Recorded Future®

Highmark Health Accelerates SOC Automation with Recorded Future

National healthcare insurer and provider takes a proactive approach to security with real-time threat intelligence insights.

HIGHMARK HEALTH

Goal: Identify threats early to prevent attacks with effective IOC prioritization and security workflow automation.

Challenge: Limited internal resources resulted in an inconsistent, reactive approach to threat intelligence.

Solution: Recorded Future threat intelligence integrated with data and insights from Health-ISAC (Information Sharing and Analysis Center)

Outcomes:

- Automated IOC triage
- Faster, more confident decisions based on timely and accurate threat intelligence
- Proactive alerts for earlier identification of threats and faster response and resolution
- Increased productivity and efficiency across threat intelligence operations

> **“Health-ISAC and Recorded Future are two of our most valuable threat intelligence partners — and this integration has only made that relationship stronger. If your leadership is pushing for more automation for your SOC, this integration is an absolute must-have!”**
>
> *Katie Schwalen*
> *Team Lead, Threat Management*

Challenge

A Reactive Threat Intelligence Approach Puts Healthcare Systems and Data at Risk

Today’s healthcare organizations face cyber threats from every angle. Their expanding ecosystems of connected medical devices and systems hold a treasure trove of valuable data — from patient records and personally identifiable information to biometrics and intellectual property — making them attractive targets for adversaries. Vulnerabilities, ransomware threats, and patient data theft are just a few of the many concerns keeping the security professionals at Highmark Health up at night.

“Before 2020, our threat intelligence program was mostly a reactive function — when something big happened, we’d create a report, but it was inconsistent and difficult for one dedicated team member to manage, let alone scale,” explains Ed Marrow, Manager of Team Information Risk Management at Highmark Health. “But in the wake of COVID-19, everything changed and there was an urgent need for timely, accurate threat intelligence.”

Solution

Teamwork and a Powerful Integration Take Shared Sector Intelligence to the Next Level

Several teams across the organization’s Security Operations Center (SOC) banded together. They created a “SWAT Team,” led by Threat Management Team Lead Katie Schwalen, to mature the program and produce actionable, high-value threat intelligence to proactively protect the Highmark enterprise.

“One of our main objectives is to cultivate and maintain intelligence-sharing relationships both inside and outside the healthcare industry,” explains Schwalen. Like many healthcare organizations, the Highmark Health team relies on Health-ISAC, a large community of critical infrastructure owners and operators within the sector, for targeted healthcare intelligence.

“Security as a whole can be a very lonely business,” adds Marrow. “As you work in your SOC, you’re not seeing what else is going on. Talking and sharing with other security professionals is essential for informed decision making and peace of mind — after all, we’re all in the trenches together.”

The opportunity to layer Recorded Future’s real-time threat intelligence — which comes from an unrivaled number of sources across the open web, dark web, technical sources, and original research — and layer it over shared H-ISAC insights was a no-brainer for the Highmark team.

Integrating Recorded Future intelligence with H-ISAC intelligence empowers the Highmark team to amplify their impact and proactively defend their network by:

- Enriching insights from the Health-ISAC community with real-time, actionable threat intelligence
- Quickly transforming raw data in the H-ISAC WeeSecrets chat into complete, contextualized intelligence that drives fast, confident decisions
- Automating manual IOC triage and speeding decision making
- Identifying, tracking, and better understanding prolific threat actors
- Gaining visibility across the broader threat landscape, such as threats on the geopolitical stage

> **“Recorded Future provides us with highly customizable threat intelligence that's unique to our environment. We can dig into the platform, put our hands on alerts we're seeing, and enrich the intelligence we receive from Health-ISAC and vice versa — it's been a huge win for us."**
>
> *Katie Schwalen*
> *Team Lead, Threat Management*

Results

Actionable Intelligence Drives Proactive Protection from Targeted Threats

“In times of crisis, the ability to combine and corroborate data from both Health-ISAC and Recorded Future has proven to be invaluable,” says Schwalen.

For example, in October 2020, the FBI issued an alert to US hospitals and healthcare organizations of an imminent threat of Ryuk ransomware attacks. Highmark immediately activated its Cyber Incident Response team to harden systems at its hospital locations and affiliate entities. “Threat intelligence from Recorded Future was imperative during this incident — from real-time alerts on Ryuk and Trickbot malware indicators, to automated IOC ingestion, to webinars and prescriptive guidance for defending our organization,” notes Schwalen.

“Recorded Future provides us with highly customizable threat intelligence that's unique to our environment,” she says. “We can dig into the platform, put our hands on alerts we're seeing, and enrich the intelligence we receive from Health-ISAC and vice versa — it's been a huge win for us.”

She concludes, “Health-ISAC and Recorded Future are two of our most valuable threat intelligence partners — and this integration has only made that relationship stronger. If your leadership is pushing for more automation for your SOC, this integration is an absolute must-have!”