REDSEC LABS

INCIDENT RESPONSE RETAINER

Strategic frameworks and response methodologies for end-to-end cyber incident containment and recovery

CONFIDENTIAL

01 OVERVIEW

Security incidents remain inevitable even for mature organisations. With attackers increasingly leveraging automation, identity compromise and cloud-based intrusion techniques, rapid, coordinated response is essential to limiting impact. RedSecLabs' Incident Response Retainer ensures that when a breach occurs, your organisation has immediate access to experienced responders and senior security specialists.

Our team consists of seasoned incident handlers, DFIR specialists and penetration testers with proven offensive security backgrounds. RedSecLabs holds PCI DSS QSA capability and CREST penetration testing accreditation, enabling evidence-driven analysis and structured response aligned with best-practice methodologies.

Throughout any incident, RedSecLabs aligns technical actions with your business priorities. Whether your objective is restoring services quickly, gathering evidence for regulatory reporting, or performing deep compromise assessment, we support you with clear communication and measurable outcomes.

- Experts in defensive and offensive security, bringing attacker-perspective analysis.
- Pragmatic response methodology prioritising rapid containment and recovery.
- Clear stakeholder engagement and communication throughout the incident.
- Accredited service capability: PCI DSS QSA and CREST-aligned penetration testing expertise.

OUR SERVICE

The RedSecLabs Cyber Security Incident Response Retainer provides guaranteed access to our Incident Response Team (IRT), complete with defined service levels, fixed response rates and a dedicated pool of retainer hours.

In the event of a security incident, our IRT delivers expert guidance from detection through containment, eradication and full recovery. Depending on your operational needs, RedSecLabs can manage the full lifecycle end-to-end or work jointly with your in-house security and IT teams.

The retainer includes a defined allocation of response hours, with the option to purchase additional hours during an active incident.

BENEFITS

- Guaranteed access to the RedSecLabs IRT with defined SLAs.
- 24×7×365 incident reporting.
- Initial triage within 4 hours.
- Remote support within 8 hours.
- 40 inclusive incident response hours (expandable at retainer initiation).
- Unused hours may be applied to scheduled RedSecLabs services within the grace period.

02 APPROACH

INTEGRATION PROJECT

Prior to retainer activation, RedSecLabs performs an integration project to collect relevant information about your environment, systems, processes and escalation paths. This ensures the IRT can engage immediately without delays during an emergency.

REMOTE ACCESS

RedSecLabs supports secure remote response using a controlled access model. Where required, a zero-configuration VPN device can be deployed to enable encrypted responder access using certificate-based authentication. All actions remain fully auditable and restricted to authorised IRT staff.

WHEN AN INCIDENT OCCURS

Upon receiving an incident report, our IRT initiates a rapid technical callback to conduct verbal triage, determine impact, severity and scope, and establish immediate containment priorities. The team then performs structured triage, identification, containment, eradication and recovery following recognised

frameworks including NIST, CREST best practices and NCSC guidance. All response activities occur via remote support unless otherwise negotiated.

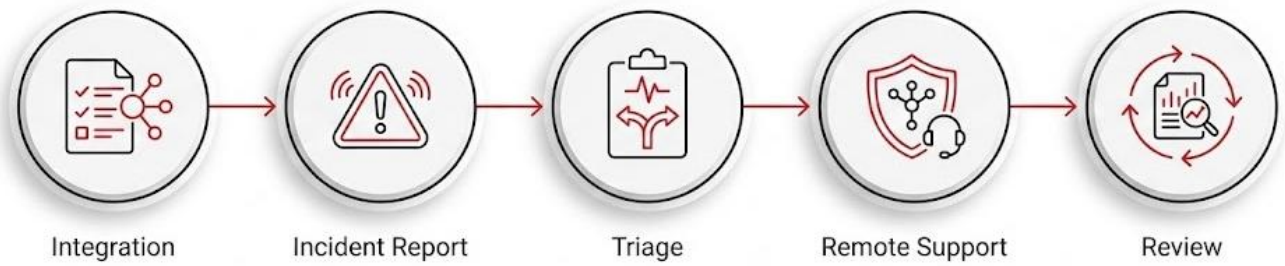
REGULAR REVIEWS

Following any incident, RedSecLabs facilitates a review meeting covering incident details, technology changes, hour utilisation, improvement opportunities and any organisational adjustments required.

UNUSED HOURS

At the end of the 12-month retainer term, unused hours may be used for scheduled RedSecLabs services for a period of up to three months. This includes DFIR support, security assessments and penetration testing.

03 RETAINER OVERVIEW



SERVICE MANAGEMENT

RedSecLabs applies a structured service management model integrated with our internal quality processes. Each engagement includes a lead consultant and project manager. Escalation procedures are maintained and activated only in cases of unresolved issues.

SERVICE CONSTRAINTS & LEVELS

SLAs and retainer terms are agreed within each Statement of Work. The standard service levels outlined in this document apply unless otherwise specified.

FINANCIAL RECOMPENSE

RedSecLabs does not provide a formal recompense model. Service quality and customer satisfaction are continually monitored as part of our operational assurance framework.

TRAINING

RedSecLabs offers training across DFIR, cloud security, threat detection and incident readiness. Bespoke training may be added to the retainer upon request.

ORDERING & INVOICING PROCESS

A Statement of Work is issued for each retainer agreement. Work begins upon acceptance via purchase order or signed order form. Fixed-price components are invoiced upon deliverable completion, while time-and-materials elements are billed monthly in arrears.

TERMINATION TERMS

Refer to the RedSecLabs Terms and Conditions document for full termination details.

DATA RESTORATION/SERVICE MIGRATION

Data restoration and service migration fall outside the scope of the retainer.

CUSTOMER RESPONSIBILITIES

Client responsibilities are defined in each Statement of Work and typically include facilitating access, providing environment information, and maintaining communication channels during an incident.

TECHNICAL REQUIREMENTS

Technical prerequisites are agreed during scoping. Requirements differ across environments and will be documented within the Statement of Work.