opentext™ | Cybersecurity

Case Study

Global Manufacturer

ArcSight Intelligence proof-of-concept detects and remediates brute force attack in process.

Complementing CrowdStrike with ArcSight Intelligence

With a global business model, cybersecurity is critical for this manufacturer. It already deployed CrowdStrike Endpoint Detection and Response (EDR) but felt it needed more intelligence around its threat management. To complement its CrowdStrike efforts, the team started a 30-day free endpoint threat detection project with ArcSight Intelligence by OpenText. With thousands of globally distributed endpoints to protect, the organization was interested in how ArcSight Intelligence leverages machine learning to compile data which is then scrupulously reviewed by the Cybersecurity OpenText™ threat detection team. Much to their surprise multiple endpoint anomalies were discovered. It was apparent there was a brute force attack in process on a server, with the attacker moving laterally to other machines in the organization. The Cybersecurity team delivered a prioritized report of action items along with access to the ArcSight Intelligence platform.

Minimized Risk of Exposure and Eliminated Immediate Threat

Using ArcSight Intelligence, the detected threats were given a 'threat grade' to help prioritize them. After the initial data review the organization's cybersecurity team took swift action to minimize the risk of exposure, not only to internal endpoints, but also to prevent possible attacks outside of their immediate environment, including associated organizations.

After a 48-hour internal remediation period addressed and implemented the actionable items to eliminate the immediate threat, ArcSight's threat hunting team further engaged with the organization. During this time, they provided additional insight and guidance to prevent the next level of recognized threats. The organization's cybersecurity team is now in the process of implementing ArcSight Intelligence for future use.

At a Glance

Industry

Manufacturing

Location

USA

Challenge

Protect thousands of globally distributed endpoints from unauthorized access

Products and Services

ArcSight Intelligence

Success Highlights

- Identified and remediated a server attack in process
- Actionable and prioritized data delivered through machine learning capabilities
- Minimized risk of exposure

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.

768-000067-002 | O | 08/23 | © 2023 Open Text