CSACyber | G-Cloud

SERVICE DESCRIPTION

CSA Purple Team Engagement

The CSA Purple Team service is a collaborative, threat-led engagement that brings together CSA's offensive security specialists (Red Team) and defensive operations analysts (Blue Team) to jointly test, measure and improve an organisation's detection and response capability.

Instead of focusing solely on compromise (Red Team) or reviewing controls (Blue Team), Purple Teaming delivers an iterative cycle of execute → detect → tune → retest, ensuring every tested attack technique results in measurable uplift.

Using MITRE ATT&CK-aligned scenarios, real adversary TTPs and threat-informed hypotheses, CSA safely emulates attack chains across endpoint, identity, email, network and cloud environments. Each technique is validated against actual detections, telemetry and response workflows, highlighting blind spots, misconfigurations and opportunities for engineered improvements.

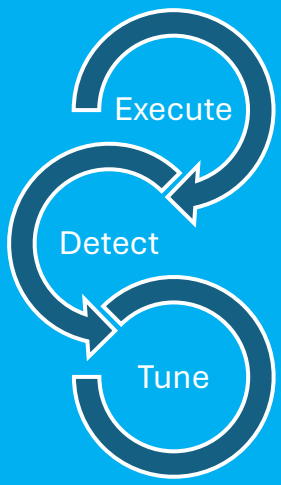
The service directly strengthens SOC/MDR effectiveness by:

- Validating use cases, detections and alert logic
- Tuning SIEM/EDR/SOAR rules and response playbooks
- Improving analyst triage and investigation workflows
- Mapping detection coverage to ATT&CK for measurable maturity tracking
- Building shared understanding between offensive and defensive teams

References and case studies can be provided on request.

BENEFITS

- Threat-led | *We bring threat intelligence into each of our Red Team and Cyber Readiness engagements, ensuring the engagement is tailored to the exact types of threat actor your organisation is likely to face*
- Collaborative approach | *We work directly with internal teams to improve defensive controls and detection and response capability through our Purple Team approach, strengthening Cyber Resilience*



CREST Security Operations – Security Operations Centre
CREST Incident Management – Incident Response
CREST Security Testing – Penetration Testing
CREST Red Teaming – Intelligence-led Pen Test
CREST Security Testing – Vulnerability Assessment

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

Assured Service Provider – in association with National Cyber Security Centre – Cyber Incident Response: Standard Level

Cyber Essentials

Cyber Essentials Plus

hello@csacyber.com
csacyber.com
0300 303 4691