Center has a unique multi-site care model consisting of three main sites, four systemic therapy sites and 15 outpatient centers, in addition to providing chemotherapy in the home and workplace. As one of the largest NHS providers of non-surgical cancer treatment, Clatterbridge is a tertiary cancer center, seeing patients who have been diagnosed and referred by other hospitals.

The Challenge

The Center's three-person security team is responsible for protecting confidential medical records, a task compounded by the fact that patient records are shared with other hospitals. "We're one of about 35 trusts which are linked together through our patients and patient records. Thousands of people who work in healthcare, education, government, and councils connect to our site."

"The most pressing challenges are phishing and user errors. We can be as secure as can be, but at the end of the day it all comes down to our staff," explains Richard Pilkington, IT Security Manager.

The Solution

From Out-of-the-Box To Actionable Data Within 48 Hours

To secure their data, Pilkington looked to a SIEM solution and chose Rapid7 InsightIDR, a cloud-native SIEM which enables his team to detect and respond to security incidents faster.

Pilkington and Andy Kilbane, Digital Systems Security Specialist, began the search for a SIEM by identifying which parts of their infrastructure they needed to secure. The Center has a multi-tenanted environment, about 2,500 endpoints, including medical devices, 300 servers and 1650 users. Clatterbridge has a SDA (software defined architecture) Cisco network.

“We broke it down into a number of categories, including endpoint management, server management, medical devices, records management, access and authentication and privileged access management,” states Pilkington. “We need to monitor all those things and that’s where InsightIDR came in. Basically, everything feeds into InsightIDR and gives us a one stop shop where we get alerted to anything that happens.”

Kilbane adds, “We looked at quite a few SIEM solutions. But when we saw InsightIDR, it seemed easy and powerful behind the scenes. And we were right. It took less than 48 hours for us to go from out of the box to up and running with quite a few of our critical systems logged in. The documentation available with InsightIDR was brilliant.”

Alerts Provide Unparalleled Visibility

For the security team, the most important feature of InsightIDR is the alerts because they provide visibility into things they wouldn’t have seen before, especially around active directory. “InsightIDR does a really good job of weeding out what is an actual alert,” notes Kilbane. “When we do get an alert, we’re able to react to it quickly. Before InsightIDR, it was a much more involved and inefficient process. Now, with InsightIDR we can see everything under one umbrella.”

Pilkington recounts one instance where one of their service desk team members had been reactivating accounts on his own. “With the information from the Active Directory alert, I was able to spot it and reach out to his manager. Turns out he wasn’t following protocol for reactivating accounts, but we were able to fix it. That was a major success for us.”

> “
>
> **When we saw InsightIDR, it seemed easy and powerful behind the scenes. And we were right. It took less than 48 hours for us to go from out of the box to up and running with quite a few of our critical systems logged in.**
>
> Richard Pilkington,
> IT Security Manager

InsightIDR Data Meets the Needs of a Diversity of Stakeholders

The reports InsightIDR generates for the Clatterbridge team provide a complete picture of breaches and security incidents over a 30-day period. The data is summarized into monthly reports presented to the organization's Digital Security Committee which is made up of members representing various departments within the hospital organization. The net effect is that the organization can track breaches accurately and show improved performance thanks to InsightIDR.

All NHS Trusts must have a DSPT (Data Security and Protection Toolkit) audit. "We received the highest rating assurance we could from the auditors and that's because of InsightIDR," states Pilkington. "I am responsible for all the reports, the graphs, the presentations, and the dashboards, so the data InsightIDR gives me for my side of the job is fantastic. And InsightIDR has been a godsend in terms of giving us a lot of data with regards to ISO 27001," states Pilkington. "It's helping us work towards 27001 certification."

Keeping Patient Data Safe Is Patient Care

"Keeping patients' data safe is patient care in its own way," states Pilkington "You don't want to be on a medical device that's suddenly attacked by a virus or stops working. We're not in that position, but hospital budgets are being reduced year on year every year and it can be hard to justify investing in cybersecurity vs medical personnel. But if you are attacked, you see the fallout from it and the money it costs to recover if you ever do recover."

"The bottom line is that InsightIDR gives us broad assurance that we're in a safe place," Pilkington says. "So, we can go to our board and say, "Look, this is where we're at. This is what we're doing. This is how many breaches we've had over the last month. And that gives the board and all our stakeholders assurance that we're in a safe environment with regards to cybersecurity. It's made life a lot easier."

About Rapid7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open source communities and cutting-edge research–using these insights to optimize our products and arm the global security community with the latest in attackers methods. Trusted by more than 10,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.

RAPID7

PRODUCTS

Cloud Security
XDR & SIEM
Threat Intelligence
Vulnerability Risk Management

Application Security
Orchestration & Automation
Managed Services

CUSTOMER SUPPORT

Call +1.866.380.8113

To learn more or start a free trial, visit: https://www.rapid7.com/try/insight/