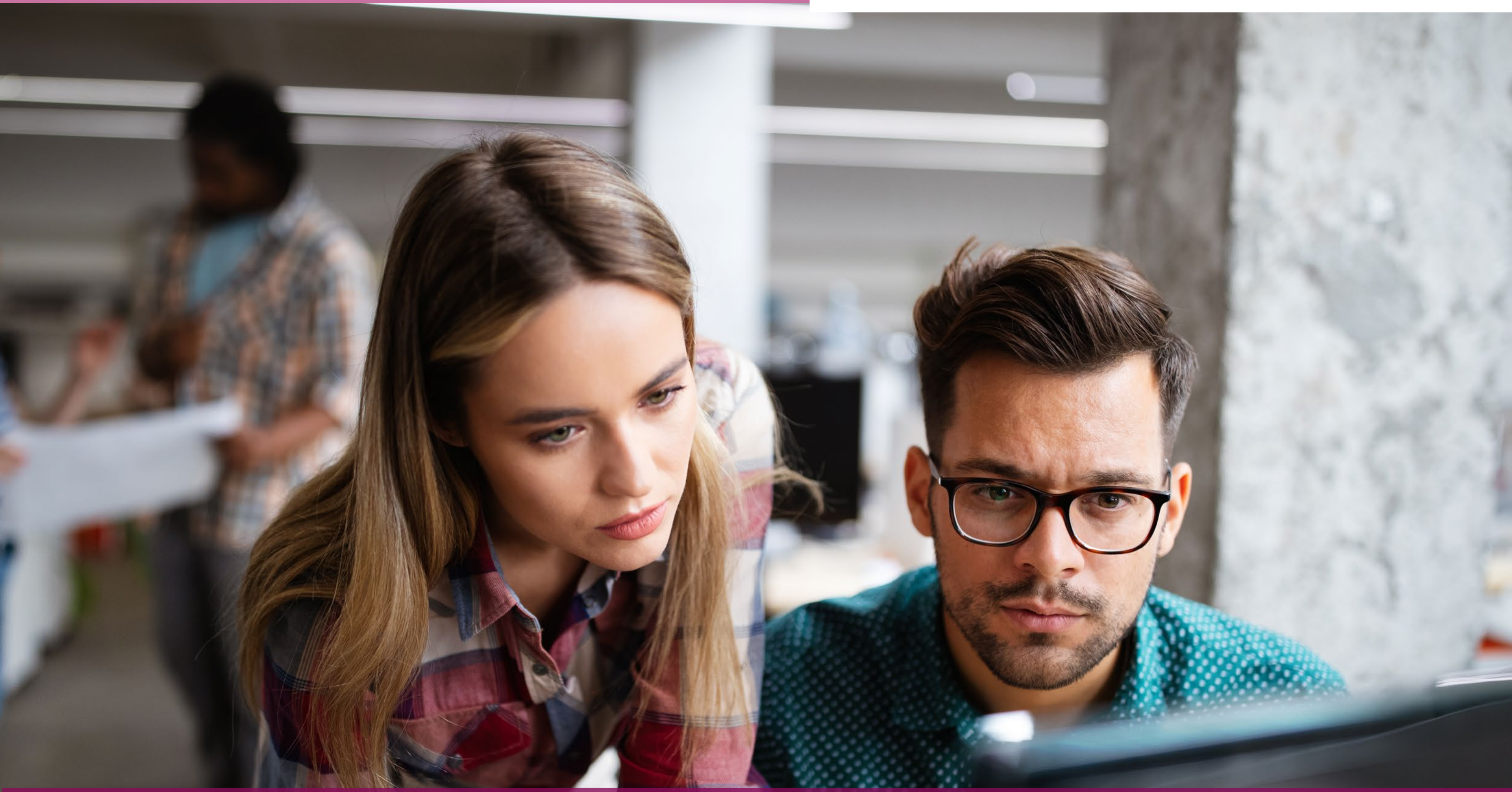
CYBERSEER
THE VISION TO PROTECT

Google Cloud
Security

Cyberseer SOC & Google SecOps

Solution brief



Discover how to get the most from Google SecOps when combined with Cyberseer's monitoring platform and highly trained Analysts to ensure you are only alerted to immediate actionable threats.

Approximate read time: 6 min

THE VISION TO PROTECT

Global Scale Threat Detection with Google SecOps

Google Security Operatons (SecOps) is a petabyte scale SIEM for investigation and detection of modern threats. The cloud native architecture enables organisations to ingest all their security telemetry into Google SecOps within a private cloud container and retain it for a full year at a fixed, predictable cost. It provides instant threat analysis and context in record speeds as it automatically and continuously normalises, index's, correlates and analyses data on users and assets.

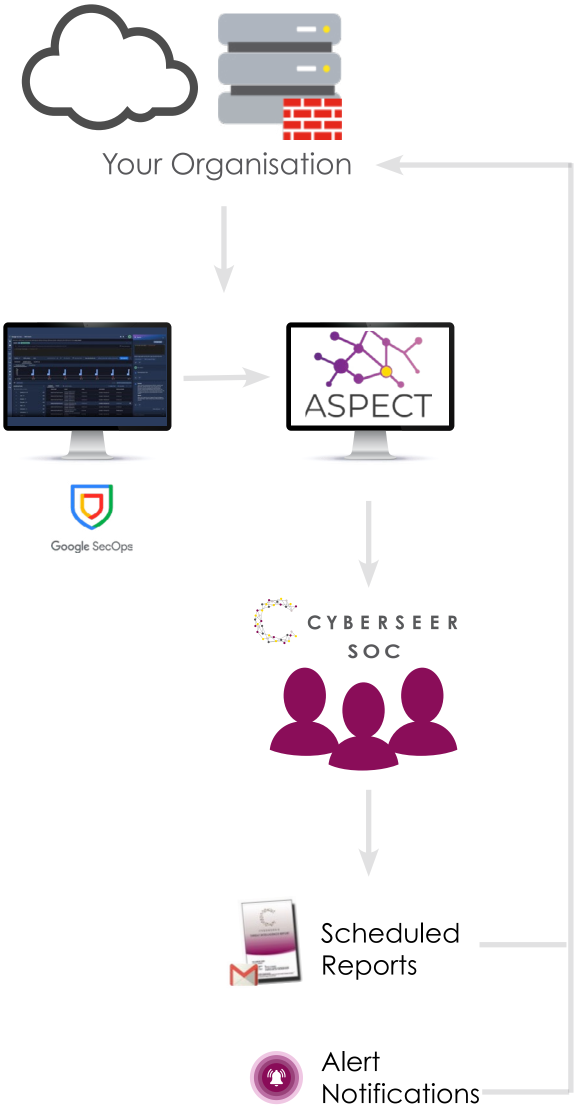
Google SecOps and Cyberseer SOC Service

Cyberseer has been providing best-in-class SOC services for customers across a wide array of industry sectors for many years. Partnering with Google gives our talented team of tier-3 security analysts access to unparalleled speed of search, threat intelligence and investigatory abilities throughout our customer's networks.

Communication is key in a partnership and providing our customers with clear and consistent communications is a critical part of the process for improving visibility and threat detection in their environments. Google SecOps and Cyberseer's SOC service align with the MITRE ATT&CK framework, classifying customer incident information in a standard, industry recognised, format.

ASPECT - is at the core of all Cyberseer services, it is our proprietary platform that integrates with our security vendor partner technologies via API to pull alerts 24x7 that are enriched, prioritised, and escalated to our forensic analysts. The automation of these repetitive and time-consuming processes, along with the enrichment of alerts with internal and external contextual threat data, enables us to do more with less by efficiently and effectively identifying and routing priority threats to analysts, which in turn reduces the time to respond so that threat dwell time can be minimised.

The purpose-built integration between Google SecOps and Cyberseer's ASPECT monitoring platform enables customers to combine the real-time threat detection and investigation capabilities of Google SecOps with Cyberseer's highly trained analysts. This ensures you are only alerted to immediate actionable threats, reducing your internal resource costs and increasing the efficiency of your SOC by removing the alert noise generated by the large volumes of flowing data and allowing you to focus on what really matters.



Google SecOps can take all your security telemetry data, process it at scale from anywhere in your environment with unrivalled speed of search. Combined with ASPECT, this automates the repetitive and time-consuming analyst tasks in to a standardised workflow that is designed to be consistent and accurate to reduce human error and the time to detect priority threats.

Unlock Instant Security with Cyberseer's Playbooks

Upon signing up for Cyberseer's SOC service, you gain immediate access to three Cyberseer-crafted SOAR playbooks, each designed to address real-world challenges:

- **Phishing:** Automate phishing threat responses with seamless Microsoft integration, enhancing your defence against malicious e-mails and links.
- **Compromised Credentials**: Streamline the detection and remediation of compromised credentials, minimising breach risks and protecting sensitive data.
- **Malware:** Leverage Mandiant's elite threat intelligence to respond effectively to sophisticated attacks, ensuring your organisation stays one step ahead of emerging threats.

Developed by our top-tier SOC team, these plug-and-play solutions empower your security team to automate critical security responses from day one. With years of hands-on experience embedded into these solutions, you can trust that industry-leading automation backs your security team.

Delivery at Scale

Cyberseer's SOC service has been specifically designed for businesses with stretched security resources in terms of time, costs or requisite skillset. Fusing advanced automation technologies with hands-on forensic expertise, we help you gain 360-visibility across your critical data, suppliers, staff and clients and find those important signals in large data sets. The result? Priority alerts are rapidly identified, time-to-detection is reduced, and your team gets back to doing the work they love. All within the per user per year subscription fee.

Gain 360 visibility across your critical data, suppliers, staff and clients.

Key Activities

- **Investigation & Hunting**: with sub-second latency, visualising anomalous domains observed within the environment
- **Advanced Threat Detection**: Rules built around MITRE Tactics Techniques and Procedures.
- **Prime use cases** – external threats, compromised insiders and malicious insiders.

Joint Solution Benefits

- **Continuous IoC matching**
  Continuous, retrospective analysis of telemetry vs. threat intelligence.

- **Hunt at Google speed**
  Sub second searches against petabytes of data. Save time on collating comprehensive audit reports and provide tangible evidence of proactive threat prevention to your board.

- **Consistent standardised workflows**
  Reduce human error with an automated 24 x 7 alert escalation platform enforcing a standardised workflow each time, every time.

- **Improve your team's productivity by finding active threat**
  Improve team's focus, by prioritising their attention on threats that matter. We reduce alert fatigue and take all the heavy lifting out of threat detection. We are with you every step of the way, so your team can get back to doing what they love.

- **Reduce time-to-detection**
  With real time threat detection from Google SecOps and Cyberseer's ASPECT monitoring platform combined with Cyberseer's highly trained analysts provides your security team with priority threats and a reduced time to detection.

- **Have certainty of spend**
  With a fixed, transparent fee. On day 1 we get you up and running, by day 14 we've deployed a base set of rules for popular log sources to start generating detections.

Delivery Model and Pricing

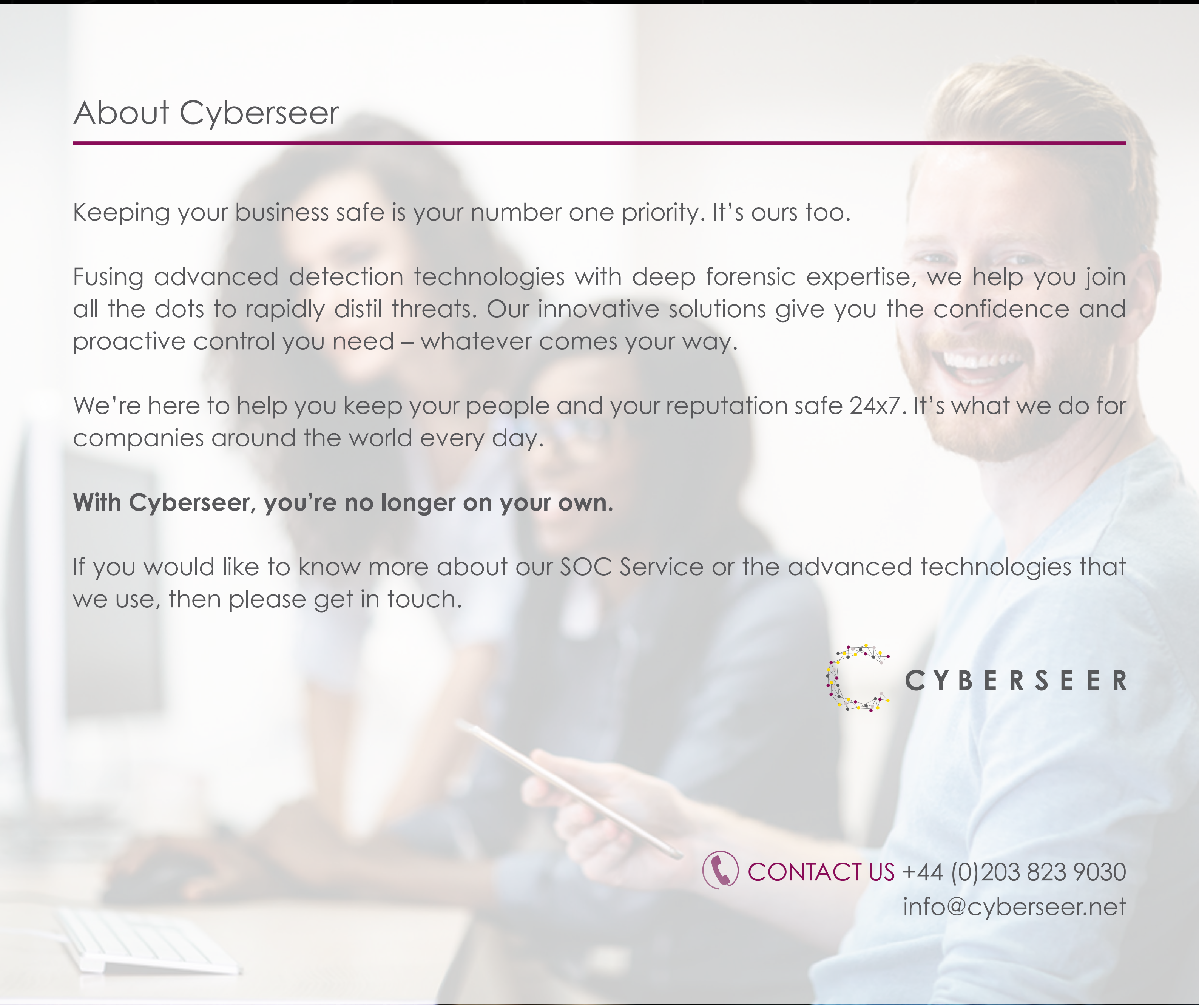
The Cyberseer Google SecOps SOC service is priced per user per year. This includes 12 months hot data retention for all your enterprise's security telemetry data. Cyberseer will consult with you to provide best practice deployment insight and guidance. Priority data sources required to meet agreed detection use cases are identified and documented for integration. This process is designed to be simple yet thorough to ensure you are onboarded into the service efficiently. All individual pricing integration and deployment will be provided under a day rate.

Cyberseer provide a clearly communicated strategy to mitigate cyber risks against your enterprise's priorities from the outset and throughout the service onboarding process. Cyberseer will then monitor the deployment during office hours while integrating ASPECT for 24x7 priority threat detection go-live.

About Google SecOps

Google SecOps, part of Google Cloud Security, is focused on enterprise cybersecurity solutions. They leverage massive data and compute resources to analyse and fight cyber threats. Our Google SecOps cloud-native SIEM helps enterprise security teams investigate incidents and hunt for threats in their networks, at the speed of search.

Google Cloud
Security



About Cyberseer

Keeping your business safe is your number one priority. It's ours too.

Fusing advanced detection technologies with deep forensic expertise, we help you join all the dots to rapidly distil threats. Our innovative solutions give you the confidence and proactive control you need – whatever comes your way.

We're here to help you keep your people and your reputation safe 24x7. It's what we do for companies around the world every day.

With Cyberseer, you're no longer on your own.

If you would like to know more about our SOC Service or the advanced technologies that we use, then please get in touch.

CYBERSEER

☎ CONTACT US +44 (0)203 823 9030
info@cyberseer.net

axi | ADDISON LEE | MARKERSTUDY LIMITED | Auto Windscreens | MIZUHO | Knight Frank