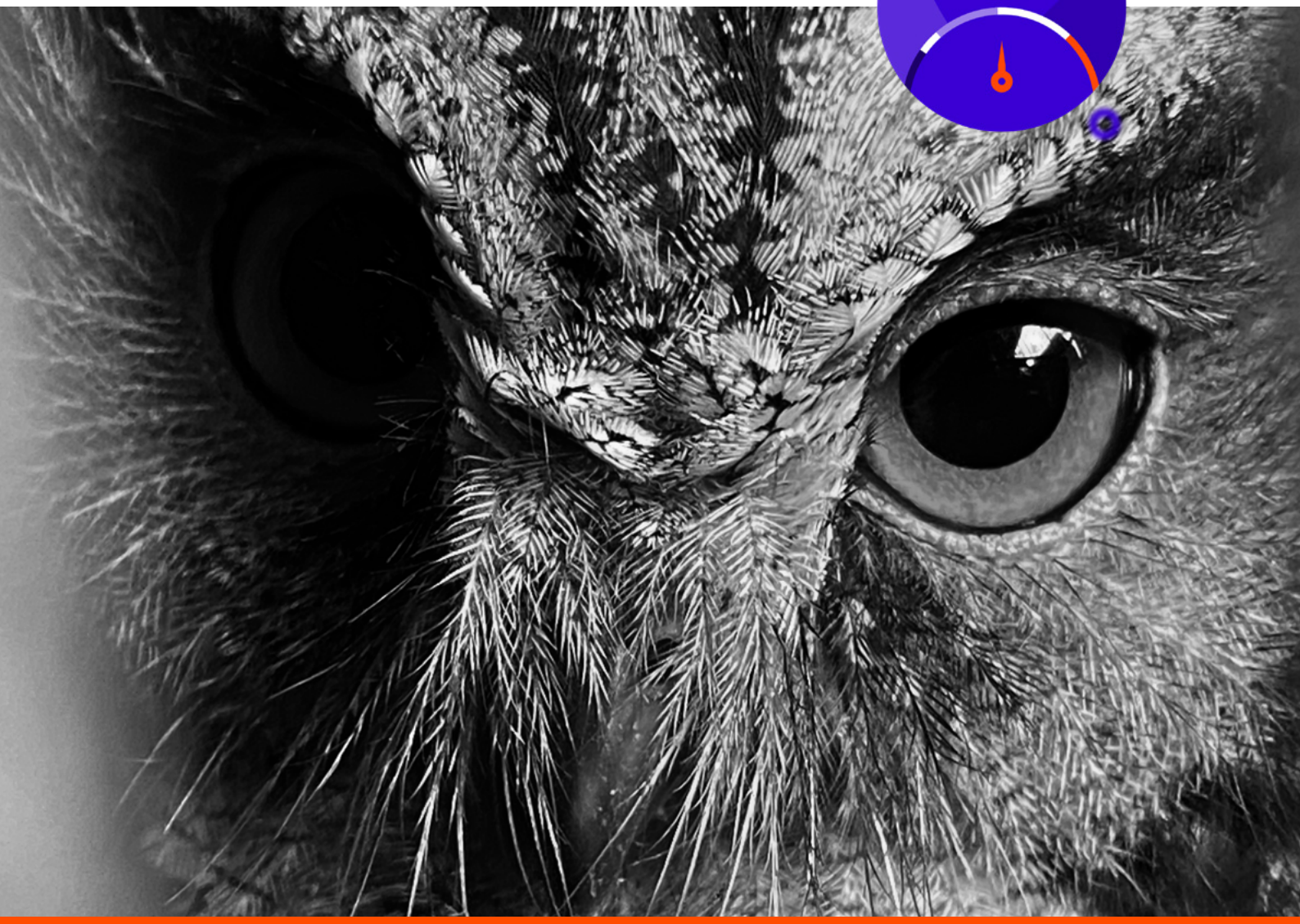
SECURITY OPERATIONS CENTRE AS A SERVICE (SOCaaS)

EVERY ORGANISATION NEEDS A SOC CAPABILITY BUT ONLY A SMALL PERCENTAGE CAN AFFORD TO BUILD THEIR OWN.



METCLOUD

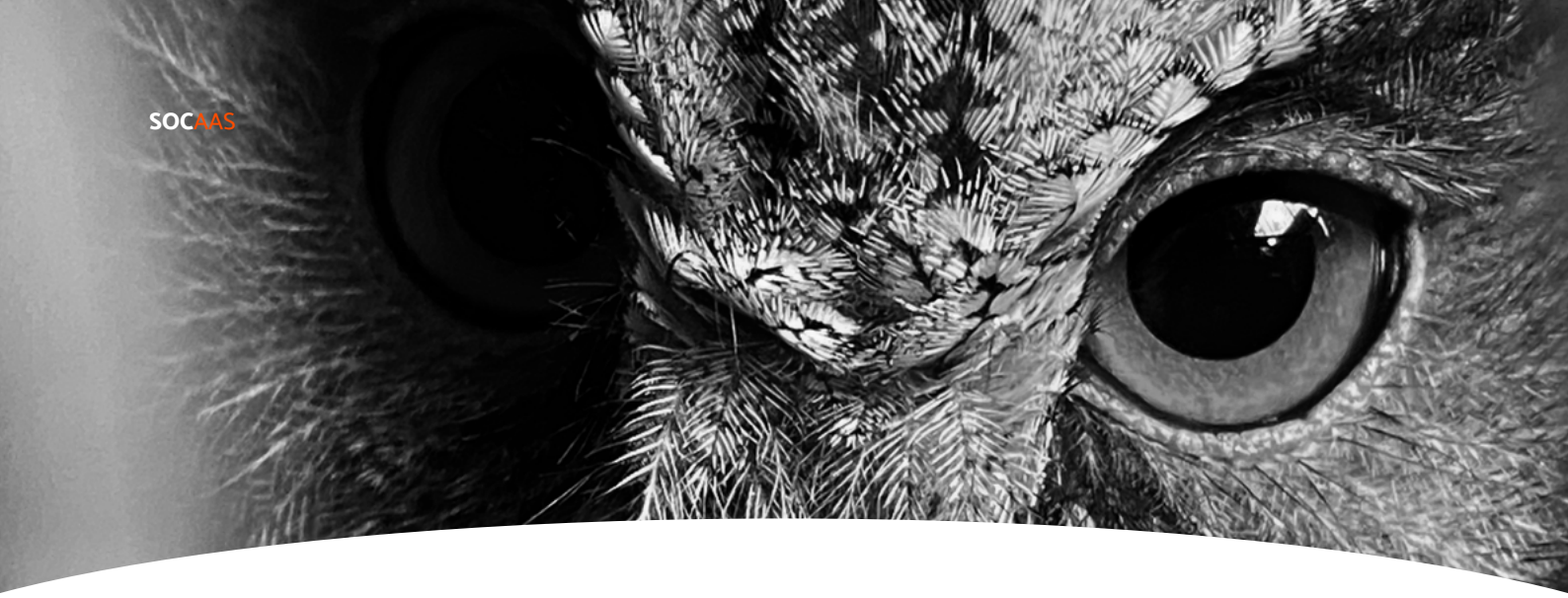
GET CONNECTED • CYBER SAFE

WHAT IS SOCaaS & HOW DOES IT WORK?

Developing and maintaining a Security Operations Centre is a huge investment:

- Identify, monitor, and control cloud applications to reduce shadow IT risks
- Salaries are high for SOC analysts, and a large team required to deliver 24/7
- The security talent pool is shallow which causes recruitment challenges
- Expensive and complex cyber monitoring systems
- Ever increasing, sophistication and velocity of threats
- Evolving regulatory and compliance requirements

A Security Operations Centre (SOC) is a command centre made up of cybersecurity experts responsible for monitoring, analysing, and protecting an organisation from cyber-attacks.



In the SOC, internet traffic, internal network infrastructure, desktops, servers, endpoint devices, databases, applications, IoT devices, and other systems are continuously monitored for security incidents. As a result, it operates 24/7 monitoring and discovery of security issues, providing strong security for an organisation.

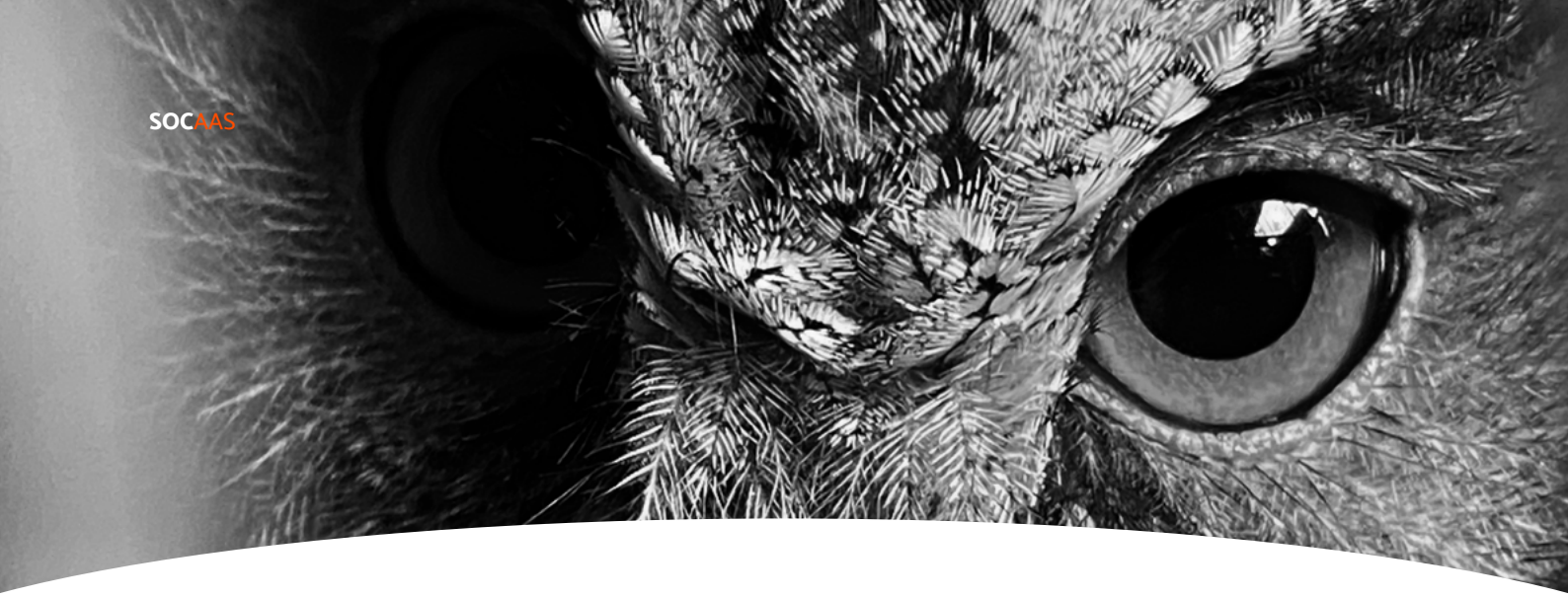
SOCaaS acts as an extension of your security and or IT team, and takes on the overhead of the skilled resources, processes, and technology investment, maintenance, and infrastructure needed to detect and respond to cyber security threats.

SECURITY INFORMATION AND EVENT MANAGEMENT SOLUTION

Security Information and Event Management (SIEM) tools provide the SOC's foundation, given its ability to correlate rules against massive amounts of disparate data to find threats. Integrating threat intelligence adds value to the SIEM activity by providing context to the alerts and prioritizing them.

BEHAVIORAL MONITORING

User and Entity Behavioral Analytics (UEBA), typically added on top of the SIEM platform, helps security teams create baselines by applying behavior modeling and machine learning to surface security risks.



ASSET DISCOVERY

Asset discovery or an asset directory helps you better understand what systems and tools are running in your environment. It enables you to determine what the organisation's critical systems are, and how to prioritise security controls.

VULNERABILITY ASSESSMENT

Detecting the gaps an attacker can use to infiltrate your systems is critical to protect your environment. Security teams must search the systems for vulnerabilities to spot these gaps and act accordingly. Some certifications and regulations also require periodic vulnerability assessments to prove compliance.

INTRUSION DETECTION

Intrusion detection systems (IDS) are fundamental tools for SOCs Security Operations Centre to detect attacks at the initial stages. They typically work by identifying known patterns of attack using intrusion signatures.

THE KEY BENEFITS OF A SOC INCLUDE:

- Uninterrupted monitoring and analysis for suspicious activity
- Improved incident response times and incident management practices
- Reducing the gap between the time of compromise and the time to detect
- Software and hardware assets are centralized for a more comprehensive approach to security
- Effective communication and collaboration to detect and classify adversarial tactics and techniques, e.g., by utilizing the MITRE ATT&CK framework
- Reduction of costs associated with security incidents
- More transparency and control over security operations
- Established chain of custody for data used in cybersecurity forensics

WHY METCLOUD?

WE MAKE IT AFFORDABLE

We deliver the cybersecurity expertise, technology, and infrastructure, 24/7 coverage, and hands-on service necessary to protect any organisation.

Why METCLOUD?

Award winning company for cybersecurity, innovation, and excellence. Our vision is to be the global brand of choice for next generation cybersecure cloud services. Our services have been architected with security by design. Ransomware, Cloud vulnerabilities, Phishing attacks Social engineering and vulnerability management are the five top global security threats. METCLOUD's portfolio of cyber security and cloud services will ensure that you protect, defend, and mitigate any potential cyber attack irrespective of how it was carried out.

Let’s get connected.

Call 0121 227 0730
and speak to one
of our experts.

Email the team.
hello@metcloud.com

Visit our website for
more information.
metcloud.com

METCLOUD

GET CONNECTED • CYBER SAFE

02/2022/V1