SOCURA

- Case study
- interactive investor

Seamlessly extending the security operations of the UK's leading subscription-based investment platform

As a leading online investment service, interactive investor (ii) is entrusted with safeguarding the life savings and pensions of its customers. In a highly regulated industry where reputation and trust are paramount, maintaining a robust security posture is not just a priority—it is a fundamental business requirement.

Partnering with Socura for **Managed Detection and Response** (MDR) ensures ii can maintain continuous threat visibility across its environments and respond swiftly and effectively to attacks to minimise risks.

The security challenge

As the UK's number one flat-fee investment platform, ii treats the security of its customers' personal and financial data with the utmost importance. Owing to the potential financial and reputational damage caused by cyberattacks, information security is the organisation's number one business risk.

Following a decision to replace its legacy Security Incident and Event Management (SIEM) solution with Google Security Operations (SecOps), ii sought a specialist service provider to help continuously manage, monitor, and optimise its new choice of technology and other controls. As an organisation regulated by the Financial Conduct Authority (FCA), ii also knew that being able to demonstrate measurable improvements to its security posture was essential to upholding compliance and stakeholder trust.

Having worked with managed service providers in the past, ii had a clear benchmark for service quality. As a result, the company knew it needed a partner that could demonstrate a thorough understanding of its bespoke requirements, was able to work collaboratively with its in-house team, and could be relied upon to be proactive rather than reactive in its approach.

interactive investor

Main security concerns

- **Protecting the personal and financial data of customers**
- **Timely detection and response to security incidents**
- **Ensuring a seamless transition to Google SecOps**
- **Compliance with the latest industry standards and best practices**

The solution

Following the evaluation of several managed service providers, ii appointed Socura as its partner for MDR. Socura's team of Security Operations Centre (SOC) analysts and engineers operate as a dedicated 'security operations arm' for ii, providing around-the-clock monitoring and expert intervention to contain and disrupt threats. Using the latest threat intelligence data, Socura also performs proactive threat hunting to identify evidence of unknown attacks.

As a Google Cloud certified provider, Socura enables ii to maximise the capabilities of Google SecOps, ensuring the platform is fully integrated with telemetry sources in its environment and is constantly tuned to identify the latest threats. All security alerts generated by Google SecOps and other controls are ingested into Socura's Incident Management Portal, where they are triaged and investigated by SOC analysts.

Once a genuine incident is confirmed, the Socura team initiates immediate containment and disruption actions, such as isolating endpoints and resetting user accounts. They also provide tailored remediation advice to help ii harden its security posture.

Google Cloud
Partner

Why Socura MDR

Specialist expertise

Socura's CREST accreditation and proven track record of threat detection within complex financial services environments assured ii that its choice of partner possessed the deep technical proficiency required to defend against attacks.

Swift deployment

During a high-pressure transition period when ii needed support migrating from its legacy SIEM to Google SecOps, Socura was able to work to tight deadlines and ensure that its MDR service was deployed smoothly and within a matter of weeks.

UK-based team

Having previously experienced frustrating delays in communication with global service providers, ii values that Socura's team is 100% UK-based and maintains a collaborative, transparent approach to service delivery.

Google SecOps partner

Following its investment in Google SecOps, ii required a partner with the technical proficiency to get the best from the platform and maintain comprehensive threat coverage at all times.

> “In Socura, we have an MDR partner that truly operates as part of our team. Having them alongside us gives us confidence that we can rapidly identify and respond to threats.
>
> **Phillip Bedford**
> Head of Information Security, interactive investor

Key benefits

How Socura MDR is enabling interactive investor to address its security needs.

01

Greater peace of mind

With Socura's SOC team detecting and responding to threats around the clock, ii has full confidence that security alerts are triaged, investigated, and addressed within minutes. A close working relationship and open lines of communication between teams also reinforces that Socura is a partner ii can rely on.

02

Relieving the load

Outsourcing the responsibility for alert management to Socura ensures ii's information security team no longer wastes time handling false positives and can focus on other high priority tasks.

03

Frequent detection engineering

Socura's proactive approach to tuning security controls is informed by the latest threat intelligence, ensuring ii maintains comprehensive coverage against the latest attack techniques.

04

Board-level visibility

Custom Google SecOps dashboards and monthly service reports enable ii to maintain a clear view of its security posture, while ensuring that evidence of

05

Proactive risk management

Socura's SOC experts work in close collaboration with ii's in-house team to identify risks and explore ways the company can strengthen its resilience. This process is supported by regular service reviews with a Socura Customer

Talk to us about your detection and response challenges

SOCURA

hello@socura.co.uk
0800 640 4067

LinkedIn
Bluesky