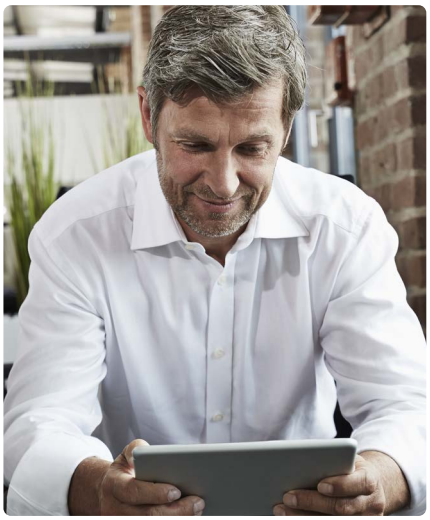
Large Online Retailer

ArcSight Intelligence teams with CrowdStrike, reveals hidden threats, and establishes outstanding advanced threat and insider threat detection to prevent breaches.



No 'One Size Fits All' When It Comes to Security

This internationally well-known company has undergone rapid online growth with hundreds of millions of monthly active users on its platform. A large user base, which requires a high number of internal staff to serve, raises the risk of insider threat, either accidental or malicious. It also makes an attractive target for cyber criminals. The organization's Chief Information Security Officer (CISO) knew that Artificial Intelligence (AI) and Machine Learning (ML) could be the key to keeping the company and its user data safe: "We have a large AI team as data analytics is really important to our business. However, this team needs to focus on our core business, rather than building, testing, refining, and deploying AI-based security models. It made more sense to us to find a partner with a purpose-built solution that we could leverage."

"Because of the way ArcSight Intelligence interacts with our data and users, Micro Focus is the only service provider that has knowledge of our corporate plans and related strategic initiatives, so that they can adjust how behaviors are monitored and evaluated. This level of trust and confidence is rare, but well-earned."

Chief Security Information Office
Large Online Retailer

Already convinced of the value of the cloud, the team decided to outsource its Security Operations Center (SOC) to a cloud-native Managed Security Service Provider (MSSP). This provides a lightweight agent infrastructure and includes coverage for both Mac and Linux, to cover the organization's main platforms. Most alerts are managed through SecureWorks, and it provides curated commodity alerts to the team on an exception basis. The organization supplemented this by introducing CrowdStrike Falcon, which is designed to create visibility into real-time and historical endpoint security events by gathering event data needed to identify, understand, and respond to attacks.
"While this provides us with a decent level of overall security, we felt we were still exposed on the user side," says the CISO. "Insider threats and targeted external attacks are notoriously difficult to detect. Users can leverage privileged access to commit fraud,

At a Glance

Industry

Retail

Location

Global

Challenge

Complement existing security measures with a user-and-workstation-focused strategy to combat notoriously difficult to detect insider threats and targeted external attacks

Products and Services

Micro Focus ArcSight Intelligence

Success Highlights

- Highly effective combination of CrowdStrike and ArcSight Intelligence
- Every Red Team attack detected
- PII exfiltration prevented and GDPR penalties avoided
- Improved GDPR compliance through better data protection
- Established zero-trust strategy

“ArcSight Intelligence is the only service we have that can detect Red Team attacks consistently. It has been instrumental in establishing a zero-trust strategy, for instance ensuring that all our critical applications require a VPN connection.”

Chief Security Information Office
Large Online Retailer

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

sabotage operations, or swipe intellectual property. When we were introduced to Micro Focus ArcSight Intelligence we realized this is exactly what it is aimed at.”

ArcSight Intelligence Detects Red Team Attacks

Combining CrowdStrike with ArcSight Intelligence identifies insider threats or targeted attacks by leveraging unsupervised machine learning to measure the normal, unique behavior of every user and other entity. This creates a unique digital footprint and makes it easy to detect unusual or suspicious behaviors. By shining a new light on user information, such as unusual processes running on each workstation, unusual login frequency, date or time of work, or access from unusual machines, ArcSight Intelligence allows threat hunters to see threats they would likely otherwise miss. Behavioral intelligence empowers triaging between accidental issues and legitimate threats so that the security team only focuses its resources on investigations that really matter.

Red Team attacks, done by internal teams or contracted to external test teams, are simulated cyberattacks on their own organization to assess the effectiveness of their security programs. The CISO was pleased to discover ArcSight Intelligence’s success in detecting Red Team attacks: “ArcSight Intelligence is the only service we have that can detect Red Team attacks consistently. It has been instrumental in establishing a zero-trust strategy, for instance ensuring that all our critical applications require a VPN connection.”

Improved GDPR Compliance through Trusted Partnership

During COVID-19 times this organization was sadly forced to change the makeup of its workforce, for example, by increasing the use of contingent workers. This can be particularly sensitive for security teams because they must balance productivity, flexibility, and security. In partnership with the HR department, the security team, using ArcSight Intelligence, was able to adjust its monitoring of user activity, paying special attention to higher sensitivity employees. As a result, a major data exfiltration event was avoided.

Because they can represent sizeable GDPR fines, data exfiltration threats are some of the most common use cases associated with insider threats. ArcSight Intelligence identifies valuable data movement anomalies and highlights these threats before they become breaches. To augment the ArcSight Intelligence capabilities, this CISO leverages the Micro Focus threat hunting team: “Our ArcSight Intelligence threat hunting team really understands our data, user behaviors, and how they relate to our security. They can make judgment calls on whether a particular set of behaviors are appropriate for our scenario. Because of the way ArcSight Intelligence interacts with our data and users, Micro Focus is the only service provider that has knowledge of our corporate plans and related strategic initiatives, so that they can adjust how behaviors are monitored and evaluated. This level of trust and confidence is rare, but well-earned.”