AUTHORIZED SECURITY VALIDATION

RedCore
Customer Onboarding Pack

Commercial discovery, authorization, Rules of Engagement, customer runner acceptance, findings, retest, and closure.

Version 1.0 / 11 August 2026
Status: Evaluation template - legal review required

Customer: _____
Engagement: _____

IMPORTANT: This pack does not authorize testing. No execution may begin until the applicable agreements, Authorization to Test, Rules of Engagement, and deployment acceptance are completed by authorized representatives.

Pack contents

1. 00 Discovery Questionnaire
2. 01 Pilot Proposal Template
3. 02 MSA and Data Protection Terms Draft
4. 03 Statement of Work Template
5. 04 Authorization to Test
6. 05 Rules of Engagement
7. 06 Customer Runner Deployment Approval
8. 07 Finding Acceptance Retest and Closure
9. 08 Vendor Security Response

RedCore sales discovery questionnaire

Status: Pre-contract intake. Do not include credentials, vulnerability details, production data, personal data, secrets, or exploit material.

Organization

- Legal company name:
- Trading name:
- Headquarters jurisdiction:
- Website:
- Primary business contact, title, email, phone:
- Security/technical contact, title, email, phone:
- Procurement/legal contact, title, email, phone:
- Approximate employee count:
- Industry and regulated activities:

Business outcome

- What decision or event is driving the assessment?
- What must be true at the end for this engagement to be successful?
- Is the need a pilot, release gate, remediation retest, compliance input, or recurring program?
- Desired start and completion windows:
- Required report audience: executive, engineering, audit, customer, regulator, other:
- Required report formats: Markdown / HTML / PDF / JSON / SARIF:

High-level scope

- Asset classes: web / API / source / cloud / identity / network / Kubernetes / other:
- Approximate number of applications, repositories, domains, IP ranges, or accounts:
- Environments: lab / staging / production:
- Are any targets operated by a third party? If yes, who provides written approval?
- Are cloud-provider testing notifications or approvals required?
- Will personal, payment, health, student, employee, export-controlled, or customer data be reachable?
- Known blackout periods and sensitive business processes:

Deployment and data handling

- Preferred execution: RedCore-managed / customer runner / undecided:
- Runner platform: Windows with WSL2 / Linux / Docker / Kubernetes / undecided:
- Can the runner make outbound HTTPS connections to the control plane?
- Required data mode: findings only / approved evidence / full artifacts by exception:
- Required data residency, retention, encryption, or deletion controls:
- Customer identity, logging, ticketing, or report-delivery requirements:

Safety and approvals

- Who can legally authorize the test?
- Who can stop testing at any time?
- Are authentication, password testing, exploitation, lateral movement, social engineering, wireless, physical, denial-of-service, or destructive techniques requested?
- Required insurance, certification, background-check, or subcontractor conditions:
- Date questionnaire reviewed with customer:
- RedCore owner and next action:

RedCore scoped pilot proposal

Status: Commercial template. Not an Authorization to Test. Legal and pricing review required.

Proposal record

- Proposal ID / version / date:
- Customer legal name:
- RedCore commercial owner:
- Valid until:
- Confidentiality basis:

Executive outcome

Describe the business decision the pilot supports, the approved system class, and the evidence the customer expects. Do not list target credentials or secrets.

Proposed engagement

- Service: Application security pilot / Application + source / Customer runner evaluation / Other
- Indicative duration:
- Expected customer start prerequisites:
- Included analyst review and meetings:
- Included report formats:
- Included retest window:
- Proposed execution location:
- Proposed data mode:

Deliverables

1. Kickoff and final scope confirmation.
2. Runner deployment and acceptance record where applicable.
3. Human-reviewed technical findings with evidence and remediation guidance.
4. Executive summary and risk themes.
5. Retest record for agreed fixes within the stated window.
6. Engagement closure and data disposition confirmation.

Explicit exclusions

Anything not listed in the signed SOW and Rules of Engagement is excluded. Denial of service, destructive actions, persistence, social engineering, physical testing, wireless testing, password spraying, production exploitation, and access to sensitive data are excluded unless expressly approved.

Commercial structure

- Professional fee and currency:
- Taxes:
- Payment schedule:

- Travel or third-party costs:
- Change-request rate or method:
- Cancellation/rescheduling terms:

Assumptions and dependencies

- Customer supplies timely authority, owners, access, test accounts, and approvals.
- Tool availability is certified on the selected runner; registry presence alone is not availability.
- Dates move when prerequisites or approvals are delayed.
- Findings are security observations, not a guarantee that no other vulnerability exists.
- Service begins only after all required contracts and authorization documents are signed.

Accepted for proposal development only:

Customer name / title / date: _____

RedCore name / title / date: _____

Master services and data protection terms - drafting checklist

Status: Counsel-owned draft checklist, not legal advice and not ready for signature without jurisdiction-specific legal review.

Master services agreement terms

Counsel should draft and approve, at minimum:

- Correct legal names, addresses, signatory authority, order of precedence, and affiliates.
- Service standard, customer dependencies, change control, acceptance, delays, and subcontractors.
- Fees, invoices, taxes, expenses, late payment, suspension, and termination.
- Customer warranties of authority and third-party/provider permissions.
- Confidentiality, compelled disclosure, residual knowledge, and publicity restrictions.
- Background IP, customer materials, deliverable ownership/license, feedback, and open-source components.
- Security obligations, incident notice, vulnerability handling, audit evidence, and access controls.
- Privacy roles, processing instructions, subprocessors, transfers, data-subject requests, and deletion.
- Warranties, disclaimers, indemnities, liability cap, excluded damages, insurance, and force majeure.
- Export controls, sanctions, anti-bribery, acceptable use, governing law, disputes, and notices.

Data protection schedule

- Controller / processor roles:
- Processing subject and duration:
- Purpose and nature of processing:
- Data subjects and data categories:
- Special/sensitive data expected: Yes / No; safeguards:
- Approved processing and storage locations:
- Approved subprocessors and notice/objection process:
- International transfer mechanism:
- Encryption and key ownership:
- Customer runner data mode:
- Evidence/artifact upload policy:
- Access roles and authentication:
- Logging and audit requirements:
- Security incident notification contacts and deadline:
- Data-subject request assistance:
- Retention schedule by data class:
- Return/deletion method and certification:
- Backup deletion limitations:

Required attachments

1. Executed Statement of Work.

2. Authorization to Test.
3. Rules of Engagement.
4. Asset inventory and data-flow register.
5. Customer runner approval where applicable.
6. Subprocessor and processing-location list.
7. Security control schedule and incident contacts.

Counsel approval: _____ Date: _____

Statement of Work

Status: Contract template. Legal and commercial approval required. This SOW does not replace the separate Authorization to Test and Rules of Engagement.

Parties and precedence

- SOW ID / version / effective date:
- Customer legal name and address:
- RedCore contracting entity/name and address:
- Governing master agreement and date:
- Order of precedence for conflicts:

Objectives and success criteria

- Business objective:
- Assessment type:
- Success criteria:
- Assumptions:

Services and phases

1. Discovery and scope validation.
2. Authorization and Rules of Engagement approval.
3. Runner deployment/certification where applicable.
4. Controlled assessment and evidence capture.
5. Analyst validation and report production.
6. Readout, remediation consultation, and agreed retest.
7. Closure, access revocation, and data disposition.

Scope summary

- Engagement ID and tenant ID:
- Included asset inventory attachment:
- Explicit exclusions:
- Environments:
- Testing start/end dates and time zone:
- Allowed daily windows and blackout dates:
- Approved accounts/roles (references only, never credentials):
- Approved technique categories:
- Prohibited technique categories:
- Maximum rates/concurrency:
- Production safeguards:

Deployment and data

- Execution target: RedCore-managed / customer runner:
- Runner ID/platform/location:
- Required certified capabilities:
- Data mode: local/findings-only / evidence / full artifacts by exception:
- Approved report/evidence transfer path:
- Retention and deletion schedule:
- Customer data owner:

Deliverables and acceptance

- Deliverables and formats:
- Draft review date:
- Final readout date:
- Customer review period:
- Acceptance criteria and deemed-acceptance rule:
- Included retest scope and expiry:
- Excluded deliverables:

Governance

- Customer engagement owner:
- RedCore engagement owner:
- Technical contacts:
- Emergency stop contacts and channels:
- Status cadence:
- Change request approvers and process:
- Incident/escalation process:

Fees

- Fixed/time-and-materials fee:
- Currency, tax, payment milestones, expenses:
- Reschedule/cancellation/change terms:

Signatures

By signing, each representative confirms authority to bind the named party. Testing remains prohibited until the Authorization to Test and Rules of Engagement are also fully executed.

Customer authorized representative: _____ Date: _____

RedCore authorized representative: _____ Date: _____

Authorization to Test

Status: Required signed authority. Obtain qualified legal review. Do not test until RedCore has verified the signer, asset ownership/authority, dates, and all required third-party approvals.

Authorization record

- Customer legal name:
- Authorizing representative, title, email, phone:
- Basis of authority over the assets:
- Engagement ID / SOW ID / RoE version:
- Authorization start/end timestamps and time zone:

Authorized assets

The signed forms/asset_scope.csv is incorporated by reference. Only rows with authorization_status=approved and an unexpired testing window are authorized.

- Approved domains/URLs:
- Approved IPs/CIDRs:
- Approved applications/APIs:
- Approved cloud accounts/subscriptions/projects:
- Approved repositories and branches:
- Approved identity/network/Kubernetes environments:
- Explicitly excluded assets, tenants, regions, data sets, and third parties:

Authorized activities

Check and initial each category:

- [ ] Passive reconnaissance
- [ ] Active discovery and service identification
- [ ] Authenticated application/API testing
- [ ] Non-destructive vulnerability validation
- [ ] Source/dependency analysis
- [ ] Cloud/IAM configuration review
- [ ] Controlled exploitation of named findings
- [ ] Credential testing under specified accounts/rates
- [ ] Lateral movement within specified boundaries
- [ ] Social engineering under a separate approved scenario
- [ ] Denial-of-service or destructive simulation under a separate safety plan

Anything not checked and further constrained in the Rules of Engagement is prohibited.

Customer representations

The customer represents that it has authority to grant this permission, has obtained required owner/provider approvals, has notified appropriate operations and monitoring teams, and will maintain reachable emergency contacts. The customer may stop work at any time through the agreed channel.

Limits

This authorization does not permit activity outside the signed scope, dates, methods, rates, or data rules; create immunity from law or third-party terms; or authorize independent testing by anyone other than the named RedCore personnel and approved runner identities.

Customer authorized representative: _____

Signature / date / time zone: _____

RedCore acceptance and authority verification: _____

Date / verification evidence reference: _____

Rules of Engagement

Status: Required operational control document. Must match the signed SOW and Authorization to Test. Any ambiguity resolves to no action until clarified in writing.

Identity and control

- Engagement ID / tenant ID / policy version:
- Customer owner / RedCore owner:
- Authorized runner IDs:
- Approved operator identities/roles:
- Start/end timestamps and time zone:
- Daily windows and blackout periods:

Target scope

- Incorporated asset inventory version/hash:
- Allowed target selectors:
- Excluded targets and adjacent systems:
- Redirect, CDN, shared-host, SaaS, cloud, and third-party handling rule:
- Newly discovered assets: stop / document only / written approval required:

Technique policy

For each category record Allowed / Prohibited / Approval-required, plus limits:

- Reconnaissance and OSINT:
- Port/service discovery:
- Web/API crawling and fuzzing:
- Authentication and session testing:
- Vulnerability scanning:
- Exploit validation:
- Credential/password testing:
- Source/dependency/secrets analysis:
- Cloud/IAM/Kubernetes testing:
- Active Directory/lateral movement:
- Social/physical/wireless testing:
- Persistence/C2/payload generation:
- Denial of service, destructive action, or data modification:

Safety limits

- Maximum requests per second and concurrent tools:
- Maximum authentication attempts and lockout controls:
- Maximum payload/evidence size:

- Sensitive records that may be viewed or sampled:
- Proof standard that avoids unnecessary data access:
- Production monitoring and rollback owner:
- Automatic stop thresholds:

Data and evidence

- Runner data mode:
- Artifact upload policy:
- Approved storage locations:
- Encryption/key owner:
- Redaction requirements:
- Report transfer channel:
- Retention/deletion dates:
- Prohibited data handling:

Emergency stop

The stop command is accepted from any named customer emergency contact. On receipt, RedCore cancels active assignments, prevents new leases, records the event, and confirms status. Safety incidents do not wait for a change request.

- Primary 24-hour customer contact/channel:
- Backup customer contact/channel:
- RedCore incident lead/channel:
- Expected acknowledgement time:
- Escalation if contact fails:
- Resume authority and required written record:

Change control and findings

Scope expansion, new techniques, new data transfer, or a new runner requires a written change approved by both named engagement owners and, where authority is affected, updated signed authorization. Customer-facing findings require analyst review; automated output alone is not a final finding.

Customer technical owner / date: _____

Customer authorizing representative / date: _____

RedCore engagement owner / date: _____

Customer runner deployment and acceptance

Status: Required for customer-hosted execution. Complete after security review and before the runner receives any real engagement assignment.

Deployment record

- Customer / tenant ID / engagement ID:
- Runner ID / hostname label / owner:
- Platform: Windows+WSL2 / Linux / Docker / Kubernetes:
- Environment and network zone:
- Image/package version and digest/commit:
- Deployment profile: standard / restricted:
- Control-plane URL and certificate validation method:
- Outbound proxy/allowlist:
- Authorized target network routes:

Identity and secrets

- Bootstrap approved by:
- Machine credential storage path/secret manager:
- Assignment verification public-key source:
- Credential issuance, rotation, revocation owners:
- Proof that control-plane signing private key is not present on runner:
- File/secret permissions reviewed:

Capability certification

- Required capability list/version:
- Actual advertised inventory attached:
- Tool versions/licenses reviewed:
- Privileged/root capabilities separately approved:
- Unavailable or substituted capabilities recorded:
- redcore runner doctor evidence reference:

Data flow

- Data mode: local/findings-only / evidence / full:
- Upload policy and approved artifact classes:
- Local evidence/report/storage paths:
- Volume encryption and key ownership:
- Retention, backup, collection, and deletion owner:
- Source code or raw customer data permitted to leave runner: Yes / No; basis:

Acceptance tests

- [ ] No inbound runner service port is exposed.
- [ ] Outbound TLS reaches only approved control-plane destinations.
- [ ] Runner cannot reach out-of-scope target networks.
- [ ] Tenant and runner identity mismatch is rejected.
- [ ] Invalid/unsigned assignment is rejected.
- [ ] Missing capability assignment is rejected.
- [ ] Heartbeat, poll, lease, renewal, evidence, finding, completion work.
- [ ] Cancellation, lease expiry, runner disablement, and reconnect work.
- [ ] Data-minimization policy blocks unapproved artifacts.
- [ ] Logs and evidence contain no unapproved secrets.
- [ ] Backup/restore or documented recovery behavior is accepted.
- [ ] Emergency stop exercise completed with timestamps.

Approval

This approval certifies only the identified runner configuration and capability inventory. Any material image, network, identity, scope, data-mode, or privilege change requires re-certification.

Customer security approver / date: _____

Customer infrastructure owner / date: _____

RedCore technical approver / date: _____

Finding disposition, retest, and engagement closure

Finding disposition

For each finding record:

- Finding ID / title / severity:
- Affected approved asset:
- Evidence reference and reviewer:
- Customer owner:
- Disposition: accepted / remediation planned / risk accepted / duplicate / disputed / false positive:
- Rationale and approval reference:
- Target remediation date:
- Retest requested: Yes / No; deadline:

Retest record

- Original finding and evidence references:
- Retest date, tester, runner, and policy version:
- Exact approved retest scope:
- Result: remediated / partially remediated / not remediated / unable to verify:
- New evidence reference:
- Residual risk and next action:
- Customer acknowledgement:

Closure checklist

- [ ] Final report passed human review and was delivered through the approved channel.
- [ ] Customer acknowledged receipt and documented finding owners/dispositions.
- [ ] Retest commitments and expiry are recorded.
- [ ] Test accounts, tokens, repository access, VPN, and runner bootstrap credentials are revoked.
- [ ] Runner is disabled, retained for an approved program, or removed as agreed.
- [ ] Temporary files and unapproved local copies are removed.
- [ ] Evidence and report retention dates are recorded by system/location.
- [ ] Required customer return/export is complete.
- [ ] Deletion actions are complete or scheduled, including backup limitations.
- [ ] Security incidents, scope deviations, and lessons learned are closed.
- [ ] Final invoice/commercial acceptance is recorded separately.

Data disposition certificate

- Data classes retained and purpose:
- Storage locations and access owners:
- Retention expiry:

- Data deleted and deletion method/date:
- Backup expiry or exception:
- Evidence that cannot be deleted and legal basis:

Customer engagement owner / date: _____

RedCore engagement owner / date: _____

RedCore data disposition reviewer / date: _____

RedCore standard vendor security response

Status: Pre-sales response framework. Answers are limited to current repository-backed controls. Replace bracketed commercial facts only with verified evidence; never infer certifications, insurance, SLAs, or audit results.

Product and hosting

- Service: AI-assisted authorized penetration testing with optional customer-hosted runner.
- Deployment: RedCore-managed execution or outbound-only customer runner.
- Customer runner inbound port: None published by the provided deployment profiles.
- Supported runner profiles: Windows/WSL2 or Linux process, Docker Compose, Kubernetes; acceptance required.
- Production hosting provider/regions: [Provide verified deployment-specific response.]

Identity and isolation

- Engagement, tenant, asset, job, runner, and evidence records carry explicit ownership context.
- Runner credentials and assignments are tenant/runner-bound.
- Control-plane assignments use signatures; only the verification public key is placed on runners.
- Roles and API authentication are configurable; production auth must be enabled and accepted.

Data protection

- Tenant-aware local vault secrets use AES-256-GCM authenticated encryption.
- Transport protection depends on production TLS and certificate configuration.
- Runner data-minimization supports local/findings-only and controlled artifact upload policies.
- Retention, residency, subprocessor, backup, and deletion terms are set in the customer agreement and data-flow register.

Secure execution and evidence

- Scope, target, technique, rate, timing, and destructive-action policy precede execution.
- Runner capability advertisements are checked against assignment requirements.
- Leases, cancellation, disablement, and offline recovery constrain remote work.
- Evidence records support timestamps, hashes, provenance, and finding relationships.
- Customer-facing findings require human review.

Assurance facts requiring separate evidence

Do not answer “yes” without supplied documentation for: SOC 2, ISO 27001, PCI assessor status, FedRAMP, HIPAA certification, external penetration-test attestation, background checks, cyber-insurance limits, formal uptime SLA, 24-hour support, data-center certifications, or regulator approvals.

Procurement evidence package

- Current architecture/security overview.
- Executed confidentiality and data terms.
- Deployment-specific data-flow and subprocessor list.

- Runner acceptance and capability certification record.
- Current test summary and release evidence appropriate for disclosure.
- Incident contacts, retention schedule, and closure procedure.

Response owner / evidence date / version: _____