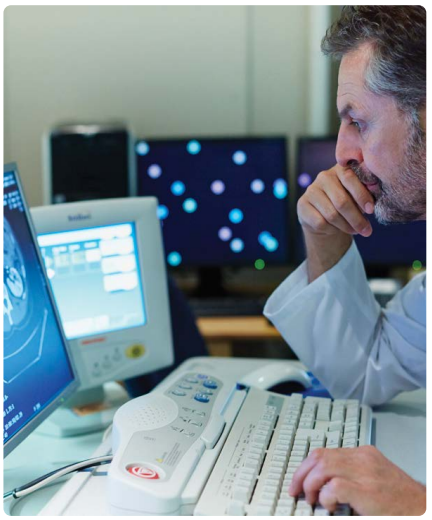
Large Healthcare Organization

ArcSight Intelligence prevents security breach in sensitive patient data.



Protecting Sensitive Patient Data from Cyber Attacks

Aa a healthcare provider this organization holds very sensitive patient data and is subject to strict regulatory compliance, such as HIPAA. Its Chief Information Security Officer (CISO) is very aware of the security threat posed: "We need the ability to detect and stop advanced attacks on our corporate network. There is also the very real risk of insider threats that we must address. Although our Security Operations Center (SOC) does a great job, we wanted to boost our productivity by focusing our analysts on investigating the threats that pose the highest risk to us."

"ArcSight Intelligence found a previously dormant active GUEST account which had not been locked despite failing hundreds of authentication attempts, all made outside of working hours. It attempted to access a classified server, and our team was able to neutralize the activity before any breach occurred."

Chief Information Security Officer
Large Healthcare Organization

CyberRes ArcSight Intelligence empowers security teams to find and respond to previously unknown threats—exactly what is needed in this situation. Its flexible deployment options aligned with the cloud vision for this organization and the team was particularly excited about ArcSight Intelligence's unsupervised machine learning (ML) capabilities. Leveraging ML, "unique normal" baselines are learned, i.e., a digital fingerprint of each user or entity which can be continuously compared to itself or peers. This approach to behavioral analytics enables security teams to detect traditionally difficult-to-find threats.

Successful Attack Prevention with ArcSight Intelligence

Following its implementation, ArcSight Intelligence was able to identify and neutralize an external attacker, a great result for the organization.

The organization plans to continue leveraging ArcSight Intelligence to augment and streamline its security team's efforts.

At a Glance

Industry

Healthcare

Location

USA

Challenge

Detect and stop advanced cyberattacks and insider threats before breaches occur, while complying with strict data privacy regulations

Products and Services

CyberRes ArcSight Intelligence

Success Highlights

- Identified and neutralized an attack preventing a security breach
- Improved threat hunters' efficiency through machine learning capabilities
- Cloud deployment in line with corporate IT policies