cybersecurity associates

SOC Managed Detection and Response Services

Executive Summary

Our fully-managed Security Operations Centre (SOC) solution provides a complete range of protection services including monitoring, managed detection and response (MDR), and prevention to security incidents 24x7x365. In addition we can provide Incident Response (IR) capability, digital forensic analysis, consultancy, design and installation/configuration to support clients' cyber security needs.

- ✓ Security Operations Centre (SOC) manned 24x7x365 by UK Government SC cleared staff
- ✓ Analysis and validation of security events by certified and trained security experts
- ✓ Continuous tuning of events to remove 'false positives'
- ✓ Threat disruption/containment (SOAR) with emergency support for priority incidents
- ✓ Optimised threat-detection with proactive human threat-hunting and advanced behavioural analytics
- ✓ Customizable advanced analytics and bespoke dashboards
- ✓ Dedicated communications channel for Clients to talk directly to SOC analysts
- ✓ Monthly security reporting
- ✓ Fully managed and audited ticketing system (aligned to ITSM)

SOC MDR Benefits:

- Continuous monitoring and management of security events
- End to end management of security incidents
- Reduced security risk and impact of incidents
- Flexible and scalable solution
- Full system deployment and configuration (turnkey technology stack)
- Cost-efficient SOC-as-a-Service with full managed SIEM solution
- Improved threat response
- Proven technology platform to drive extended visibility and operational excellence
- Strong data governance, with data residing in clients tenant and not migrated to 3rd party service
- An inherently improved security posture, reducing the risk of data breaches and cyber threats.

Microsoft SentinelOne APPGUARD The Malware Disruptor

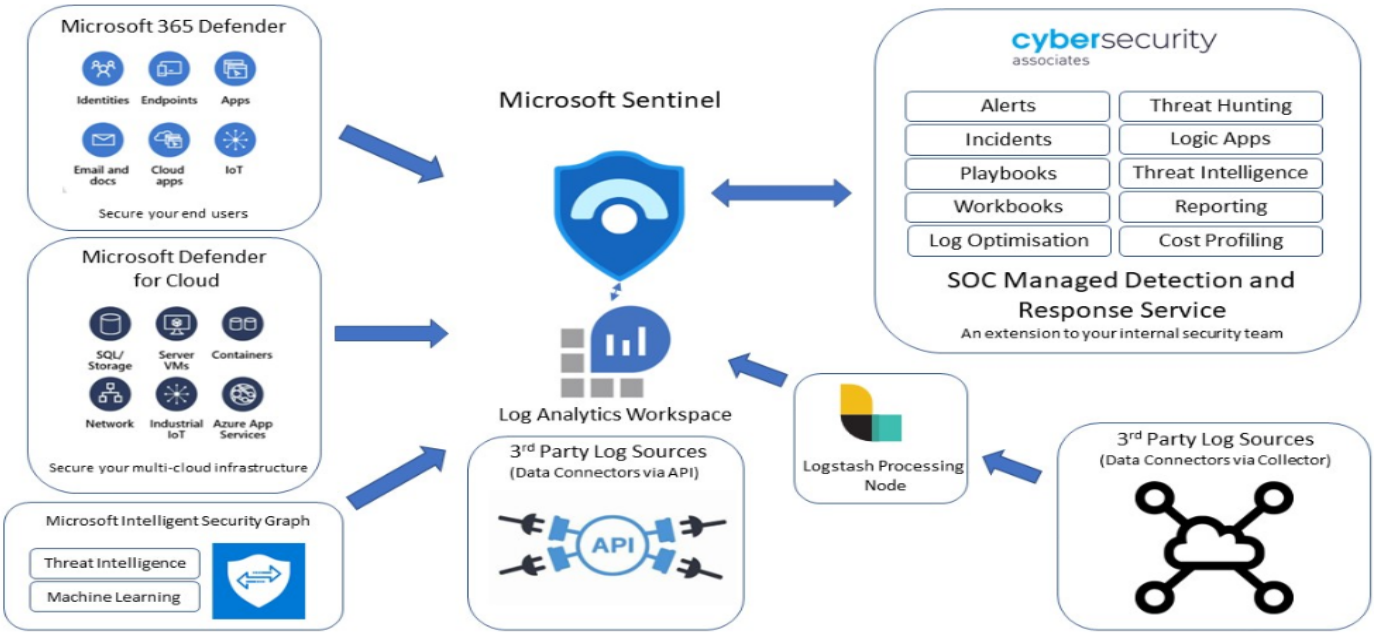
SOC Services	24x7 Monitoring 365 days a Year	Managed Detection & Response	Trained and Certified Analysts	Continuous Tuning & Reporting	Advanced threat feeds and analytics

www.csa.limited
+44(0) 300 3034691

Our Services & Approach

We work closely with our clients to understand their needs and expectations as part of every engagement, and ensure any significant objectives and milestones are understood. Our SOC services in more detail cover:

- **24x7x365 Monitoring:** Persistent, Nonstop Cyber Security Surveillance, the SOC diligently oversees the complete extended IT ecosystem, including applications, servers, system software, computing devices, cloud workloads, and the network. This vigilant monitoring occurs around the clock, 365 days a year to guarantee an efficient and effective service.
- **Managed Detection and Response:** Our trained analysts comb through your digital landscape 24/7 perpetually putting you ahead of the cyber threat. We craft bespoke remediation plans—whether it's isolating compromised systems, or disabling user accounts. Your security, our priority.
- **Trained and Certified Analysts:** Our MDR services are backed by experienced security analysts who understand the intricacies of threat landscapes. Their insights, and qualifications combined with automation, enable efficient threat hunting and incident analysis.
- **Continuous Tuning & Reporting:** Threats morph incessantly. Adversaries relentlessly explore both familiar and uncharted avenues to infiltrate systems. Our commitment is to outpace these threats by perpetually refining your platform. As novel techniques and tactics emerge, we adapt swiftly, ensuring detection capabilities for the digital environment. But how do we transform raw data into meaningful guidance? We distill vast information repositories into actionable insights and targeted reports.
- **Advanced Threat Feeds and Analytics:** Our SOC services blends and utilises a range of researched open and closed source threat intelligence feeds enabling robust contextualisation and threat identification with high levels of confidence. Our extensive analytic and automation playbook library offers a diverse range of functionality and detection capabilities. Continuously being developed and designed with intention, built upon use cases to fulfil their maximum potential and ensure our clients are safeguarded against cyber threats.



Case Study: Construction

The project with CSA was prompted by a major contract win to construct datacentres for a prominent US company, necessitating heightened security measures to protect sensitive project information.

The Company sought a comprehensive solution that addressed specific requirements, including special data residency considerations, the flexibility of mixing storage options to reduce costs, scalability to accommodate future growth, and the capability to seamlessly transition the management of the SIEM from CSA to the company if they decided to establish its own internal security team in the future.

The main insight from this engagement was that by leveraging the investment in Microsoft E5, the customer was able to realise almost instant value.

Endorsement

"I think CSA's main strength is the expertise they have in the cyber risk industry and the knowledge they bring in. This stems from the background that they've had, its just amazing what they know. It's reassuring to me knowing that they are the experts".

IT Officer, Local Authority

www.csa.limited
+44(0) 300 3034691