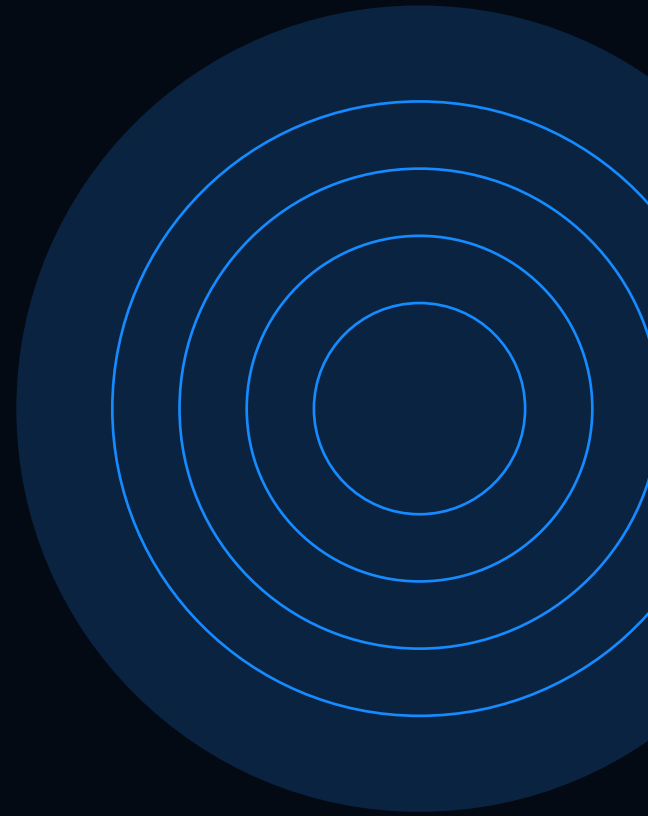




CYBER DEFENCE

Cyber Defence & SecOps

Operational defence, security operations engineering, adversary validation and incident readiness.



MAKE THE ADVERSARY WORK FOR IT.

C3SA combines security operations engineering, threat intelligence, adversary-led testing and response readiness to help organizations detect, disrupt and recover from cyber threats.

SECOPS MODERNIZATION Architecture, SIEM/SOAR/XDR engineering, detection content and operating-model improvement.	THREAT INTELLIGENCE External threat, exposure, dark-web and adversary context translated into operational decisions.
RED / PURPLE TEAMING Adversary-led testing that connects attack paths to detection and response improvement.	THREAT HUNTING Proactive investigation for hidden compromise, suspicious behaviour and attacker persistence.
SECURITY VALIDATION Breach and attack simulation, control validation and evidence-driven improvement.	INCIDENT READINESS Playbooks, tabletop exercises, live-fire training and CyberFIRE response capability.

A DEFENCE OPERATING LOOP

Effective cyber defence is a continuous system: intelligence informs priorities; engineering creates telemetry and controls; adversary testing exposes gaps; response evidence drives improvement.

Collect the telemetry and external intelligence required to understand exposure and

Focus detections and controls on material threats, critical assets and plausible att

Engineer detection logic, correlation and investigation workflows.

Test controls and detections against realistic adversary behaviour.

Contain, investigate, eradicate and recover with clear authority and evidence.

Feed lessons back into architecture, detection content, procedures and readiness

SECURITY OPERATIONS TRANSFORMATION

C3SA supports organizations moving from tool-centric monitoring toward an integrated defence capability.

Architecture Telemetry, data pipelines, trust boundaries, cloud/endpoint/network/identity sources and retention.	Detection Engineering Use cases, correlation, YARA-L/SIEM content, tuning and measurable detection coverage.
Automation SOAR workflows, enrichment, triage, containment and analyst-assist patterns.	Operations Roles, escalation, playbooks, case management, service levels and governance.
Validation Purple teaming, BAS, adversary emulation and control testing.	Metrics Evidence that measures coverage, response performance and residual risk rather than alert volume alone.

5D CYBER DEFENCE

C3SA uses layered defensive thinking to make attacker progress harder, slower and more visible.

DENY Prevent unauthorized access and reduce exposed attack paths.	DELAY Increase the time and effort required for an adversary to progress.
DISRUPT Break attacker infrastructure, access, tooling or operational momentum.	DECEIVE Use controlled deception and instrumentation to expose adversary behaviour.
DEFEND Coordinate people, process and technology around mission-relevant threats.	RECOVER Restore operations and incorporate lessons into the next defensive cycle.

WHEN AN INCIDENT IS ALREADY UNDERWAY.

Cyber defence planning must connect to response. C3SA's CyberFIRE capability supports rapid investigation, containment, recovery and the transition from incident evidence into longer-term remediation.

Start with the operational question: What must we detect, what must we protect, and what must still function when the attacker is already inside?

c3sa.com/cyber-defence