EDR Alert Escalation & Investigation Service Definition

Document title	EDR Alert Escalation & Investigation Service Definition		
Reference No.	IF-SER-004	**Version**	1.0
Author	Lisa Washer, Head of Cyber		
Reviewed by	Neil Bacon, Incident Response Specialist		
Issue date	28/01/2026		

EDR Alert Escalation & Investigation Service Definition

Document Control

Version	Name	Comment	Date
0.1	Lisa Washer	Initial Draft	07/01/2026
0.2	Neil Bacon	Review and comments	28/01/2026
1.0	Lisa Washer	Minor amendments and publish	28/01/2026

Correlation Chart

Clause	FSR Code of Practice v2	ISO/IEC 17025:2017	ILAC-G19 :06/2022	ISO 9001:2015	ISO/IEC 27001:2022
Review of Requests, Tenders and Contracts	16	7.1	4.1, 4.7	8	4.2

EDR Alert Escalation & Investigation Service Definition

Contents

1. EDR Alert Escalation & Investigation Service

1.1 Service Overview

1.1.1 The EDR Alert Escalation & Investigation Service provides organisations with structured, expert-led triage, escalation, and investigation of security alerts generated by Endpoint Detection and Response (EDR) platforms. The service uses the Strand Intelligence Platform to automate evidence collection, execute consistent investigation workflows, and present clear, defensible investigation outcomes.

1.1.2 The service supports security operations, incident response, and risk management teams by rapidly assessing alert validity, determining impact, and escalating confirmed threats for containment or remediation by the client or their managed security provider.

1.2 Service Objectives

1.2.1 The objectives of the EDR Alert Escalation & Investigation Service are to:

a) Rapidly triage and validate EDR alerts

b) Reduce alert fatigue through structured investigation

c) Identify malicious activity, scope, and impact

d) Support timely escalation and response decisions

e) Provide clear, auditable investigation outputs

2. Service Features

2.1.1 Below is a list of the core capabilities and characteristics of the EDR Alert Escalation & Investigation service, describing what is delivered and how the service operates:

a) **Automated Alert Ingestion and Normalisation** - Secure ingestion of alerts from supported EDR platforms, normalised into a consistent investigation format within the Strand Intelligence Platform.

b) **Structured Triage and Prioritisation** - Alerts are automatically categorised and prioritised based on severity, confidence, and potential business impact to support efficient analyst focus.

c) **Guided Investigation Workflows** - Predefined, repeatable investigation playbooks aligned to common EDR alert types ensure consistency, completeness, and defensibility of investigations.

d) **Endpoint Forensic Evidence Collection** - Automated collection of relevant endpoint artefacts, including process activity, file system data, persistence mechanisms, and user context at the time of investigation.

e) **Contextual Correlation and Analysis** - Correlation of alert data with endpoint behaviour, historical activity, and related artefacts to provide meaningful investigative context and reduce false positives.

f) **Alert Validation and Threat Determination** - Clear determination of whether alerts represent benign activity, suspicious behaviour, or confirmed malicious activity, supported by documented evidence.

g) **Severity and Impact Assessment** - Assessment of the scope and potential impact of confirmed threats at the endpoint level, supporting informed escalation and response decisions.

h) **Clear Escalation Outputs** - Structured escalation reports provided to client SOC, IT, or incident response teams, including findings, evidence, and recommended next steps.

i) **Centralised Investigation and Reporting Platform** - All investigations, evidence, decisions, and outcomes are captured within the Strand Intelligence Platform, providing a single source of truth.

j) **Auditability and Transparency** - Full audit logging of investigation actions, evidence collection, and decision points to support assurance, compliance, and post-incident review.

k) **Role-Based Access Control** - Granular access controls ensure that only authorised users can view alerts, investigations, and sensitive evidence.

l) **Scalable, Cloud-Based Delivery** - The service scales to support fluctuating alert volumes without requiring additional client infrastructure or tooling.

3. Service Benefits

3.1.1 The EDR Alert Escalation & Investigation Service provides organisations with timely, expert support to understand and respond effectively to cybersecurity incidents. Key benefits include:

a) **Faster Alert Triage and Decision-**Making - Rapid, structured investigation of EDR alerts enables quicker understanding of risk and supports timely escalation or closure decisions.

b) **Reduced Alert Fatigue** - Automated evidence collection and guided investigation workflows significantly reduce the volume of alerts requiring manual review by security teams.

c) **Consistent and Defensible Investigations** - Standardised investigation playbooks ensure investigations are repeatable, complete, and defensible, reducing reliance on individual analyst experience.

d) **Improved Security Operations Efficiency** - Security teams can focus on confirmed threats rather than raw alerts, improving overall SOC efficiency and effectiveness.

e) **Clear Escalation with Evidence** - Confirmed threats are escalated with structured findings and supporting evidence, enabling faster and more confident response actions.

f) **Improved Visibility of Endpoint Risk** - Centralised analysis of endpoint behaviour provides clearer insight into endpoint-level threats and potential impact.

g) **Audit-Ready Investigation Records** - Comprehensive logging of investigations, decisions, and evidence supports assurance, compliance, and post-incident review.

h) **Scalable and Flexible Service** - The service scales to match fluctuating alert volumes without requiring additional client infrastructure or staffing.

i) **Enhanced Collaboration Between Teams** - Clear outputs support effective collaboration between SOC, IT, and incident response teams.

j) **Supports Security Maturity Improvement** - Investigation outcomes and trend analysis inform improvements to detection rules, response processes, and overall security posture.

k) **Trusted Accredited Delivery** - Delivered by CREST- and SANS-accredited specialists operating as an NCSC CIR accredited provider.

4. Scope of Service

4.1 In-Scope of Service

4.1.1 The EDR Alert Escalation & Investigation Service provides structured triage and investigation of endpoint security alerts generated by supported EDR platforms. The scope of the service includes the following activities:

a) Ingestion of security alerts generated by supported EDR platforms via secure integration.

b) Initial triage to validate alert relevance, severity, and potential business impact.

c) Automated and guided investigation workflows tailored to the alert type and threat category.

d) Collection of endpoint forensic artefacts relevant to the alert, including process execution, file activity, persistence mechanisms, registry entries, user context, and system state at the time of investigation.

e) Correlation of alert data with endpoint behaviour and historical activity to provide investigative context.

f) Identification and documentation of indicators of compromise (IOCs) and suspicious behaviours.

g) Determination of alert outcome, including classification as benign, suspicious, or confirmed malicious activity.

h) Assessment of scope and impact at the endpoint level for confirmed threats.

i) Escalation of validated and confirmed threats to the client's SOC, IT, or incident response teams, supported by clear findings and evidence.

j) Documentation of investigation steps, decisions, and outcomes within the Strand Intelligence Platform.

k) Provision of investigation summaries and supporting artefacts suitable for audit, assurance, or post-incident review.

4.2 Out-of-scope activities

4.2.1 Unless explicitly agreed in advance and documented within the statement of work or incident-specific authorisation, the following activities are outside the standard scope of the EDR Alert Escalation & Investigation Service:

a) Active containment, remediation, or eradication actions on endpoints, except where specific containment actions have been pre-approved or authorised on a case-by-case basis.

b) Configuration, tuning, or ongoing management of the client's EDR platform.

c) Network-level monitoring, investigation, or response activities.

d) Full managed detection and response (MDR) or security operations centre (SOC) service delivery.

e) Incident response coordination beyond investigation and agreed escalation or containment actions.

f) Regulatory notification, legal advice, or direct communications with external stakeholders.

g) Proactive or continuous threat hunting activities not directly linked to an EDR alert.

4.2.2 Any containment or response actions undertaken are subject to explicit client authorisation, documented approval, and confirmation of scope, timing, and risk prior to execution.

4.3 Assumptions, Constraints and Dependencies

4.3.1 Delivery of the EDR Alert Escalation & Investigation Service is based on the following assumptions:

a) The client has lawful authority to collect, process, and analyse endpoint security data, including personal data where applicable.

b) Supported EDR agents are deployed, operational, and correctly configured on in-scope endpoints.

c) The Strand Intelligence Platform has appropriate permissions to ingest alerts and collect investigative artefacts from the EDR platform.

d) Endpoints are accessible and connected at the time of investigation to allow evidence collection.

e) Investigation scope, escalation thresholds, and any permitted containment actions are clearly defined and agreed in advance.

f) The client has appropriate internal processes in place for incident response, escalation, and remediation following investigation.

4.3.2 Delivery of the service is dependent on the following factors:

a) Availability and stability of the client's EDR platform and supporting infrastructure.

b) Timely ingestion of alerts from the EDR platform into the Strand Intelligence Platform.

c) Availability of endpoint telemetry and artefacts retained by the EDR platform at the time of investigation.

d) Cooperation from client stakeholders, including SOC, IT, legal, and compliance teams, to support escalation and decision-making.

e) Availability of specialist analysts and platform resources to perform investigations within agreed service levels.

f) Timely client approvals where containment or response actions are requested.

4.3.3 The following constraints may impact the scope, timelines, or outcomes of investigations:

a) EDR alerts and investigations provide a point-in-time assessment based on available endpoint data.

b) Telemetry retention limits, agent configuration, or endpoint offline status may restrict evidence availability.

c) False positives, alert noise, or incomplete telemetry may limit investigative certainty.

d) Platform, operating system, or endpoint-specific limitations may affect the depth of artefact collection.

e) Investigations prioritise accuracy, defensibility, and auditability over speed, which may impact response times.

f) The service does not provide continuous monitoring or guarantee detection of all malicious activity.

g) Service delivery is subject to agreed commercial terms, technical feasibility, and specialist availability.

5. Onboarding

5.1.1 Onboarding to the EDR Alert Escalation & Investigation Service is delivered through a structured, remote-led process designed to enable rapid, secure, and effective service activation.

5.1.2 The onboarding process includes confirmation of service scope, escalation criteria, and supported EDR platforms, along with validation of required permissions and integrations. Secure connectivity between the client's EDR platform and the Strand Intelligence Platform is established, including configuration of alert ingestion, evidence collection permissions, and role-based access controls.

5.1.3 Client stakeholders are onboarded to the platform through guided access setup and orientation, covering alert visibility, investigation outputs, and escalation workflows. Where applicable, escalation paths, approval requirements for containment actions, and communication protocols are formally agreed and documented.

5.1.4 Onboarding concludes with validation testing to confirm successful alert ingestion and investigation execution. Standard onboarding activities are included within service engagement, with enhanced onboarding or tailored configuration available subject to separate agreement.

6. Service Delivery Model

6.1 Delivery Approach

6.1.1 The EDR Alert Escalation & Investigation Service is delivered as a managed, analyst-supported service using the Strand Intelligence Platform. The service is designed to integrate with the client's existing EDR tooling and security operations model, providing structured investigation and escalation rather than replacing existing SOC, MDR, or incident response capabilities.

6.1.2 Alerts generated by supported EDR platforms are securely ingested into the Strand Intelligence Platform via API integration. Each alert is assessed using predefined triage criteria and guided investigation workflows to ensure consistency, proportionality, and defensibility.

6.1.3 The Service delivery model has the following characteristics:

a) Delivered remotely using a secure, cloud-based platform

b) Scalable to handle fluctuating alert volumes

c) Analyst oversight combined with automated workflows

d) Clear separation between investigation and remediation

e) Designed to integrate with existing security operating models

6.2 Investigation Workflow

6.2.1 Once an alert is received, the service follows a structured delivery workflow:

a) **Alert Intake and Triage -** Alerts are validated to confirm relevance, severity, and potential impact, reducing false positives and noise.

b) **Automated Evidence Collection -** Relevant endpoint artefacts are collected at the time of investigation, providing contextual evidence aligned to the alert type.

c) **Analysis and Correlation -** Endpoint activity is analysed and correlated to determine whether the alert represents benign behaviour, suspicious activity, or a confirmed threat.

d) **Outcome Determination -** Each alert is classified with a documented outcome and supporting rationale.

e) **Escalation and Handover -** Where required, findings are escalated to the client's SOC, IT, or incident response teams with clear evidence and recommended next steps.

6.3 Containment and Response Integration

6.3.1 The service supports escalation to containment and response activities but does not automatically perform remediation as standard. Where containment actions are required, these may be executed only where explicitly authorised and documented in advance, either as part of standing approvals or incident-specific agreement. All actions are recorded within the platform to maintain auditability.

6.4 Delivery Modes

6.4.1 All investigations are conducted in accordance with recognised security and forensic best practice. Investigation steps, evidence collection, decisions, and escalation actions are logged to provide transparency, traceability, and audit readiness. Regular service reviews may be conducted to assess performance, trends, and opportunities for improvement.

7. Support Model

7.1 Alert Escalation Options

7.1.1 The EDR Alert Escalation & Investigation Service supports two escalation models, allowing organisations to align the service with their existing security operations and risk appetite.

7.2 Automated Alert Escalation

7.2.1 Under the automated escalation model, EDR alerts meeting predefined criteria are **automatically forwarded** to the Strand Intelligence Platform for investigation. Escalation rules are configured during onboarding based on alert type, severity, confidence level, or affected asset classification.

7.2.2 This model enables 24/7 managed investigation**,** reducing reliance on internal analyst availability and ensuring rapid triage and response for time-critical alerts. Automated escalation is suited to organisations seeking continuous coverage and minimal manual intervention.

7.3 Analyst-Initiated Escalation

7.3.1 Under the analyst-initiated escalation model, alerts are first reviewed by the client's internal SOC or security analysts. Alerts assessed as requiring further investigation are manually escalated to the Strand Intelligence Platform.

7.3.2 This approach allows organisations to retain direct control over which alerts are investigated, supporting environments with established SOC capability or where selective escalation is preferred. Investigations are performed following escalation and supported by agreed service levels.

8. Service Level Agreements

8.1 Service Availability

8.1.1 The EDR Alert Escalation & Investigation Service is delivered as a managed service with 24/7 operational availability, excluding planned maintenance. The Strand Intelligence Platform is designed to provide high availability, with service continuity monitored continuously.

8.1.2 Planned maintenance is scheduled outside of core operating hours wherever possible and communicated in advance. Emergency maintenance may be performed where required to protect service security or stability.

8.2 Alert Handling and Response time

8.2.1 Alert handling and response times are measured from the point an alert is received by the Strand Intelligence Platform through automated escalation, or from the time a client analyst submits an alert for investigation under the analyst-initiated escalation model.

8.2.2 The service operates on a **24/7 basis** for automated escalations. Target response times are aligned to alert priority and are intended to support timely investigation and escalation while maintaining accuracy, transparency, and evidential integrity.

a) **P1 – Critical Alerts** - Alerts indicating active compromise or high-risk malicious activity. Investigation is initiated within 15 minutes, with initial findings and escalation provided within 60 minutes, subject to endpoint availability and telemetry access.

b) **P2 – High Alerts** - Alerts indicating likely malicious or suspicious activity requiring urgent validation. Investigation is initiated within 30 minutes, with initial findings provided within 2 hours.

c) **P3 – Medium Alerts** - Alerts indicating unusual or potentially suspicious behaviour requiring analysis. Investigation is initiated within 4 hours, with findings typically provided within one business day.

d) **P4 – Informational Alerts** - Low-risk or informational alerts with no immediate security impact. Investigation is initiated within one business day and handled on a scheduled or best-effort basis.

8.2.3 Investigation timelines may vary depending on alert complexity, volume, endpoint availability, and data retention. All investigations prioritise accuracy, defensibility, and auditability over speed.

8.3 Investigation Outcomes

8.3.1 Each alert investigation results in a documented outcome, including classification (benign, suspicious, confirmed threat), supporting evidence, and escalation recommendations where applicable. All actions and decisions are logged for auditability.

8.4 Escalation and Incident Management

8.4.1 Standard service delivery is provided during business hours, with enhanced or out-of-hours support available by agreement. Availability may be extended for high-severity incidents, subject to resource availability and agreed terms.

9. Roles and Responsibilities

9.1.1 The following roles are defined to ensure effective governance, delivery, and communication throughout the EDR Alert Escalation & Investigation Service engagement.

9.2 Account Manager

9.2.1 Acts as the primary commercial and engagement contact for the organisation. Responsible for contract management, service coordination, and service governance. Ensures the service is delivered in line with the agreed scope, service levels, and escalation model, and manages strategic escalation where required.

9.3 Incident Manager/Investigation Manager

9.3.1 Provides overall operational leadership for alert escalation and investigation activities. Responsible for prioritisation of alerts, coordination of investigation workflows, oversight of escalation decisions, and communication management. Acts as the primary operational point of contact during active investigations or high-severity alerts.

9.4 EDR Investigation Specialist

9.4.1 Responsible for the technical investigation of EDR alerts using the Strand Intelligence Platform. Conducts triage, evidence collection, analysis, and documentation of endpoint activity in accordance with recognised security and forensic best practice. Provides expert input to support escalation, impact assessment, and containment or response recommendations.

9.5 Cyber Incident Response (CIR) Specialist

9.5.1 Responsible for the technical investigation and forensic analysis following the confirmation of a Security Incident. Conducts evidence collection, analysis, and documentation in accordance with recognised forensic standards. Provides expert input to support containment, remediation planning, and reporting.

9.6 Client Incident Lead

9.6.1 Acts as the organisation's primary point of contact for the service. Responsible for defining escalation criteria, approving any authorised containment actions, coordinating internal response activities, and supporting decision-making based on investigation findings.

9.7 Client SOC, IT and Incident Response Teams

9.7.1 Provide operational support following escalation, including remediation, containment, recovery, and stakeholder communications. Where analyst-initiated escalation is used, client security teams are responsible for initial alert review and escalation to the service.

10. Technical Requirements

10.1 Client Environment Requirements

10.1.1 To enable effective delivery of the EDR Alert Escalation & Investigation Service, the following technical requirements apply:

a) A supported Endpoint Detection and Response (EDR) platform must be deployed, licensed, and operational on all in-scope endpoints.

b) Endpoints must have active EDR agents installed and capable of transmitting telemetry and alerts.

c) The client must provide appropriate API access and permissions to enable secure alert ingestion and evidence collection via the Strand Intelligence Platform.

d) Endpoints must have network connectivity at the time of investigation to support artefact collection, subject to EDR platform capabilities.

10.2 Platform Access Requirements

10.2.1 Access to the Strand Intelligence Platform is provided via a modern web browser (e.g. current versions of Chrome, Edge, or Firefox).

10.2.2 Users must support multi-factor authentication (MFA) and role-based access controls.

10.2.3 Secure connectivity (TLS-encrypted) is required for all platform interactions.

10.3 Data and Telemetry Requirements

10.3.1 Sufficient telemetry retention must be configured within the EDR platform to support investigation timelines.

10.3.2 The availability and depth of investigation findings are dependent on EDR configuration, retention policies, and endpoint operating systems.

10.3.3 The service relies on point-in-time data available at the time of investigation.

10.4 Integration and Configuration

10.4.1 Initial configuration of alert ingestion, severity mapping (P1–P4), escalation rules, and authorised containment actions is completed during onboarding.

10.4.2 Changes to integrations, permissions, or escalation logic require documented approval and may be subject to change control.

10.5 Client Responsibilities

10.5.1 The client is responsible for:

a) Maintaining the operational health of the EDR platform and endpoint agents

b) Ensuring lawful authority to collect and process endpoint data

c) Managing endpoint remediation, recovery, and patching activities

d) Maintaining internal incident response and escalation processes

10.6 Constraints

10.6.1 Technical constraints may include EDR platform limitations, endpoint availability, telemetry retention limits, operating system restrictions, and network connectivity issues. These factors may affect investigation depth, timelines, or outcomes.

11. Exit and Offboarding

11.1.1 Exit and offboarding activities are designed to ensure a controlled, secure, and auditable conclusion to the EDR Alert Escalation & Investigation Service.

11.1.2 Upon service termination or contract expiry, access to the Strand Intelligence Platform is revoked in accordance with agreed notice periods. Alert ingestion and investigation activities are ceased, and any automated integrations with the client's EDR platform are disabled or removed.

11.1.3 Investigation data, reports, and audit logs generated during the engagement are made available to the client for export within an agreed timeframe. Data is retained or securely deleted in line with contractual requirements, data protection obligations, and information retention policies.

11.1.4 A formal service closure confirmation is provided, including confirmation of access removal and data handling actions. Where required, knowledge transfer or handover support may be provided to support continuity of internal security operations, subject to separate agreement.

*****END OF DOCUMENT*****