opentext™ | Cybersecurity

Case Study

High Tech Manufacturer

ArcSight Intelligence improves insider threat program by prioritizing threat hunting through data analytics.

Protecting Valuable IP from Theft

With over 50,000 employees and valuable Intellectual Property (IP) to protect, this organization opted for an advanced insider threat program. As data theft cases were becoming more commonplace, the team's Data Security Analytics Manager decided a more sophisticated solution was required. They were using Securonix, but as their data sources grew, they wanted to use analytics to detect insider threats and targeted external attacks, in the form of data theft. ArcSight Intelligence by OpenText™ had the capabilities to meet their needs and it replaced their Securonix implementation.

ArcSight Intelligence empowers the security team to preempt elusive attacks. With contextually relevant insights from behavioral analytics, analysts can quickly zoom in on what truly matters in their battles against complex threats such as insider threats and advanced persistent threats (APT).

Leveraging Analytics to Prioritize Threat Hunting

Multiple data types, including DLP endpoint data, Active Directory, email and source code repository logs, flow into ArcSight Intelligence's unsupervised learning models. The team has also introduced event criteria and automated user importance tuning, in particular for employees who are due to leave the organization. Examples of actions that automatically trigger investigation are data exfiltration via email, unusual access to source code repositories, unusual data saved to a removable drive, and others. These additional inputs finetune the analytical results based on a company-specific context and drive the threat hunting priorities.

At a Glance

Industry

Manufacturing

Location

USA

Challenge

Deploy data analytics to protect valuable IP in the face of targeted external attacks and insider threats

Products and Services

ArcSight Intelligence

Success Highlights

- ArcSight Intelligence replaces Securonix
- Wide variety of data sources feed into unsupervised learning models
- Automated user importance tuning highlights risk of impending departures

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.