Major Financial Services Organization

Astonishing POC insight leads to ArcSight Intelligence for CrowdStrike implementation to combat insider threat.

Who Touches Our Data and for What Purpose?

These are vital questions that the Chief Operating Officer of this organization asked his security team. Despite having an advanced security posture operated through a leading MSSP and CrowdStrike to protect against external threats, the customer identified a need for additional visibility to protect its sensitive customer data from insider threats. The customer described the challenge as: "With 1000s of employees, our systems log over 6.6 billion security events per year making manual inspection difficult, expensive, and time-consuming. We already have one full-time resource manually checking emails for any potential insider threat. This is obviously not a scalable process, and it relies on inherently error-prone humans. In our highly regulated industry, the risk of reputational damage is just too high for us, so we looked for a solution that would complement our existing security infrastructure and focus specifically on insider threats."

"Adding ArcSight Intelligence for CrowdStrike and the threat hunting service to our CrowdStrike and MSSP infrastructure significantly reduced our risk of reputational damage by protecting our sensitive customer data."

Security Manager
Large Financial Services Organization

Actionable Insights through ArcSight Intelligence POC

Extensive market research led the customer to ArcSight Intelligence for CrowdStrike, delivered by CyberRes. This is designed to leverage an existing CrowdStrike endpoint security investment. Delivered as a Software-as-a-Service (SaaS) solution, no additional endpoint agents are required, and it will simply ingest the CrowdStrike event data and run advanced analytics against it. It is a SaaS-based approach offering lower cost of ownership and reducing the burden of maintenance and administration. No additional staff was needed, and because it is operated on a subscription basis, it has no Capital Expenditure (CapEx) impact. This unsupervised machine learning solution optimizes over time as it constantly learns what 'normal' means for every employee, machine, and authentication source. ArcSight Intelligence for CrowdStrike

At a Glance

Industry

Finance

Location

Multinational

Challenge

Strengthen an already robust security posture with insider threat detection without adding to the burden of an overstretched security team

Products and Services

ArcSight Intelligence for CrowdStrike

Success Highlights

- Serious insider threats highlighted through POC
- 3-month full ROI
- Improved efficiency through advanced analytics
- SaaS delivery for maintenance-free approach
- Integrated insider threat detection with comprehensive existing security infrastructure

> **"Our security posture has improved, and the convenient ArcSight Intelligence for CrowdStrike SaaS model provides this without adding any burden to our security team or administration staff."**
>
> **Security Manager**
> Large Financial Services Organization

Contact us at **CyberRes.com**
Like what you read? Share it.

has an optional threat hunting service with a proven track record of using ArcSight Intelligence for CrowdStrike to find elusive threats that hide in an organization.

The organization decided on a Proof-of-Concept (POC) to test whether ArcSight Intelligence for CrowdStrike was the right solution for them. A subset of informed staff were included in the POC, which ran for 45 days. During this time, ArcSight Intelligence for CrowdStrike consumed 24 million events, which identified over 90,000 deviations from normal behavior. From these deviations, ArcSight Intelligence for CrowdStrike identified a few high-quality threat leads for threat hunters to investigate further for malicious behavior.

'We unfortunately discovered that users were copying sensitive information onto a USB device," says the security manager. "We identified numerous dubious applications, as well as failed login attempts, high volumes of file creations, and exceptional numbers of processes. This led us to believe that a specific financial advisor account may have been performing internal reconnaissance activities. These findings allowed us to tweak our HR processes to better manage disciplinary action when required."

The organization employs a 'red team' (a team emulating a potential attack to test an enterprise's security posture), and the security team was delighted to see that ArcSight Intelligence for CrowdStrike also detected their activity, such as simulated Log4Shell attacks, pass the hash attacks, and DLL injection attacks.

Full ROI within Three Months and Reduced Risk of Reputational Damage

Convinced of the value that ArcSight Intelligence for CrowdStrike in combination with the CyberRes threat hunting service could bring to the organization's security posture, the COO set about defining the business case for his C-level colleagues. Rather than attempting to estimate what a security breach would cost in terms of reputational damage, the Micro Focus CyberRes team created a calculator to determine what operational efficiencies could be achieved by replacing manual effort with an automated advanced analytics solution. This put to one side the obvious benefit of having a much more effective process to detect insider threats and focused just on the financials. It clearly showed that a full return on investment (ROI) would be achieved within just three months of purchasing ArcSight Intelligence for CrowdStrike.

The security manager concludes: "Adding ArcSight Intelligence for CrowdStrike and the threat hunting service to our CrowdStrike and MSSP infrastructure significantly reduced our risk of reputational damage by protecting our sensitive customer data. Our security posture has improved, and the convenient ArcSight Intelligence for CrowdStrike SaaS model provides this without adding any burden to our security team or administration staff."

CyberRes
A Micro Focus Line of Business