

Financial Services Organization

ArcSight Intelligence protects business-critical trading algorithms.



Boost Productivity of a Small Security Team

In a highly regulated industry such as financial services protecting sensitive data is key. In this organization's case they particularly wanted to protect specific trading algorithms which were the source of differentiating intellectual property (IP). Its Security Architect recognized another challenge: "We have a small security team in place with many different priorities. I understand the need for proper anomaly detection, and needed a solution that gave

"ArcSight Intelligence identified a local service account used to successfully access certain resources, even though most of its authentication attempts failed. We believe this was a reconnaissance activity that could have resulted in data theft. Thanks to ArcSight Intelligence this is currently under investigation."

Security Architect
Financial Services Organization

us real analytics, rather than the 'black box' messages we received from some vendors. Furthermore, I had tried Open Source solutions and found them to be too resource intensive. We needed something that was easy to maintain."

With an analytics-led approach, ArcSight Intelligence by OpenText™ uses a process of baselining and scoring to boost the efficiency and speed at which security teams detect, triage, investigate, and respond to threats. An intuitive, web-based dashboard allows users to quickly and easily determine which alerts present the greatest potential risk.

ArcSight Intelligence Identifies and Neutralizes Unknown Threat Vectors

ArcSight Intelligence was deployed in a SaaS model for worry-free maintenance and support. Early analytical results identified previously unknown threat vectors with several active service accounts connected to retired target applications. These threats neutralized and investigated; the organization can rest assured its IP is safe.

The organization plans to expand ArcSight Intelligence data sources and profile every network device for greater coverage.

At a Glance

Industry

Finance

Location

USA

Challenge

Deploy sophisticated anomaly detection to protect confidential trading algorithms that are central to the success of the business

Products and Services

ArcSight Intelligence

Critical Success Factors

- SaaS deployment for ease of maintenance and support
- Analytics-led security approach boosts productivity of small team
- Identified and neutralized previously unknown threat vectors