Amethyst Cyber Group
Common Sense Cyber Security

CLIENT CONFIDENTIAL

PREREQUISITES CHECKLIST

Purple Team Prerequisites

Information, access, and defensive context required before a purple team exercise begins.

CLIENT	DOCUMENT REF
[Client Organisation]	ACG-PRE-PT2
VERSION	**ISSUED**
2.0	June 2026

Purpose. Purple team exercises are collaborative — both offensive and defensive teams participate openly. Complete this checklist before the exercise begins to ensure the defensive environment is properly understood.

Purple Team Prerequisites

Purple team exercises are transparent and collaborative. Both the red and blue teams work together openly — the aim is detection improvement and knowledge transfer, not stealth. Complete all sections before the exercise begins.

Contacts and Environment Access

- [ ] Provide a named project contact, technical escalation contact, and an emergency stop contact with direct phone numbers.
- [ ] Provide the lead defender contact: the individual who will attend joint sessions and liaise with the ACG team on detection outcomes.
- [ ] Confirm agreed exercise dates, session format (full-day, half-day, remote, on-site), and the number of sessions planned.
- [ ] Confirm test account provisioning: provide domain user accounts, cloud identities, or application accounts as required for the techniques being exercised.
- [ ] Confirm VPN or network access to the exercise environment if sessions are conducted remotely.
- [ ] Do not send credentials or access material by email — use the agreed secure channel.

Defensive Stack and Visibility

- [ ] Provide details of all security tooling in use: EDR platform (vendor and version), SIEM (vendor and log sources), NDR, email security, cloud security posture tool, and identity protection tools.
- [ ] Confirm which log sources are currently ingested into the SIEM: Windows Event Logs, Sysmon, PowerShell logging, network flow, DNS, proxy, cloud audit logs, and identity logs.
- [ ] Confirm whether PowerShell ScriptBlock logging, Module logging, and Transcription logging are enabled on endpoints.
- [ ] Confirm whether command-line argument logging (e.g., Process Creation event 4688 with full command line) is enabled in Windows audit policy.
- [ ] Confirm whether network traffic logging (NetFlow, Zeek, packet capture) is available and from which vantage points.
- [ ] Identify known logging gaps before the exercise — areas where visibility is absent or limited, so the exercise can focus on improving coverage.
- [ ] Provide the SIEM / SOC analyst contact who will be joining the live sessions to observe alerts and tune rules in real time.
- [ ] Confirm the EDR platform's prevention vs. detection mode during the exercise — note any policies that may automatically block techniques being exercised.

MITRE ATT&CK Technique Selection

- [ ] Confirm the tactic and technique scope for the exercise: which ATT&CK categories are prioritised (e.g., Initial Access, Execution, Persistence, Privilege Escalation, Lateral Movement, Exfiltration).
- [ ] Identify the highest-priority techniques to validate detection coverage for, based on the client's threat intelligence or sector risk profile.

- [ ] Confirm whether sub-techniques should be tested at a granular level (e.g., specific credential access methods) or at a higher tactic level.
- [ ] Confirm whether any techniques are explicitly excluded due to environment risk (e.g., no data staging, no account manipulation in production).
- [ ] Confirm whether the exercise will test cloud-specific techniques (e.g., Entra ID token theft, AWS role assumption abuse, S3 enumeration) alongside endpoint techniques.

Exercise Format and Workshop Setup

- [ ] Confirm the exercise format: live fire (real-time execution and detection), atomic testing (tool-driven individual technique tests), or a blend of both.
- [ ] Confirm whether a test environment (lab, dedicated VM estate, sandbox tenant) is available, or whether exercise activity will occur in a production environment with appropriate safeguards.
- [ ] Confirm whether the exercise includes a knowledge-transfer workshop component — where techniques are explained, detection logic is reviewed, and detection rules are written or tuned live.
- [ ] Confirm attendees for joint sessions: SOC analysts, detection engineers, threat intelligence staff, and any platform owners whose tools are in scope.
- [ ] Confirm the expected artefacts at the end of each session: detection rule drafts, coverage heat map update, gap register, and any playbook additions.

Measurement and Improvement Tracking

- [ ] Confirm the baseline detection coverage measurement: how current detection is scored before the exercise begins (e.g., ATT&CK Navigator heat map, SIEM alert mapping).
- [ ] Confirm how improvement will be measured at the end of the exercise: new rules created, detection coverage percentage increase, mean time to alert for exercised techniques.
- [ ] Confirm whether a post-exercise follow-up session is required to validate that newly created detection rules perform correctly in production.
- [ ] Confirm the report format: a coverage gap analysis, technique-by-technique detection outcome log, and recommended detection engineering roadmap.