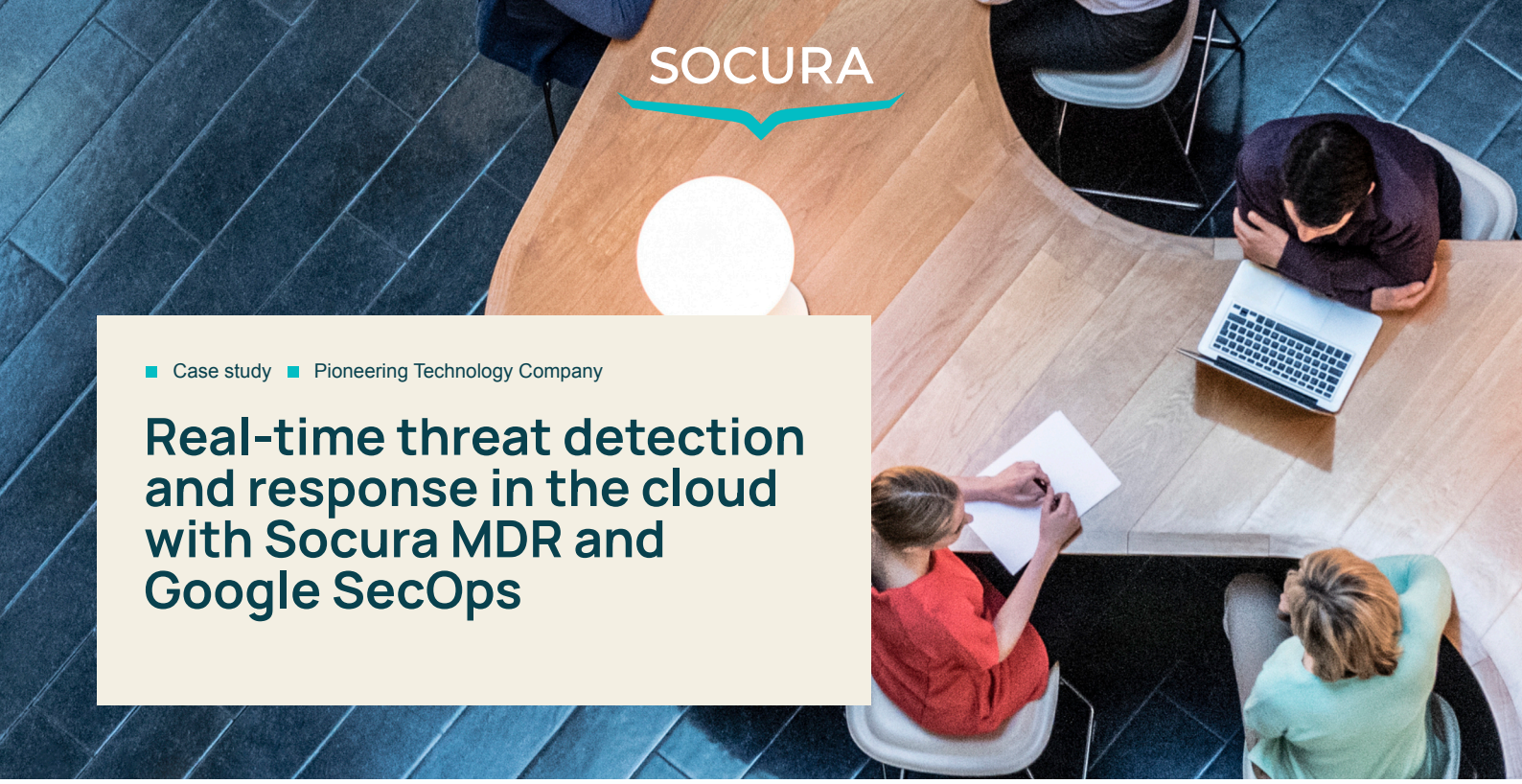

Case study ■ Pioneering Technology Company

Real-time threat detection and response in the cloud with Socura MDR and Google SecOps

This leading technology company protects organisations from fraud. After investing in Google Security Operations (SecOps) to increase threat visibility across its cloud environments, the company sought a managed services partner that could enable its security team to get the best from the platform and adopt a white-box approach to threat detection and response.

After evaluating several managed services, the company selected **Socura Managed Detection and Response** for its technical proficiency with Google SecOps, tailored service offering, and automated threat response capabilities. Only months into the service, the company's capacity to identify and disrupt threats has shown measurable improvements.

The security challenge

Specialising in identity fraud detection, this company treats information security with the utmost importance. Its solutions are trusted by governments and enterprises around the world, so a security-first culture is fostered throughout the business.

Through the process of hardening its own technology, the company recognised that continuous improvement is vital for resilience. As a scaling business focused on cloud and machine learning, it remained wary of the risks inherent in rapid innovation. As the Head of Cyber Security noted: "Change is the time when you're most vulnerable."

Despite having already invested in EDR and NDR controls, the company wanted to expand its threat coverage and visibility even further. After deciding to invest in Google SecOps to help tackle the coverage challenges it faced, the company knew that the next step was to identify a managed services partner with which it could work to achieve its desired outcomes.

Main security concerns

- **Protecting customer data and intellectual property**
- **Keeping systems secure in line with innovation and growth**
- **Timely detection and response to security incidents**
- **Over-reliance on vendor-supplied detection rules**

The solution

With experience in bringing Managed Detection and Response providers to four other organisations, the company's Head of Cyber Security knew that she needed a partner with both the technical expertise and flexibility needed to support the company's security goals.

After evaluating several Google Cloud Security MSSP partners, Socura MDR emerged as a standout choice for several reasons. These included a UK-based Security Operations Centre team, a wide range of playbooks to automate response to threats, and a tailored approach. The high calibre of Socura's security engineers was also a decisive factor.

"One of the biggest challenges when it comes to choosing an MDR service is finding a provider with very good talent in the engineering department," says the Head of Cyber Security.

"Socura immediately stood out as being extremely capable for its ability to write custom detections, support a wide range of integrations, and automate incident response actions".

"Trust is a precious commodity, both in business and cyber security. From the first moment I spoke with Socura, I got the impression that the service is led by people who know the work."

Google Cloud Partner

Included as part of Socura MDR

- Detection and response across networks, endpoints and clouds
- 24/7 alert triage, analysis and investigation
- Genuine incident notification
- Bespoke detection rule development and maintenance
- Proactive human-led threat hunting
- Automated threat containment and disruption
- Monthly reporting and service reviews

> "Socura isn't like a typical service provider where you have an issue, raise a ticket, and don't know who's going to pick it up. Our relationship with the Socura team is very good and the attention we receive means we benefit from a bespoke service.

Head of Cyber Security
Pioneering Technology Company

Key benefits

How the company is benefiting from Socura MDR and Google SecOps.

01

Broad threat visibility

After deploying Google SecOps and configuring it to ingest logs from Google Workspace and other sources, Socura has enabled the company to increase threat coverage and visibility across its cloud environments. To centralise visibility, Socura's Incident Management Platform is integrated with Google SecOps, as well as the company's existing EDR and NDR controls. These integrations enable Socura to obtain the high degree of context required to triage, investigate, and respond to alerts swiftly.

02

Rapid response to threats

As a specialist in both threat detection and incident response, Socura has enabled the company to be even more proactive in its approach to security. Socura's SOC team monitors the company's environments 24/7 and performs regular threat hunts using the latest threat intelligence data. In the event threats are identified, automated response playbooks are in place to contain and disrupt them before they can spread.

03

A white-box approach to detection engineering

Having been reliant on detection rules supplied by vendors, partnering with Socura has enabled the company to tailor its approach to threat detection and implement rules specific to the unique risks it faces, such as its use of machine learning technologies. A white-box approach to detection engineering also means fewer false positives.

04

Cross-sector intelligence

By outsourcing threat detection and response, the company now benefits from Socura's cross-sector expertise in detecting threats across a range of environments When Socura observes threat activity targeting other customers, its SOC analysts can take swift action to protect the company against the same threats.

05

Swift service onboarding

Following its decision to invest in Google SecOps, the company was keen for the technology to be deployed as early as possible. Working with Socura meant that both the platform and MDR service were deployed in a matter of weeks. To make the process as smooth as possible, the company's onboarding was handled by a dedicated Customer Success Manager and Security Engineer from Socura.

hello@socura.co.uk
0800 640 4067
LinkedIn
Bluesky