360 DEFENCE (UK) LTD – SERVICE DEFINITION

C3a. Threat Assessment – Enhanced (TxA-E)

Service attributes	
Service type	Lot 3: Cloud Support
Service name	
Service name	C3a. Threat Assessment – Enhanced (TxA-E)
About 360D Service 360 Defence (UK) Limited (360D) delivers defence grounded in threat-informed, attacker-shaped understanding of cyber, security and risk. We are specialists in adversary-centric analysis, decision-grade risk clarity and assurance-aligned outcomes, built on the principle that context, definitions and situational understanding are essential to defensible security.	
Service description	**You are a target.** Threat Assessment – Enhanced (TxA-E) confirms or refreshes the threat baseline, then applies real-world Threat Groups aligned to TxA threats, including their campaigns, software, tooling and producers. This attacker-informed view enables defensive actions that protect against multiple threats by disrupting shared attacker behaviours.
Service categories	• Cloud Support Services

	○ Security Services ○ Security Strategy ○ Security Risk Management ***This service is delivered under Cloud Support and does not include hosted platforms or managed services.***
Service features and benefits	
Features	• Confirm or refresh Threat Assessment (TxA) baseline • In-depth threat capability review , update and alignment to groups • Analyse threat groups, behaviours and usage patterns • Identify shared offensive DNA across multiple adversaries • Apply defensive improvements apply across multiple adversaries using shared approaches • Produce intelligence suitable for operational consumption • Enable updates to Threat Modelling and Risk Assessment • Defender-Led attacker-informed analysis using professional analyst judgement
Benefits	• Intelligence that can be acted on, not just read or stored. • Reduced complexity through collapsed and prioritised threat space for defenders. • Single defensive actions reduce exposure to multiple attacker-relevant threats. • Strengthens threat intelligence, enhances SOC performance, improving organisational risk management.. • Improves prioritisation of mitigations and detections based on attacker behaviour.

	• Supports proactive and reactive defence through attacker-aligned, pre-emptive defensive improvement.
Service Delivery benefit	• You are a target. TxA-E confirms or refreshes the threat baseline, then applies real-world Threat Groups aligned to TxA Threats, including their campaigns, software, tooling and producers. This attacker-informed view exposes the shared behaviours and offensive patterns that cut across multiple adversaries, enabling defensive actions that reduce risk across many threats simultaneously. • TxA-E goes deep into the fine-grain reality of how adversaries operate: what they target, how they run campaigns, the tooling they rely on, and the behaviours they consistently repeat. This level of analysis provides decision-grade clarity, allowing organisations to prioritise defences that disrupt multiple threats at once rather than responding to individual threats in isolation.
Service Implementation Planning	• Initial scoping discussion to confirm objectives, boundaries and context • Analyst-led, attacker-informed assessment conducted offline using structured threat methodology • Review of relevant contextual material and existing threat or risk documentation (where available) • TxA-E produced using attacker-led analysis and PHIA likelihood language • Delivery of written Threat Assessment report with optional briefing (remote by default; face-to-face by agreement)

	•
Service scope	
TxA-E	**TxA-E** includes confirmation or refresh of the existing Threat Assessment (TxA) to establish a current, evidence-based threat baseline. It then applies enhanced analysis of real-world Threat Groups, their behaviours, usage patterns and defender implications, reflecting how adversaries operate in practice and what their campaigns, tooling and approaches mean for the assessed organisation. TxA-E does not conduct a formal Risk Assessment (RxA) or score controls or countermeasures. Instead, it provides attacker-informed, evidence-led insight that supports control/countermeasure improvement, prioritisation and operational change by showing how real threats behave and which defensive measures matter most to the defending organisation. Outputs inform operational threat intelligence, defensive capability development, Threat modelling (TxM), Risk Assessment (RxA), and wider assurance and security operations activities.
Service constraints	Dependent on timely provision of contextual information. Delivery is primarily analyst-led and conducted offline, with optional remote briefing of findings.
Do you hold a suitably scope ISO27001 certificate for this G-Cloud Service.	ISO27001 is not applicable to this service. It is a skills-based service with no hosted platforms, operational systems or data custody.

Relevant information surrounding our service in relation to Government Classification Scheme	360D security specialists include NCSC Lead Certified Cyber Practitioner (and equivalent) professionals with information assurance and cyber security expertise to support the design, development and operation of systems handling information up to **SECRET**, in accordance with applicable HMG policies and client requirements.
Details of the level of backup/restore and disaster recovery that will be provided;	**This does not apply to this risk management service provision** Not applicable (The service involves with no hosting, platform operation or data custody.)
On-boarding and Off-boarding processes/scope etc.;	**On-boarding:** Initial engagement to confirm scope, baseline status and organisational context. Agreement of Information handling expectations and delivery timelines. Limited client interaction required beyond provision of contextual material. **Off-boarding:** Formal handover of Threat Assessment enhanced report and supporting outputs. Optional briefing on findings, baseline confirmation and recommended next steps.
Consumer responsibilities:	Provide relevant contextual information and a nominated point of contact. Supply any existing threat assessment or related material to support the organisations current baseline. **Details of any trial service available:** Not applicable (this is a skills-based service).

Reselling	
Supplier Type	360D is not a reseller
User Support	
Email or ticketing support	No
Phone support	No This service does not include a standing helpdesk or call-out capability. Support relates solely to engagement coordination and delivery of agreed outputs.
Web chat support	No
Support levels	*This service does not include a standing user helpdesk; support relates to engagement coordination only.* Named service lead responsible for delivery and quality assurance. Single-point coordination for scope clarification, report delivery, and optional briefing.
Financial Recompense	
Financial recompense model for not meeting service levels:	Any recompense for not meeting agreed service levels is defined in the contract and confirmed at call-off. Termination terms are defined in **360 Defence Terms and Conditions**.

Termination terms: By consumers (i.e. consumption); and By the Supplier (removal of the G-Cloud Service):	See 360 Defence Terms and conditions
Data restoration / service migration	Not applicable (no data hosting or migration deliverable).
Staff Security	
Staff Security Clearance	Staff screening performed which conforms to BS7858:2019
Government security clearance	Up to Developed Vetting (DV)
Pricing	
Discount for educational organisations	Yes Pricing (including unit prices, volume discounts (if any), data extraction etc.) Pricing is based on SFIA-aligned effort and does not include fixed-price deliverables unless explicitly agreed at call-off.
Documents	
Service definition document	This document

Terms and Conditions	See 360D terms and conditions separate document
Pricing document	Our prices are published in the 360D G-Cloud pricing and SFIA rate card document/matrix. Pricing is based on role and effort. We may offer fee discounts where an individual resource is contracted for engagements exceeding 60 full working days, subject to agreement at call-off.