

Currencies Direct

Case Study



Overview

Established in 1996, Currencies Direct was the first non-bank foreign exchange provider in Europe. Today, following a period of high growth, Currencies Direct employs over 1,500 staff across 7 global locations. They have won multiple industry awards for their innovative use of technology to make transferring money simple and secure.



Challenge

Currencies Direct were fully aware they were a high-risk target for cybercrime due to the volume of financial and personal data processed daily through their online platform. They recognised that a successful cyberattack could have serious implications for their reputation and lead to significant financial loss.

Despite having an experienced IT team and several cyber security products, they lacked dedicated security experts in-house. Their existing security information and event management (SIEM) service generated a high volume of alerts, making it unclear which to prioritise and where to focus remediation efforts, leading to delayed responses. With their SIEM on-premises, they knew they would struggle to adapt to continued growth and change in their business.



At a Glance

Customer: Currencies Direct

Organisation Size: 1,000–3,000

Industry: Financial Services

Solution: SOC & MDR

Products: Microsoft Sentinel,
Microsoft Azure, Microsoft Power BI,
Tenable Nessus



Solution

After deciding to engage with a specialist managed security service provider, CyberOne was the obvious choice, considering their successful partnership to date. Currencies Direct were impressed by the speed of implementation and close collaboration with their in-house IT team, including scoping calls, technical configuration sessions and weekly technical catch-ups. CyberOne reviewed the data sources configured in their current SIEM, replicating and improving the setup.

CyberOne's SOC analysts now work as an extension of the Currencies Direct team. Lines of communication are strong, with immediate investigation, prioritisation, and triage for all alerts, and rapid-response escalation procedures for threat neutralisation and isolation 24x7. At the heart of CyberOne's SOC and MDR is Microsoft Sentinel, the leading cloud-native SIEM. In addition to Sentinel, ongoing vulnerability scanning is performed.

CyberOne's SOC analysts now work as an extension of the Currencies Direct team. Lines of communication are strong, with immediate investigation, prioritisation, and triage for all alerts, and rapid-response escalation procedures for threat neutralisation and isolation 24x7. At the heart of CyberOne's SOC and MDR is Microsoft Sentinel, the leading cloud-native SIEM. In addition to



Results

- **Reduction in Alerts** - Continuous analysis and investigation of security alerts, cutting through the “noise” to report only genuine threats to Currencies Direct.
- **Threat Hunting & Intelligence** - CyberOne SOC analysts leverage threat-hunting tools proactively to identify threats before they become security incidents. Threat intelligence is fed into Sentinel to identify indicators of compromise.
- **Managed Vulnerability Scanning** - Ongoing vulnerability scanning, with the SOC team continually monitoring the Currencies Direct estate for new vulnerabilities.
- **Complete Visibility** - Comprehensive visibility of threats covering the entire Currencies Direct infrastructure, offering protection across attack surfaces from a single, fully managed platform.
- **Improved Reporting** - Customised Power BI dashboards allow Currencies Direct to easily see the incidents and attacks that have been stopped.
- **Reduced & More Predictable Costs** - A flexible consumption-based, pay-monthly subscription model means Currencies Direct doesn't pay for any unused capacity. With no upfront investments in technology, training, or resources, their pricing plan is clear, simple, and transparent.



CyberOne are always willing to go the extra mile and feel more like an extension of our team than a third party we're dealing with.

The opportunity to employ CyberOne's SOC and MDR service gives us a 24x7 capability and that's really important to our global business

Chris Congreve, Information Security Specialist, Currencies Direct

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

