cybersecurity associates

Incident Response Services

Executive Summary

SureCloud Cyber Services have an experienced team capable of offering a dedicated suite of Incident Response and proactive services. Our experienced team of consultants, backed by our dedicated in house SOC, are able to meet the response needs of your organisation.

Whether you want to be prepared in case of a breach by securing our incident response retainer service, or are looking for a programme to increase your internal resilience and readiness against potential incidents, SureCloud Cyber Services is able to help with our combined proactive and reactive capabilities:

- ✓ **24/7** on-call initial response support to cyber incidents via teleconference or video conference.
- ✓ **18 hour travel-reaction time** for one of our responders to be on their way to you, whatever the situation
- ✓ Full suite of proactive and reactive incident management capabilities including Threat Hunting, Tabletops, IR Plans, Purple Teaming
- ✓ Backed and supported by CSA's industry-leading managed SOC and penetration testing teams
- ✓ Capability to bring SME support across all areas of cyber security
- ✓ All UK-based, security cleared staff

Incident Response Benefits:

- Peace of mind knowing that should the worst happen, you have a dedicated team to call and respond to your needs
- Immediate leadership and support for any confirmed cyber incident
- Improved organisation and communication skills internally through simulated exercises
- Increased staff knowledge and preparedness through standard operating procedures
- Human led investigations backed by industry leading tools and experience
- Post incident analysis and reports to allow for follow up activities and board reporting

CREST VA PEN TEST STAR

Assured Service Provider
in association with National Cyber Security Centre
CHECK Penetration Testing

Incident Response Retainers	Emergency Incident Response	Threat Hunting	IR Tabletops & Live-ranges	IR Plans & Runbooks	Purple Teaming & Ransomware Simulation

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 services include, but are not limited to:

- **Incident Response Retainers:** Our leading incident response offering, providing you with a dedicated phone number, and a travel response time within 12 hours, you know that you are covered. Our retainer service is tailored to you, and offers a credit system to allow you the flexibility to use our time for other incident-preparedness activities such as Tabletops, Threat Hunting and even Purple Teaming to ensure your teams are as ready as possible to face any threat.

- **Emergency Incident Response:** Should an incident strike at an unsuspecting time, SureCloud Cyber Services can be engaged to conduct emergency incident response for your business, allowing rapid response, investigation and triage, subject to availability.

- **Threat Hunting:** Sometimes when it comes to investigating a potential breach, it's not easy to know whether a system or network is compromised. We offer a Threat Hunting service which deploys a gamut of industry-leading tools to analyse activities on systems, applications and networks, review threat intelligence, and even scan for vulnerabilities, backed by our consultant's expertise to give you clarity on the health of your network.

- **IR Plans and Runbooks:** Having prepared staff with a go-to- action plan plays a huge part in the efficacy of responding to incidents. We offer creation incident response runbooks, as well as broader plans and policies such as IR Plans and Business Continuity Plans. These documents are created and tailored to your business's capabilities and structure.

- **Tabletops and Live-ranges:** Do you know how well your staff know their responsibilities, who and how to escalate? Would you know what to do in a business continuity event? We offer incident tabletop exercises to simulate the order of events as they might unfold in the real world, starting with technical triage, working through to needing to engage with potential third-parties and even senior stakeholder management to invoke business continuity. For the particularly daring, we offer a hands-on live-range engagement, where we will test your team's capability to respond in a hands-on-keyboard environment with our pentest team acting as a malicious actor inside the network.

- **Purple Teaming & Ransomware Simulation:** Our in-house penetration testing and SOC team are able to conduct purple-teaming engagements to test the effectiveness of your security team and recommend improvements. Our own SOC MSP expertise can be leveraged to further assist with detection engineering and overall alerting and monitoring.

Case Study: Network Compromise

SureCloud Cyber Services responded to an incident where a suspected network breach had caused a critical database to go offline. A ransomware note was left on the server. Our engagement took the reins to provide initial triage and immediate actions during the incident, and to conduct an investigation to look for the root cause of the breach, search for any indicators of continued compromise and advise on further actions and hardening to take place against affected assets and network segments to reduce any risk of reinfection or further breaches.

Case Study: Major Incident Management

SureCloud Cyber Services staff have experience handling major events and critical infrastructure at key times, including dealing with live analysis and monitoring of dynamic networks where there is vested interest from hostile organized crime groups and nation states to conduct cyber warfare. In one instance while providing security coordination, an adjacent but unconnected public-facing system was compromised, and terrorism-related threats were spread at large scale rapidly. The onsite consultants responded immediately to this information, conducted root cause analysis of how access was gained and where the content was being hosted, and the immediate incident was contained within 20 minutes. Post-incident, additional measures were made to monitor adjacent systems and networks and maintain operational resilience of the networks.

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