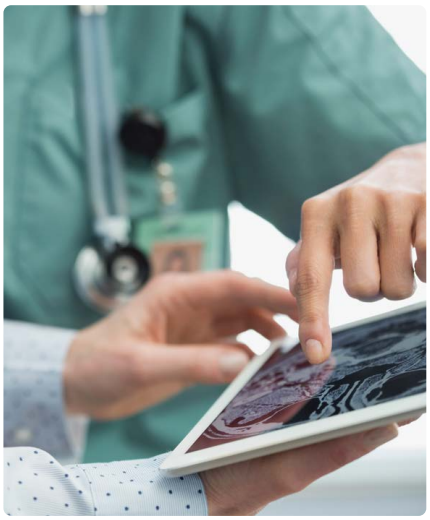
Major Healthcare Company

ArcSight Intelligence neutralizes insider threats and prevents sensitive data theft.



Move from Hypothesis-Based Threat Hunting to Analytics-Driven

With over 12,000 internal users accessing sensitive patient data, this organization had to face the reality of potential insider threats to their data security. Its security operations center (SOC) already deployed hypothesis-based threat hunting where an actionable hypothesis is created, executed, and tested to completion. This method aims to connect the dots, determine what's normal and what's not, and identify anomalies. Its Chief Information Security Officer (CISO) explains what he would prefer: "Instead of managing a flood of distracting false positives derived from hypothesis-based threat hunting, we felt we could augment our hunting efforts better by creating more accurate behavioral intelligence-based hypotheses."

"ArcSight Intelligence found a successful authentication to a rarely used server, which attempted to access servers globally. Narrowed down to an administrator who was dismissed as a result, ArcSight Intelligence then spotted the same account trying to re-authenticate after the individual had been terminated. All attempts were identified and neutralized."

Chief Information Security Officer
Large Healthcare Organization

CyberRes ArcSight Intelligence provides a contextualized view of the riskiest behaviors in the enterprise and gives SOC teams the right tools to visualize and investigate threats. It links unusual behavior with real threats by using statistical probability and unsupervised machine learning to identify the most suspicious entities.

Neutralized Insider Threat

Following its implementation in a hosted cloud environment ArcSight Intelligence was able to identify and neutralize an insider attempt to access sensitive data in an EMC application. An administrator exploited a vulnerability on a server which, if successful, would have resulted in data theft.

The organization plans to expand the data sources into ArcSight Intelligence to broaden its coverage.

At a Glance

Industry

Healthcare

Location

USA

Challenge

Find a more efficient method to identify insider threats through security anomalies in a large organization

Products and Services

CyberRes ArcSight Intelligence

Success Highlights

- Identified and neutralized sophisticated insider attack
- Analytics-driven threat hunting is more efficient and effective
- Unsupervised machine learning dramatically increases threat hunting productivity