

Investment Management Firm

Case Study

Implementing a best-in-class threat defence solution and FCA readiness



Overview

A London-based wealth management services company offering financial planning and investment advisory services for clients in the United Kingdom. They manage funds worth billions of pounds, meaning strong cyber security controls are a high priority at board level.



Challenge

The client sought a cyber security partner to help them address four primary objectives:

- To ensure their information assets were suitably protected through a full investigation of the current measures and infrastructure in place.
- To assess the level of readiness of their security systems and processes should they be audited by the Financial Conduct Authority or other regulatory bodies.
- To support their small in-house IT team and bring together and simplify the cyber security services received from current providers.
- To recommend a security monitoring solution to provide water-tight threat defence.

At a Glance

Industry: Investment Management

Solution: Cyber Security Assessment, SOC & MDR

Products: Microsoft Sentinel, Microsoft Defender XDR



Solution

To deliver the initial investigation into the client's current cyber security set-up, CyberOne's team of engineers and analysts leveraged the NIST 800-30 risk-scoring methodology. This is a detailed approach to characterise the current system, establish a history of attacks and threats, list potential vulnerabilities, understand the threat source motivation and determine the current level of risk and controls. The results from the investigation were delivered to the client in a clear and detailed risk assessment report.

The report covered factors including:

- External & Internal Penetration Testing
- Network and Perimeter Monitoring
- Web & HTTP Security
- Access & Cloud Services
- Data Protection Security
- Security Awareness of Staff
- Endpoint Devices
- Physical Security

The investigation laid bare the weaknesses in the current processes and the likelihood of a potential cyber breach. The solutions in place were insufficiently working together and were leaving security gaps. It was also clear that any external audit would spot these weaknesses and be likely to fail.

CyberOne presented our award-winning SOC and MDR services. We combine industry-leading vendor technologies with human expertise to deliver an outcome-based solution. At its heart is Microsoft Sentinel, the industry-leading cloud-native security information and event management solution (SIEM) from Microsoft. CyberOne is a Microsoft Security Solution Partner with expertise second to none in this space.

CyberOne's consultancy-led architectural approach was relentlessly focused on delivering to the highest standard, ensuring the installation of the solution ran smoothly. This was delivered in close collaboration with the client to bespoke to their needs and resolve any technical issues smoothly as they came up.

With CyberOne's SOC and MDR service in place, the client has seen a step-change in their cyber security posture, with all security gaps and incompatibilities with their current solutions now closed. They are seeing their alerts investigated and triaged at speed with actionable remediation advice for quick and effective resolutions to incidents - 24x7. The replacement of their on-premises platform with the Microsoft Sentinel SIEM is enabling them to adapt and scale at speed, with their ever-growing data volumes being handled effortlessly.

The client is now fully confident to face any future audits by the Financial Conduct Authority or any other regulatory bodies, safe in the knowledge that their security systems and processes are watertight.



Results

- **Complete Visibility**

The client enjoys comprehensive visibility of their threats, covering their entire IT infrastructure, offering protection across multiple attack surfaces from within a single, fully managed platform.

- **AI-Powered Threat Intelligence**

CyberOne uses AI and machine learning to gather insights into threats and establish the relationship between them, minimising false positives and working the collated data harder to improve overall security for the client.

- **Enhanced Productivity**

By taking away the burden of day-to-day security management from their in-house teams, the client can focus more effectively on their core objectives.

- **24x7 Service**

Many competitors pay lip service to "24x7", however CyberOne lives and breathes it. All incidents are investigated immediately by our expert SOC team with rapid-response escalation and neutralisation.

- **Reduced and More Predictable Costs**

Our service works on a flexible consumption-based, pay-monthly subscription model, so the client does not pay for any unused capacity. They have had to make no up-front investments in technology, training or resources, and their pricing plan is clear, simple and with nothing hidden.

- **Enhanced Compliance**

The client is now fully compliant with Financial Conduct Authority guidelines as well as ISO27001 and Cyber Essentials Plus.

About CyberOne

A Microsoft Security Elite Partner and member of the Microsoft Intelligent Security Association (MISA), delivering world-class AI-augmented Managed Extended Detection & Response (MXDR) services. Our Microsoft-verified Managed XDR solution combines Microsoft's security platform with CyberOne's accredited experts to help organisations prevent, detect and respond to modern cyber threats faster while accelerating cyber maturity and maximising Microsoft investments.

Through our 24x7x365 Global Security & Network Operations Centre (SNOC), CyberOne provides continuous protection supported by NCSC-accredited Cyber Incident Exercising and Response, CREST-accredited SOC services and Penetration Testing, alongside clear, measurable service level agreements (SLAs). CyberOne's Consulting, Professional and Managed Security services help organisations protect critical operations, strengthen compliance and move confidently from cyber risk to cyber resilience.



+44 (0) 3452 757575

hello@cyberone.security

cyberone.security

