CYBERSEER
THE VISION TO PROTECT

Google Cloud Security

CROWDSTRIKE

Cyberseer SOC & Google SecOps & CrowdStrike

Solution brief

Discover how the combination of Cyberseer's SOC, Google Security Operations & Crowdstrike Falcon, when delivered as a service, provides comprehensive visibility to improve your advanced threat detection and response capabilities. Understand the additional benefits of having access to expert analysts who operate as an extension of your existing team and overcome resource issues.

Approximate read time: 6 min

THE VISION TO PROTECT

Executive Summary & Key Benefits

- Cloud-native security, endpoint protection, detection, and response.
- Investigation & hunting with sub-second latency, visualising anomalous domains and endpoints observed within the environment.
- Utilise the full potential of CrowdStrike Falcon.
- 24x7 threat detection & priority alerts.
- Advanced threat detection via curated detection rules.
- Rules built around MITRE tactics, techniques, and procedures.
- Actionable intelligence from Tier 3 Forensic Analysts.
- Reduced dwell time and increased confidence in detections.
- Advanced threat hunting and automated response capabilities.
- Centralised visibility of your environment including discoverable endpoints.
- Attack surface reduction.
- Combined management information.
- Prime use cases – external threats, compromised insiders, and malicious insiders.

Cyberseer has integrated CrowdStrike and Google Security Operations into its managed service offering, providing managed detection and response across your environment. Cyberseer continually monitors your environment, triaging and prioritising alerts, and escalating critical threats that require your immediate attention.

The Challenge

Today's businesses face complex challenges in securing the digital landscape, driven by digital transformation initiatives, remote work, cloud adoption and diverse infrastructures. As the threat landscape grows, security teams struggle to keep up while facing business pressures to rationalise spending.

Common attacks

According to the CrowdStrike 2023 Global Threat Report, "There was a continued shift away from malware use, with malware-free activity accounting for 71% of all detections in 2022 (up from 62% in 2021). This was partly related to adversaries' prolific abuse of valid credentials to facilitate access and persistence in victim environments."

Detecting attacks of this nature requires a mix of automation and human expertise in the form of threat hunting, reviewing content and adding context to detections. A mix of art & science, which cannot be completely solved by machine learning.

> **"68% of organisations have experienced one or more endpoint attacks that have compromised their data or infrastructure." ***

Visibility:
Security teams struggle to gain a holistic view of the environment due to the use of multiple security solutions. The lack of integration between these best-in-class security tools makes it cumbersome for teams to correlate information for investigation and triage. Achieving comprehensive visibility is crucial to quantify the risk within your business and enhance your security posture.

The Endpoint Challenge:
The focus on user endpoint devices has intensified, given their role as access points to corporate data and services from anywhere. The security implications are obvious; poorly protected user endpoints connected to a corporate network become prime targets for malicious actors. The Ponemon Institute study indicates that a significant number of organisations (68%) have experienced one or more successful endpoint successful endpoint attacks.[*1] The aftermath of a successful endpoint attack can be financially crippling for organisations. The average cost of a successful endpoint attack is estimated to be $1.8 million annually, encompassing factors such as lost productivity, system downtime, data theft, IT infrastructure damage, brand damage and potential fines.[*2]

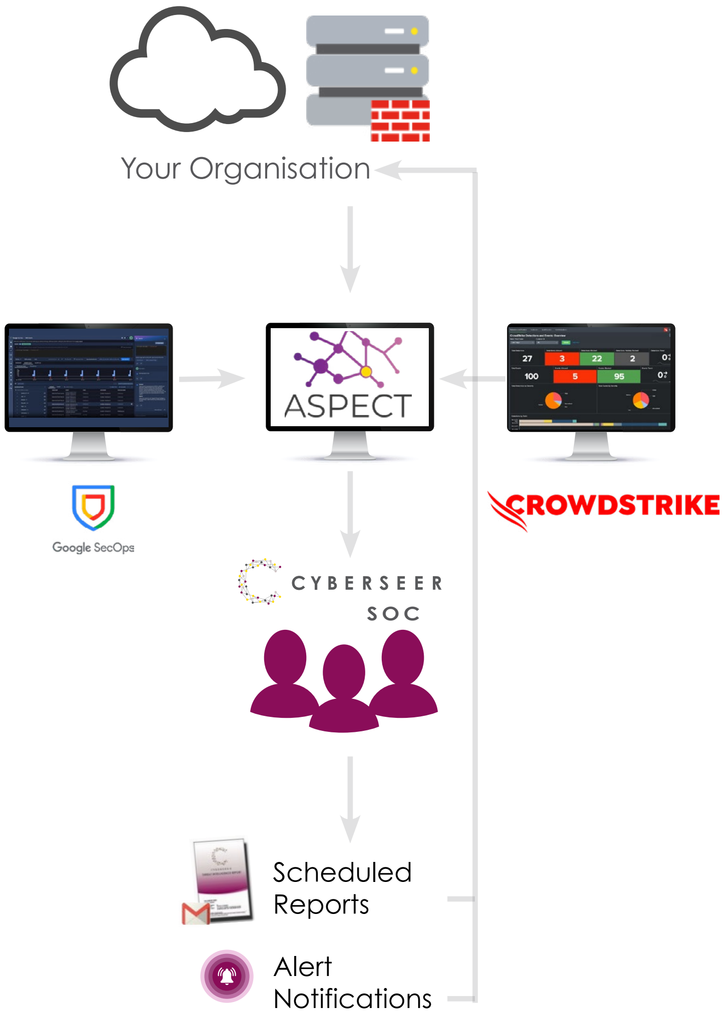
Cybercriminals are employing sophisticated techniques to evade traditional antivirus technologies. Initial access is still commonly seen via phishing e-mails. One such technique is the use of file-less malware combined with living-of-the-land (LOLbins) techniques. This involves leveraging legitimate operating system tools like PowerShell, to execute file-less code that runs only in memory.

The Solution: Cyberseer SOC, Google SecOps & CrowdStrike Falcon

Google SecOps is a cloud-native platform designed to handle massive amounts of security telemetry data and enable real-time threat hunting and incident investigation. It offers scalable data ingestion, intelligent threat detection, timely threat hunting and automated threat intelligence.

CrowdStrike Falcon is a leading endpoint protection platform, offering next-gen antivirus, endpoint detection and response (EDR) and proactive threat-hunting capabilities. Its features include endpoint visibility, behavioural-based threat detection, malware prevention and EDR and incident response with detailed endpoint telemetry.

The integration of CrowdStrike Falcon with Google SecOps through Cyberseer's ASPECT platform provides a comprehensive and powerful solution for managed detection and response. By efficiently pulling and enriching alerts from Google SecOps and CrowdStrike, we reduce response times and minimise threat dwell time, enabling a quick and effective response to critical threats.



ASPECT from Cyberseer – is at the core of the Cyberseer SOC. It is a proprietary, 24x7, distributed platform that integrates with Google SecOps and CrowdStrike via API to pull alerts for enrichment, prioritisation, and escalation 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. This combination of Google SecOps, CrowdStrike and ASPECT means Cyberseer analysts are responding to priority issues ASAP which in turn reduces the time to respond, minimising threat dwell time.

All Cyberseer SOC Analysts are Tier 3 people who are trained to comprehensively threat hunt, triage, and investigate prioritised activity; and be an extension of your security team, building a deep understanding of your environment and organisation. This style of working relationship is key as it provides further context for the Analysts to understand the impact of a threat in your environment. Also, when you are contacted out-of-hours you will not need to bring the Analyst up to speed on your environment which further reduces your overall response time.

Cyberseer Analysts perform an initial triage process to classify an incident, before alerting the customer using pre-defined communication channels and escalation contacts. The Analyst will walk the customer through their current understanding of the incident and classification that has been assigned, and then support the customer with their response efforts and investigate the activity further.

Cyberseer provides all customers with three types of reports:

1. Priority incident reports detailing escalated priority threats.
2. Weekly reports detailing all threat tickets raised during the week.
3. Monthly trend reports detailing the number of incidents, threat classifications, breaches by attack phase, total threats, and risk scores.

Delivery at scale

Cyberseer's 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.

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.

Joint Solution Benefits

- **Improved Threat Visibility**
  The integration of Google SecOps and CrowdStrike offers an unmatched level of visibility into network, cloud, and endpoint activity, enabling threats to be rapidly detected and responded to promptly.

- **Threat Intelligence Enrichment**
  The integration of threat intelligence feeds enhances the context of security events, aiding in the identification and understanding of potential threats.

- **24/7 Priority Threat Detection & 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**
  Improve the 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.**
  By efficiently identifying and prioritising threats we can stop them early in the attack lifecycle, therefore reducing response times and mitigating business risk.

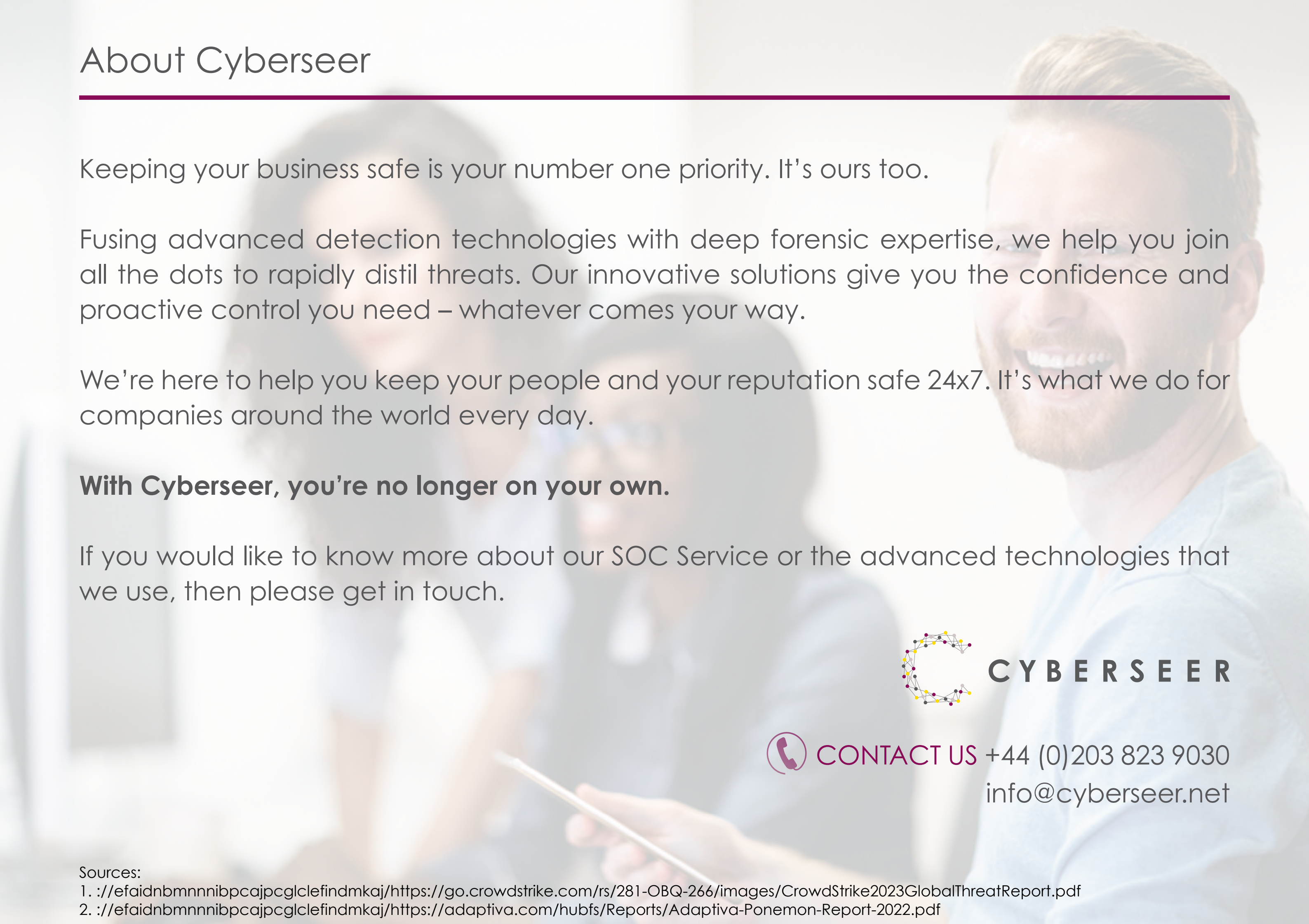
- **Have Certainty of Spend.**
  With a fixed, transparent fee, priced per user per year. On day 1 we get you up and running, by day 14 we've deployed a base set of rules for popular log sources to start generating detections.

About Google SecOps

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

About CrowdStrike

The CrowdStrike Security Cloud correlates trillions of security events per day with indicators of attack, the industry's leading threat intelligence and enterprise telemetry from across



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.

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

Sources:
1. ://efaidnbmnnnibpcajpcglclefindmkaj/https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrike2023GlobalThreatReport.pdf
2. ://efaidnbmnnnibpcajpcglclefindmkaj/https://adaptiva.com/hubfs/Reports/Adaptiva-Ponemon-Report-2022.pdf