

Renowned Medical Center Streamlines Security Incident Response Management



Company Profile

The University of Rochester Medical Center (URMC) is one of the nation's top academic medical centers and the centerpiece of the University's health research, teaching, patient care, and community outreach programs. Its mission is to use education, science, and technology to improve health—transforming the patient experience with fresh ideas and approaches steeped in disciplined science and delivered by health care professionals who innovate, take intelligent risks, and care about the lives they touch.

Challenges

Healthcare is one of the most highly regulated industries in the United States, with constantly evolving Federal and local regulatory and compliance mandates, including HIPAA Security, HIPAA Privacy, Breach Notifications, HITECH, NPDB and more.

URMC is committed to the sanctity of patient health information. The information security team wanted to develop, implement, and rapidly evolve a program that could withstand shifts in regulatory requirements without sacrificing URMC's status as a premiere medical and research facility.

While compliance-related incidents created regulatory challenges, URMC also recognized that compliance wasn't enough to ensure the proper treatment and protection of patient and other sensitive data. Vulnerability identification and management plays a huge role in this process as well. But gaining this risk intelligence in a format that was actionable was challenging due to the wide scope of deployments on the medical centers network, even using internal penetration testing tools.

Over the last five years, URMC has garnered more than \$1.38 billion in biomedical research, landing the University of Rochester School of Medicine and Dentistry in the top one-quarter of U.S. medical Centers in federal research funding. Anchored by Strong Memorial Hospital, 800-bed, University-owned teaching hospital; consistently ranked among "America's Best Hospitals," according to U.S. News & World Report.

Solution

URMC chose Rsam to help them automate and streamline their incident management process, allowing them to detect, monitor and resolve incidents quickly thereby maintaining compliance.

Rsam's Security Incident Risk Platform (SIRP) offered flexibility and easy integration into their existing infrastructure, including their Security Information and Event Management (SIEM) product.

Today URMC uses the Rsam platform and customizable reporting functionality to monitor, detect and remediate important compliance-related issues and track them to complete remediation.

In addition, URMC uses the flexibility of the Rsam Security Operations Analytics and Reporting Platform (SOAR) to categorize their vulnerabilities and prioritize them with a risk-based approach.

URMC conducts comprehensive vulnerability scans of their environment, leveraging Rsam to merge vulnerability data, asset management data, and packaged exploits available in MetaSploit and Exploit DB. The Rsam platform automatically adjusts the priority of a known vulnerability if an exploit is available and tracks the organization's response toward remediation.



Benefits

- Quickly get a comprehensive view of compliance related-incidents.
- Continuously monitor vulnerability and risk.
- Get actionable intelligence to mitigate security and compliance threats quickly and efficiently.

Leveraging Rsam, URMCM has Gained:

- More accurate risk-based remediation process.
- Single repository of incidents.
- Decrease in the number of outstanding action items by system owners.
- Reduction of 50% in response time to vulnerabilities.

About Rsam

Rsam is a leader in the field of Governance, Risk, and Compliance (GRC) solutions and is the fastest time-to-value GRC provider. The Rsam platform delivers unparalleled flexibility for companies to leverage out-of-the-box solutions and "Build Your Own" (BYO) applications for a wide range of GRC functional areas, including audit, business continuity management, compliance, enterprise risk, IT risk, incident management, operational risk, policy management, security risk intelligence, vendor risk management, regulatory change management and more. Learn more about Rsam at <http://www.rsam.com>

