

SCALR™ XDR CyberSOC for Large Healthcare Organization



Client Profile

- \$3 billion healthcare system
- 7 hospitals, 1583 beds
- 358 outpatient sites
- 2,600 physicians, 12,000 staff

About SRA

Security Risk Advisors (SRA) provides cybersecurity consulting and 24x7x365 operations services to organizations across all industries, with a focus on Fortune 500 and Global 1000 clients.

SRA does not resell for profit and is neutral to recommend best-fit controls and solutions. SRA demonstrates thought leadership in cutting edge security topics, presenting at several industry events each year, and developing free tools for the security community.

Contact Us

Security Risk Advisors
1600 Market St., Suite 3000
Philadelphia, PA 19103

Website: <https://sra.io>
Email: info@sra.io
Phone: (215) 867-9051

Challenge

- Large Midwest Healthcare Provider had been experiencing growing CyberSOC costs from their MSSP due to technology and cloud consumption.

Solution

- SRA's SCALR™ XDR service is built on the Microsoft Sentinel ecosystem and is available for organizations to use regardless of their current Microsoft footprint.
- SCALR™ architecture allows for ingestion of any cloud based EDR endpoint and network, logs into a cost-efficient data lake with intelligent SIEM routing and uses built-in SOAR capabilities for efficient response to common notables.
- SRA provides expert 24x7 monitoring response along with their signature Purple Teams testing and benchmarks.
- More at <https://SCALR.sra.io>

Benefit

- SCALR™ XDR replaced a legacy SIEM with a modern detection ecosystem complete with SRA's playbooks. This is a lasting capability because the XDR is deployed in the client's own tenant and enables the benefits of modern technologies like SOAR and Data Lake. If the client decides to resource its 24x7 staffing internally, they will retain the system that is built and working.
- SRA pioneered the inclusion of Purple Teams in its SCALR™ XDR service. This approach brings transparency to visibility gaps and promotes knowledge sharing and joint ownership of defense success. Quantitative benchmarked metrics enable the client's security leadership to communicate the journey of a threat-driven program with progressive MITRE ATT&CK alignment.
- Since implementing SCALR™ XDR with SRA, the client's savings have been dramatic – **saving over 50%** off their previous legacy on-prem spend and nearly 85% like-for-like against the most well-known cloud hosted SIEM solution on the market. This efficiency has allowed the client to invest more in other security programs.
- **SRA expects most XDR users will achieve about 50% savings.**