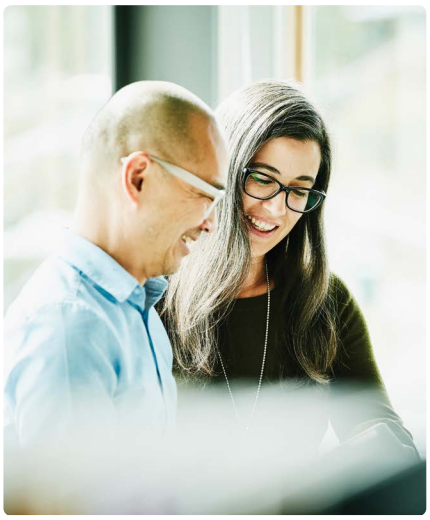
Financial Services Organization

ArcSight suite delivers enhanced data analysis capabilities with 400% threat hunting improvement.



Need for Scalability and Increased Visibility

This organization is one of the world's leading and most diverse derivatives marketplaces. Following a security breach which involved customer data and platforms, the security threat hunting team was asked to improve security by not only analyzing security incidences of concern (IOCs), but also introducing a threat assessment plan including a set of different data sources. Its Security Architect explains: "We already used Micro Focus ArcSight as the foundation of our security program but wanted to be more proactive and scale up to include our active directory, virtual private networks, and Windows data so that we can scan more effectively for potential threats. Also, although we had visibility of end-user machines in our analysis, we couldn't actually link any unauthenticated access to users themselves. The same was true for our partner and public websites; we didn't have visibility of the ultimate users."

"The ArcSight suite has given us data analysis capabilities beyond any scale we dreamed of. With our new-found visibility we can protect effectively against data exfiltration and proactively manage our SecOps program."

Security Architect
Financial Services Organization

400% Threat Hunting Improvement with 100 Billion Events Analyzed

Adding Micro Focus ArcSight Intelligence enabled the team to run queries and perform data analysis on a scale of 100 billion events. The additional data sources increased threat hunting capabilities by 400 percent. The extra data coverage and visibility protects against data exfiltration through various cyberattack methods. Any activity via partner websites or through end-user machines, is now tied uniquely to the specific user in question for full user authentication.

The organization plans to continue expanding and building on its SecOps program, focusing on pre-emptive threat mitigation and agile and proactive cyberattack management.

At a Glance

Industry

Finance

Location

USA

Challenge

Expand SecOps program beyond just analyzing IOCs and include different data sources in a threat assessment plan

Products and Services

Micro Focus ArcSight Enterprise Security Manager (ESM)
Micro Focus ArcSight Logger
Micro Focus ArcSight Intelligence

Critical Success Factors

- 400% security threat hunting improvement
- 100 billion security events analyzed
- New user visibility protects against data exfiltration