Service Definition Document:
Managed Detection and Response

ATOMIC RISK MANAGEMENT

Collaborate | Innovate | Accelerate

Introduction

Atomic Risk Management provides cyber security and risk services to help organisations protect critical services, maintain business continuity and make defensible decisions. Our Managed Detection & Response (MDR) service is designed to improve operational security in a practical, risk-led way, working alongside AlienVault, Microsoft, AWS and other leading suppliers.

Purpose

To provide an MDR capability that prioritises action over noise; monitoring and triaging security telemetry, validating material threats, and supporting rapid, coordinated response to reduce impact on critical services.

Overview

Atomic Risk Management MDR helps organisations strengthen detection and response without needing to build a full in-house SOC. We focus on the threats that matter most, to reduce alert fatigue and deliver clear, decision-ready reporting for leadership assurance and confidence.

The service is delivered using a blend of people, process and technology. We can integrate with your existing security tooling and processes, and tailor coverage and operating model to your environment and risk priorities. We deliver MDR working alongside AlienVault, Microsoft, AWS and other leading suppliers, helping customers maximise value from their chosen platforms.

What the service includes (as agreed in the SOW):

- 24 x 7 monitoring and risk-led triage of agreed telemetry
- investigation support and recommended actions
- incident escalation and response coordination
- reporting with priorities, trends and improvement actions
- continuous improvement through tuning and operational learning

How it works:

1. discovery and onboarding (goals, scope, escalation routes)
2. telemetry alignment (confirm the alerts that matter most)
3. risk-led triage and investigation (validate threats, reduce noise)
4. response support (guided containment and remediation actions)
5. assurance reporting (actions taken, residual risk, next priorities)

Quality Assurance and Performance Testing

Quality is assured through structured operating procedures for triage, investigation and escalation, defined success measures, and evidence-based reporting. We review detection performance and operational outcomes regularly, track improvement actions, and tune detections to reduce false positives and improve coverage. Any security testing (e.g., penetration testing) is provided only where explicitly scoped and permitted.

Security Services

Core MDR capabilities (tailored and agreed in the SOW) may include:

- continuous monitoring and risk-led triage
- alert validation and investigation support
- escalation management and response coordination
- response playbooks and agreed escalation routes
- integration with existing tools and workflows
- system design and assurance for logging, detection and response processes
- support selecting systems, vendors and telemetry sources (where required)
- monthly reporting with trends, priorities and improvement actions
- continuous tuning to reduce noise and improve detection outcomes
- optional enhanced coverage models (including 24/7) where agreed

Ongoing Support

Support levels

- **Standard (included):** Email and phone support during normal working hours; operational guidance and clarification; delivery management by the technical lead.
- **Enhanced (optional):** Extended hours (evenings/weekends) and increased review cadence, agreed in the SOW.
- **Emergency / on-call (optional):** Out-of-hours urgent support by prior arrangement, with response targets and escalation routes defined in the engagement plan/SOW.

Typical response times (Standard)

- **Email:** within **1 working day**.
- **Weekends/out-of-hours:** not included unless explicitly agreed.

Information Assurance

Atomic Risk Management uses suitably qualified and experienced personnel, including security-cleared staff where required. Delivery can align to customer handling and classification requirements. Processing of higher-classification information is performed only on customer-accredited systems/environments, subject to access approvals and engagement constraints.

Pricing

Services are priced using **SFIA-aligned day rates**, based on the anticipated delivery requirement. Pricing is confirmed in the Order Form/Statement of Work (SOW) before commencement.

Pricing models available:

- **Fixed price:** milestone-based delivery with agreed scope, assumptions and contingency.
- **Time and materials:** invoiced monthly in arrears against actual effort.
- **Flexible/subscription:** based on customer requirements and/or usage, defined in the SOW.

Travel and subsistence are chargeable only if explicitly permitted and agreed in advance.

Service Management and Constraints

Service management
A technical lead manages day-to-day delivery and liaises with the customer lead, including escalation routes and reporting cadence. Contracts are managed by an account manager with director oversight and escalation.

Constraints buyers should be aware of
Service effectiveness depends on timely customer access to agreed telemetry sources, stakeholders and escalation routes. Monitoring and response coverage is limited to the systems, data sources and actions defined in the SOW; restricted or unsupported integrations may reduce visibility. Any containment actions requiring changes to customer environments must follow customer approvals and access controls. Delivery is typically remote; on-site support is available subject to customer security/site access, scheduling and agreed travel costs. Out-of-hours or 24/7 coverage is available only where explicitly agreed.

Data Backup and Business Continuity

Atomic Risk Management maintains regular backups of corporate systems and devices to support continuity of service delivery. Data handling aligns to agreed classification and customer requirements. The Supplier can process data at **OFFICIAL** on Supplier systems where agreed; data at higher classifications is processed only on customer-accredited systems/environments.

Onboarding/offboarding

Onboarding follows our standard process or aligns to customer requirements. We confirm scope, objectives, telemetry sources, access methods, response playbooks, escalation routes, reporting format and success measures.
Offboarding includes orderly removal of access/integrations (where applicable), handover of agreed reports and documentation, and a review against objectives with recommendations for next steps.

Ordering and invoicing process

Customers raise an enquiry and agree requirements. Atomic Risk Management provides a costed proposal and engagement details. On receipt of signed approval and a valid purchase order, a start date, delivery plan and payment schedule are agreed. Invoicing follows the pricing model in the SOW (monthly in arrears for time and materials; milestone-based for fixed price). Standard payment terms are **30 days from invoice date**.

Customer responsibilities

Customers are expected to:

- nominate a customer lead and make stakeholders available
- provide timely access to agreed telemetry sources, systems and documentation
- agree escalation routes and approvals for response actions
- operate internal incident/change processes needed to implement actions
- review reports and provide feedback within agreed timescales

Why work with us

Atomic Risk Management MDR is **risk-first**: we focus on what matters most, not what's loudest. We reduce alert noise, guide effective response actions, and provide clear, decision-ready reporting that supports leadership assurance—designed for sensitive and high-consequence environments and delivered alongside leading suppliers including AlienVault, Microsoft and AWS.