848

848 Secure Business - Respond

Part of

The Secure Business

Prepared by

Dave Cheetham

Pursuit Intelligence and Growth Lead

Monday, 05 January 2026

Service Overview and Context

What Our Customers Experience

Organisations operate in environments where digital services, users, and workloads change continually, and where security incidents can have immediate operational and reputational impact.

When an incident occurs, teams often struggle to coordinate activity, make decisions under pressure, and understand what actions are required to contain the threat safely. Information may be incomplete, roles unclear, and communication pathways untested, creating uncertainty at the moment clarity is most needed.

These conditions slow response, increase risk, and make it difficult to protect critical services. Leaders depend on reliable information, yet early incident insight is often fragmented.

Operational teams require structure and guidance, yet processes may be undocumented or inconsistently applied.

Organisations recognise the need for a predictable, well-governed incident response capability that enables them to act decisively and with confidence during disruptive events.

Our Framework for Clarity and Improvement

848's Intelligent Business Framework provides the structure organisations use to build dependable, repeatable operational capability. It defines how outcomes are achieved and ensures each service strengthens capability through predictable, aligned, and evidence-based delivery.

Within this Framework, incident response is treated as an organisational capability, not a reactive activity. It is shaped by governance, informed by risk, and supported by defined processes that connect technical actions with business decision-making.

By delivering work through this Framework, organisations gain consistency, traceability, and a clear understanding of how services contribute to operational resilience.

It provides the foundation for structured incident handling, enabling teams to manage security events using defined roles, controlled actions, and clear escalation pathways.

This creates the conditions required for safe, coordinated, and confident response when incidents occur.

The Secure Business Outcome Area

The Secure Business outcome area supports organisations in reducing exposure, strengthening protection, and responding effectively when security conditions change. It provides the clarity, control, and resilience needed to maintain safe operation across complex and evolving environments.

Within this outcome area, structured response capability is essential. It ensures that when incidents occur, organisations can minimise impact, preserve operational continuity, and return to stable conditions in a controlled and predictable way.

By strengthening capability in this area, organisations improve how they assess risk, apply governance, and manage security events.

They gain confidence in their ability to contain threats, coordinate teams, and support informed decision-making during high-pressure situations.

Respond contributes to this outcome area by ensuring that incidents are met with clarity rather than confusion and with coordinated action rather than ad-hoc reaction.

848 Secure Business – Respond

The Respond Service Stream enables the organisation to act decisively and effectively when a security incident occurs. It establishes the structured processes, operational readiness, and expert support required to manage incidents in a controlled, coordinated, and evidence-led manner.

Respond addresses the challenge of uncertainty during disruptive events by ensuring that teams understand their roles, follow defined procedures, and make decisions based on verified information.

As part of the Secure Business outcome area, Respond ensures the organisation can contain threats safely, assess impact accurately, and recover services in a predictable and well-governed manner.

It provides clarity during high-pressure conditions, enabling leaders and operational teams to work from a shared understanding of what has happened, what must be done, and how actions affect business continuity.

The stream also embeds learning and improvement, strengthening readiness for future incidents and reinforcing organisational resilience.

Respond creates the dependable response capability that supports safe operation across the wider Intelligent Business, ensuring that when an incident occurs, the organisation is prepared, coordinated, and capable.

Purpose of This Document

This document defines how 848 delivers the Respond Service Stream within the Secure Business outcome area. It explains the purpose of the stream, how it aligns to the Intelligent Business Framework, and what customers should expect when commissioning Respond services.

It provides a clear structure for understanding scope, delivery method, and the conditions required to establish effective response capability.

The document is intended for procurement teams, security leaders, and operational stakeholders who need clarity on how structured incident response supports organisational resilience.

It should be read alongside the Intelligent Business Framework and the Secure Business overview, which together explain how Respond contributes to safe, predictable, and well-managed operations.

The Intelligent Business Framework

Modern organisations depend on technology that support clear outcomes: reliable operations, effective protection, efficient processes, informed decisions, and the ability to adapt. Achieving these outcomes requires more than individual systems or isolated projects. It demands a structured approach that links technology, governance, and operational practice to the results the organisation is working toward.

The Intelligent Business Framework provides this structure. It is the model 848 uses to organise, deliver, and improve services in a way that aligns directly to business need. Rather than presenting a catalogue of independent services, the Framework shows how each area of capability connects to a defined aspect of organisational performance. This gives customers a consistent way to understand what each service is designed to achieve and how it contributes to wider improvement.

The Framework also brings coherence across the 848 portfolio. It defines the outcome areas that modern organisations typically strengthen and introduces a common language for discussing priorities, risks, and investment decisions. This supports focused planning and ensures work progresses in a coordinated and integrated manner, regardless of where an organisation chooses to begin.

Introduction to 848's Intelligent Business Framework

An Intelligent Business is an organisation that develops and operates its technology, processes, and governance in a way that directly supports its core outcomes. It uses platforms, data, security controls, and ways of working to maintain resilience, reduce risk, improve performance, and adapt to change in a controlled and predictable manner.

In an Intelligent Business, technology is not implemented as a set of isolated systems. It functions as an integrated part of how work is carried out, how decisions are made, and how the organisation meets its obligations. Stability, protection, efficiency, insight, and innovation are treated as connected aspects of the operating model rather than separate technical concerns.

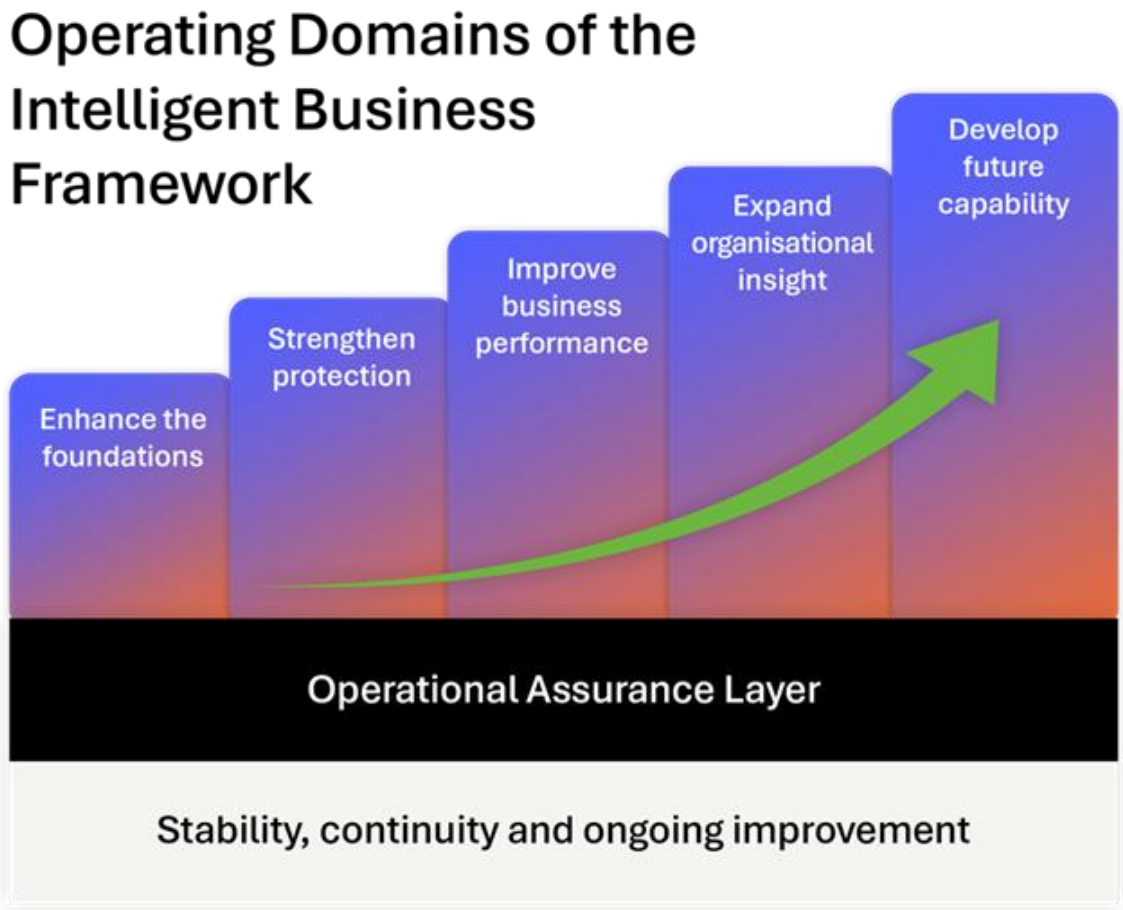
An Intelligent Business has clear visibility of its environment, understands how its services and processes interact, and makes decisions based on evidence, risk, and organisational impact. It can respond effectively to new demands, maintain operational continuity as conditions change, and introduce new capability without undermining what is already in place.

Ultimately, an Intelligent Business uses technology, governance, and operational practice to support reliable, secure, and continually improving performance. It focuses on outcomes, aligns effort to organisational need, and ensures that improvements contribute to long-term capability rather than short-term fixes.

The Intelligent Business Framework is the structure 848 uses to help organisations develop the capabilities required to operate in this way. It translates these characteristics into clear areas of focus, showing how different types of work contribute to stability, protection, efficiency, insight, and future capability. By organising services around these areas, the Framework provides a predictable way to understand what each service achieves and how it supports wider operational goals. This creates a practical link between the outcomes an Intelligent Business depends on and the work required to build and maintain them.

The Operating Domains of The Intelligent Business

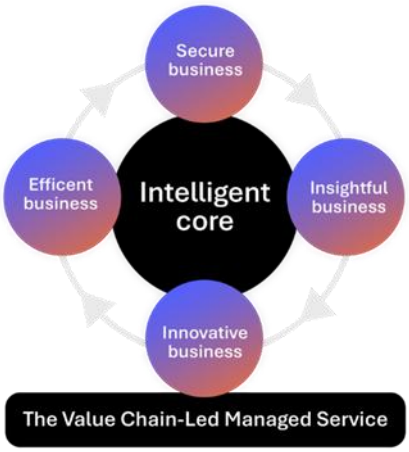
An Intelligent Business strengthens capability across several interconnected domains that influence how effectively the organisation operates. These domains reflect the areas where stability, protection, performance, insight, and future capability are developed over time. Each domain represents a different aspect of organisational need, and improvements in one area support progress in others. Organisations may focus on any domain depending on their priorities, with no fixed starting point or prescribed order.



The Operating Domains describe where organisations strengthen capability, while the Outcome Areas show how the 848 portfolio is structured to support that development. Each Outcome Area represents a defined category of work within the Framework, organising services into clear themes that align to organisational performance. Together, they translate the operating domains into a practical, service-aligned structure that enables consistent planning, delivery, and improvement.

The Six Outcome Areas

The Outcome Areas represent the structured way the Intelligent Business Framework organises capability. Each area describes a distinct aspect of organisational performance and provides the lens through which 848 designs, delivers, and aligns its services. Together, they form a connected model that supports stable, secure, efficient, insightful, and adaptable operations. These areas are not sequential; organisations may focus on any one of them depending on priorities, pressures, or the state of their current environment.



The Intelligent Core

The Intelligent Core provides the technical foundations that support the organisation's ability to operate reliably and scale responsibly. It focuses on the architecture, platforms, and engineering practices that underpin modern digital environments. This includes establishing stable cloud environments, defining coherent enterprise architecture, and applying disciplined platform engineering approaches such as DevOps and SecDevOps.

Strengthening the Intelligent Core ensures that technology aligns to organisational objectives, reduces operational fragility, and creates the structural consistency required for higher-level capability. It enables the organisation to introduce new services, adapt to change, and maintain performance without compromising stability or security.

The Secure Business

The Secure Business focuses on protecting people, data, applications, and operations. It helps organisations understand their risk landscape, implement appropriate safeguards, and maintain resilience as threats and environments evolve. This outcome area ensures that security is embedded into everyday operations rather than treated as a separate or reactive activity.

By strengthening this area, organisations gain clearer visibility of their exposure, greater confidence in their protection measures, and a structured way to govern risk. It supports responsible decision-making and ensures that security contributes directly to safe, predictable, and well-managed operations.

The Efficient Business

The Efficient Business strengthens how work flows across the organisation. It focuses on reducing friction, improving process reliability, and supporting teams to deliver work consistently and effectively. This outcome area addresses the operational constraints that affect performance, from duplicated effort and unclear responsibilities to inconsistent ways of working.

By improving efficiency, organisations reduce operational drag and increase the capacity of teams to deliver value. This supports better utilisation of technology, clearer accountability, and smoother end-to-end processes that contribute to predictable, scalable performance.

The Insightful Business

The Insightful Business enables organisations to make informed, timely, and confident decisions. It focuses on improving visibility of operations, strengthening reporting, and ensuring that data is captured, managed, and interpreted in a way that supports organisational objectives.

Developing this outcome area improves the organisation's ability to understand current performance, identify emerging issues, and assess the impact of change. It provides the foundation for measurement, analysis, and evidence-based planning across all areas of the Intelligent Business.

The Innovative Business

The Innovative Business supports the development of new capability and structured improvement. It enables organisations to explore new approaches, adopt modern tools and methods, and respond effectively to changing needs or opportunities. This outcome area covers areas such as automation, AI adoption, and the creation of new service models or ways of working.

Strengthening this area helps organisations evolve at a controlled pace. It ensures that innovation is introduced safely, aligned to organisational priorities, and built on a stable foundation, without disrupting existing operations or increasing the organisation's level of risk.

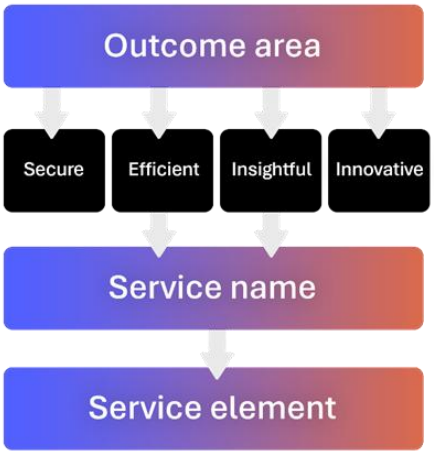
The Value Chain-Led Managed Service

The Value Chain-Led Managed Service provides the operational assurance that underpins every other outcome area. It maintains continuity, stability, and performance by aligning support to the organisation's value chain — the real end-to-end flow of work that keeps the organisation operating.

This outcome area ensures that services are monitored, governed, and improved through a structured, consistent approach. It reduces operational friction, maintains alignment between service delivery and business need, and supports the organisation's ability to sustain improvements made across the other outcome areas.

How Services Align to the Outcome Areas

Each Outcome Area is supported by a set of Service Streams, and each Stream contains the individual Service Elements that make up the work delivered. This structure provides a clear line of sight from each Service Element to the organisational outcome it supports. It ensures that services are delivered consistently, contribute to defined areas of performance, and can be selected according to the organisation's priorities without needing to follow a fixed sequence or maturity path.



The Secure Business

The Secure Business is one of the six outcome areas that make up the Intelligent Business Framework. It represents the organisational conditions required to operate safely, maintain control, and manage security in a way that supports wider business objectives. Within the Framework, the Secure Business strengthens the organisation's ability to reduce exposure, maintain resilience, and ensure that protection is integrated into everyday operations rather than treated as a separate technical activity.

What the Secure Business Is

The Secure Business outcome area focuses on the capability an organisation needs to protect people, data, platforms, and operations in a controlled and consistent manner. It helps organisations maintain dependable service delivery in environments where risks evolve quickly and where security must support, not constrain, how work is carried out. Rather than addressing threats in isolation, the Secure Business provides a structured way to assess exposure, understand risk, and maintain appropriate safeguards across the organisation.

Security within this outcome area is not limited to technical controls. It includes how the organisation manages access, governs information, validates behaviour, and responds to emerging conditions. The Secure Business contributes to stability, continuity, and responsible operational practice by ensuring that protection is applied proportionately and aligned to the organisation's risk landscape and operating environment.

How Work Is Structured Within the Secure Business

To organise the work required across this outcome area, the Secure Business is delivered through five Service Streams. Each Stream represents a different aspect of security capability and provides a defined structure for assessment, protection, monitoring, response, and recovery. While each Stream focuses on a distinct area of work, together they provide a coherent approach for maintaining appropriate levels of protection and for managing security in a predictable and systematic way.

This structure allows organisations to engage with the areas that matter most to them, without needing to follow a fixed sequence or maturity path. It ensures that each service delivered within the Secure Business contributes to a clear outcome and is aligned to the organisation's wider operating model and priorities.

What the Secure Business Helps Organisations Achieve

The Secure Business supports organisations by strengthening their ability to:

- Maintain safe and reliable operations in changing conditions;
- Reduce exposure through appropriate safeguards and informed decision-making;
- Ensure consistent standards of control, governance, and oversight;
- Integrate security considerations into routine activity and project delivery;
- Understand how security affects operational performance and organisational continuity.

These contributions are defined in outcome terms rather than technical terms. The Secure Business enables organisations to maintain trust, uphold obligations, and operate confidently, even as their environments grow and evolve.

How This Outcome Area Supports the Intelligent Business

By developing protection, control, and resilience in a structured way, the Secure Business helps organisations build the dependable foundations that support efficiency, insight, and future capability across the wider Framework. It ensures that work carried out within this outcome area is aligned to organisational objectives, contributes to long-term capability, and reinforces the operating conditions an Intelligent Business depends on.

848 Secure Business – Respond

Alignment to The Intelligent Business

he Respond Service Stream strengthens the Intelligent Business by ensuring the organisation can act with clarity, coordination, and confidence when a security incident occurs.

It provides the capability required to contain threats quickly, assess impact accurately, and recover services in a controlled and accountable manner.

Respond transforms incident handling from reactive activity into a structured organisational function governed by clear procedures and informed decision-making.

Within the Intelligent Business Framework, Respond supports operational reliability by enabling organisations to maintain continuity during disruptive events.

It ensures that decisions are made based on verified information, that communication is coordinated, and that actions follow a predictable and well-governed process. This reduces uncertainty, limits business impact, and supports safe operation under pressure.

Respond also improves value flow across the Secure Business by ensuring that incidents are managed efficiently and consistently. It supports leaders, technical teams, and governance functions with clear insight into what is happening and what must occur next.

By embedding structured response capability, the stream strengthens accountability, supports regulatory and organisational obligations, and improves readiness for future events.

Through these contributions, Respond reinforces the operating conditions required for resilience, stability, and responsible security management across the Intelligent Business.

Service Purpose

The purpose of the Respond Service Stream is to ensure organisations can act decisively and effectively when a security incident occurs. It provides the structures, processes, and expert support required to manage incidents in a controlled, coordinated, and outcome-led manner.

Many organisations struggle with uncertainty during an incident—roles may be unclear, evidence difficult to interpret, and decisions made under time pressure without reliable guidance.

Respond resolves this challenge by establishing defined response procedures, clear escalation pathways, and the capability to assess and manage incidents from initial identification through to safe recovery.

It strengthens the organisation's ability to contain threats, minimise impact, and restore normal operations while maintaining control and preserving evidence.

The stream also embeds post-incident learning, ensuring each event contributes to improved readiness and strengthened resilience.

By enabling structured, predictable incident response, Respond ensures organisations can operate safely even when faced with disruptive or high-pressure security events.

What This Service Provides

The Respond Service Stream provides individuals across the organisation with the clarity, coordination, and structured support required to handle security incidents safely and confidently.

It ensures that roles, expectations, and decision pathways are understood before an incident occurs and that stakeholders have the information and guidance needed during high-pressure events.

Each role group benefits from improved readiness, stronger governance, and a predictable approach to managing disruption.

Role Group	What They Gain	Why They Matter
Executive Teams & Senior Leaders	Clear understanding of incident impact, decision points, and escalation requirements. Confidence that the organisation can contain threats, protect critical services, and recover safely. Assurance that response activities align to governance, regulatory, and operational expectations.	They hold accountability for organisational resilience and must make strategic decisions during disruptive events.
Governance, Risk & Compliance Stakeholders	Visibility into incident handling, supporting compliance oversight and risk assessment. Clarity on how decisions are made, how evidence is handled, and how response aligns to policy. Insight that informs improvement planning and control governance.	They ensure the organisation meets its obligations and maintains responsible, transparent security practice.

Security & Technology Leaders	Defined response structures that guide technical teams during containment, investigation, and recovery. Clear pathways for decision-making and escalation. Information that supports prioritisation and coordinated operational action.	They direct the technical and operational aspects of incident management and depend on reliable processes to act effectively.
Operational & Infrastructure Teams	Clear instructions for containment, restoration, and verification tasks during incidents. Defined communication and collaboration expectations. Assurance that technical actions align with the wider response plan.	They manage the platforms, systems, and services affected by incidents and play a critical role in recovery.
Security Operations & Monitoring Functions	Structured escalation and response procedures for handling validated incidents. Clarity on their role in triage, analysis, and coordination. Support for interpreting events and initiating the correct response pathway.	They provide the first assessment of incident information and trigger response activity across the organisation.

How This Service Is Delivered

The Respond Service Stream is delivered through a structured methodology that ensures organisations are prepared before an incident occurs, supported during the incident, and strengthened afterwards. This approach provides predictable, coordinated, and evidence-led response activity that protects critical services and enables safe recovery. Each stage reinforces organisational resilience and supports clear decision-making throughout the incident lifecycle.

Method Component	Stage 1: Establish Readiness & Response Structures	Stage 2: Identify, Assess & Prioritise the Incident	Stage 3: Contain the Threat & Conduct Investigation	Stage 4: Recover Services & Restore Safe Operation	Stage 5: Review, Learn & Strengthen Future Readiness
Stage Description	This stage prepares the organisation for effective incident handling by defining the structures, processes, and conditions under which response will operate.	This stage confirms that an incident has occurred, assesses its significance, and determines the appropriate response pathway.	This stage focuses on reducing harm, preserving evidence, and understanding the incident's cause, scope, and impact.	This stage supports the organisation in safely restoring affected services and validating that normal operations can resume.	This stage transforms incident insight into improved organisational resilience and refined response capability.
Purpose of the Stage	To ensure the organisation can act decisively when an incident occurs, supported by clear roles and prepared structures.	To establish clarity at the outset, ensuring that response begins in a controlled, informed, and coordinated manner.	To minimise disruption, uncover root cause, and establish a reliable basis for recovery and improvement.	To ensure recovery is safe, traceable, and supported by evidence-led decision-making.	To ensure each incident contributes to continuous improvement and maturity development across the Secure Business.
Activities Included	Reviewing existing response processes and organisational context Defining roles, responsibilities, and escalation pathways Establishing incident classification and	Reviewing initial alerts, telemetry, and stakeholder reports Applying incident classification and severity criteria	Guiding containment actions such as isolating systems or accounts Conducting structured investigation based on available evidence	Advising on restoration steps and service recovery sequencing Validating system integrity and confirming removal of malicious activity	Conducting post-incident reviews and lessons learned sessions Identifying gaps in readiness, communication, or control effectiveness

	decision-making structures Validating tooling, communication channels, and response dependencies	Assessing potential business impact and areas affected Confirming stakeholders who must be engaged	Reviewing timelines, behaviours, and attack progression Providing recommendations to remove threat activity and confirm stability	Coordinating actions across technical and business teams Ensuring communication pathways and governance requirements are supported	Producing improvement recommendations and prioritised actions Updating response plans, playbooks, and governance materials
What This Provides	A clear and operationally ready foundation for coordinated incident response.	A verified understanding of the incident and a structured approach for determining next steps.	Verified insight into the organisation's real security position.	A controlled path back to stable operation, aligned to business priorities and risk expectations.	Clear, actionable improvements that uplift future readiness and strengthen operational resilience.

Service-Level Benefits

The key business-level benefits of the Detect service are:

- Reduces business impact through structured, coordinated incident response.
- Improves recovery speed with clear roles and defined actions.
- Strengthens organisational resilience during high-pressure security events.
- Ensures incidents are handled consistently and traceably.
- Provides expert support for confident decision-making under stress.
- Protects operational continuity during unexpected disruptions.
- Enhances accountability with documented response activities.
- Identifies root causes to prevent future incidents.
- Improves team readiness through validated response processes.
- Supports leadership with clear, actionable incident intelligence.

Service Scope

In-Scope Summary

The Respond Service Stream covers the structured activities required to prepare for, manage, and learn from security incidents.

It focuses on establishing readiness, coordinating response actions, supporting containment and investigation, guiding safe recovery, and strengthening future capability through structured improvement.

The scope includes the processes, decision pathways, and expert support needed to handle disruptive events in a controlled, evidence-led, and predictable manner.

Theme	Description
Response Readiness and Planning	Developing, validating, or reviewing response structures, roles, plans, and escalation pathways.
Incident Assessment and Prioritisation	Confirming that an incident has occurred, assessing severity, and determining initial response actions.
Containment Guidance and Support	Advising on safe and appropriate containment actions to minimise business and operational impact.
Investigation and Evidence Review	Analysing telemetry, reviewing activity, and interpreting available evidence to understand cause and scope.
Recovery Support and Coordination	Guiding restoration of services and validating that systems are safe to return to normal operation.
Post-Incident Learning and Improvement	Conducting structured reviews, identifying gaps, and defining actions to improve readiness and resilience.
Stakeholder Communication and Alignment	Supporting engagement across leadership, governance, operational teams, and third parties where relevant.

Scenario Validation and Preparedness Exercises	Running simulated incidents to test readiness and refine roles, communication, and decision-making structures.

Out-of-Scope Summary

The Respond Service Stream does not include continuous monitoring, proactive threat hunting, long-term operational response management, or the implementation of protection or detection controls delivered through other Secure Business streams.

It does not replace legal, regulatory, or business continuity functions and does not cover remediation or rebuild activities beyond guided recovery support. These exclusions ensure Respond remains focused on structured, controlled incident handling and organisational readiness.

Exclusion	Description
Continuous Monitoring or Alert Triage	Ongoing security monitoring services, SOC operations, or MDR unless separately contracted.
Proactive Threat Hunting	Searching for undetected threats or adversary activity outside the scope of a confirmed incident.
Protection or Detection Control Implementation	Configuring identity, device, data, or platform controls delivered through other Secure Business streams.
Full Remediation or Infrastructure Rebuild	Executing long-term remediation, patching, or system rebuilds following an incident.
Business Continuity or Disaster Recovery Execution	Implementing DR plans or coordinating full-service failover and continuity activities.
Legal, Regulatory, or Insurance Representation	Managing communication with authorities, insurers, or legal bodies beyond technical evidence support.
Third-Party Forensic Certification	Providing forensic services requiring law-enforcement-grade certification unless pre-agreed.
Development of Non-Scoped Playbooks or Processes	Creating additional response materials outside those defined in the engagement scope.
Unscoped or Inaccessible Systems	Responding to incidents affecting systems outside the agreed scope or where access cannot be provided.

Service Element: Incident Response Preparedness Assessment

Description

The Incident Response Preparedness Assessment evaluates the organisation's ability to respond effectively to cybersecurity incidents. It reviews current incident response policies, processes, communication paths, and role definitions to confirm they are clear, actionable, and aligned with recognised good practice such as NIST SP 800-61, ISO 27035, and NCSC guidance.

The assessment examines how people, processes, and technology work together during an incident, identifying gaps that may delay containment, escalate business impact, or hinder recovery. The output is a factual and prioritised improvement plan that strengthens incident response readiness across the organisation.

Deliverables

Deliverable	Description
Readiness Assessment Report	A detailed evaluation of existing incident response capability across people, process, and technology.
Maturity Scorecard	A scored baseline aligned to recognised incident response frameworks.
Gap Analysis	A breakdown of deficiencies, risks, and operational weaknesses affecting response effectiveness.
Improvement Roadmap	A prioritised set of actions to enhance readiness and reduce incident impact.
Stakeholder Presentation	A structured review of findings, dependencies, and recommended next steps.

Dependencies

Delivery of this Service Element requires the following:

- Access to existing incident response policies, procedures, and communication plans.
- Availability of relevant stakeholders for interviews and workshops.
- Access to architecture diagrams or tooling documentation where required.
- Existing monitoring or detection capabilities available for contextual review.

Constraints

This Service Element is subject to the following constraints:

- Assessment findings are dependent on the accuracy and completeness of documentation and stakeholder input.
- The service does not validate technical control effectiveness beyond incident response processes.
- Simulation or testing activities are not included unless scoped separately.

Benefits

This service strengthens The Secure Business by establishing a clear and objective baseline of incident response readiness.

It reduces uncertainty during cyber events, improves coordination across technical and business roles, and provides a practical roadmap for building a more resilient and predictable response capability.

The assessment ensures the organisation understands its current state and has prioritised actions that improve containment, decision-making, and recovery across the security lifecycle.

848 Responsibilities

Under this Service Element, 848 will:

- Conduct documentation review and stakeholder interviews.
- Assess roles, responsibilities, communication paths, and escalation routes.
- Evaluate readiness against recognised incident response frameworks.
- Produce all assessment outputs and improvement recommendations.
- Deliver a structured findings presentation and facilitate knowledge transfer.

Customer Responsibilities

The customer must:

- Provide timely access to incident response documentation and supporting materials.
- Make relevant stakeholders available for interviews and workshops.
- Confirm availability of technical and governance representatives for clarification.
- Review findings and agree ownership of improvement actions.

Assumptions

This Service Element is delivered on the basis that:

- The customer has defined internal contacts for coordination.
- All documentation supplied is accurate and reflects current operating practice.
- Stakeholders are available within agreed timeframes.
- The organisation has an existing security monitoring capability for contextual review.

Exclusions

This Service Element does not include:

- Development of new incident response plans, playbooks, or communication models.
- Live incident response or breach investigation activities.
- Forensic data acquisition or evidence handling.

- Remediation or implementation of improvement actions.
- Business continuity or disaster recovery planning.

Success Measures

This Service Element is successfully delivered when:

- A complete and evidence-based assessment of incident response capability.
- Clear, actionable improvement recommendations aligned to organisational needs.
- Stakeholder understanding of gaps and priorities.
- Agreement and ownership of next steps following the findings presentation.
- Establishment of a measurable readiness baseline for future improvement activities.

Service Element: Incident Response Plan & Playbook Development

Description

The Incident Response Plan & Playbook Development service designs and documents a complete incident response framework tailored to the organisation's operational and regulatory context. It defines how the organisation identifies, classifies, prioritises, and manages security incidents across their lifecycle.

The service produces a formal Incident Response Plan, a standardised Security Event Classification and Severity Framework, clear roles and responsibilities, and a defined set of incident-specific playbooks covering key threat scenarios such as ransomware, data breach, insider threat, or system compromise.

All outputs are aligned with recognised good practice, including NIST SP 800-61, ISO 27035, and NCSC guidance. The resulting framework is actionable, repeatable, and designed to support coordinated incident response across technical and business teams.

Deliverables

Deliverable	Description
Incident Response Plan (IRP)	A formal document defining the organisation's incident response structure, roles, decision points, and process lifecycle.
Security Event Classification & Severity Framework	A standardised model for categorising security events and determining severity, escalation paths, and prioritisation.
Incident Response Playbooks	Tailored, scenario-specific playbooks defining steps for identification, containment, communication, and recovery.
Roles and Responsibilities Matrix (RACI)	A clear mapping of responsibilities across technical, operational, and business stakeholders.
Communication and Escalation Pathways	Defined channels, responsibilities, notification triggers, and required communication steps during an incident.
Maintenance and Review Guidance	Instructions for ongoing upkeep, governance, and periodic review of all response documentation.
Stakeholder Validation Workshop	A structured session to review and confirm the final framework with operational and leadership stakeholders.

Dependencies

Delivery of this Service Element requires:

- Access to existing incident response processes, policies, and any current IR documentation.

- Engagement with stakeholders across IT, security, HR, legal, and communications functions.
- Availability of incident logs or previous incident reports for contextual design.
- Alignment with any existing SOC or MDR operating models where applicable.

Constraints

This Service Element is subject to the following constraints:

- The quality of the framework depends on the accuracy and completeness of customer-provided information.
- Outputs are documentation-based and do not include technical implementation or automation configuration.
- Playbook development is limited to the scenarios agreed at project initiation.
- The service does not include process testing unless delivered through a separate simulation or validation service.

Benefits

This service strengthens The Secure Business by establishing a structured, consistent, and repeatable approach to incident management. It ensures that response activities are coordinated, predictable, and aligned to recognised standards, reducing decision-making delays and improving containment and recovery.

By defining clear roles, escalation paths, and scenario-specific actions, the service enhances organisational readiness and ensures incidents are handled in a disciplined and controlled manner across all business functions.

848 Responsibilities

Under this Service Element, 848 will:

- Conduct discovery sessions and review existing documentation and incident history.
- Define the incident response structure, processes, and governance model.
- Develop a formal Incident Response Plan tailored to the organisation.
- Create agreed incident response playbooks based on priority threat scenarios.
- Produce severity classification and event categorisation models.
- Define communication and escalation pathways.
- Facilitate the validation workshop and complete all documentation handover.

Customer Responsibilities

The customer must:

- Provide access to relevant personnel, documentation, and incident information.

- Participate in interviews, workshops, and validation sessions.
- Review draft materials and provide timely feedback.
- Define internal owners for maintaining and updating the delivered artefacts.
- Confirm the priority incident scenarios for playbook development.

Assumptions

This Service Element assumes:

- Customer stakeholders are available within agreed timeframes for workshops and reviews.
- Existing security incident records, if available, are complete and accessible.
- The organisation has a defined governance model for security and incident management.
- The customer will manage ongoing maintenance of the framework unless separately contracted.

Exclusions

This Service Element does not include:

- Live incident response or active breach management.
- Digital forensics, evidence acquisition, or post-incident investigation.
- Creation of additional playbooks beyond those agreed at initiation.
- Automation design or SOAR configuration.
- Development of business continuity or disaster recovery plans.

Success Measures

This Service Element is successfully delivered when:

- A complete and organisation-approved incident response framework.
- Playbooks that are clear, actionable, and aligned to recognised standards.
- A classification and severity model understood and accepted by stakeholders.
- Improved clarity of roles, responsibilities, and escalation routes.
- Positive validation and agreement from both operational teams and leadership.

Service Element: Incident Automation & Orchestration Enablement

Description

Incident Automation & Orchestration Enablement designs and implements controlled automated response workflows using Microsoft Sentinel, Logic Apps, and Defender XDR. The service integrates detection alerts with pre-approved containment and remediation actions to accelerate incident response and reduce dwell time.

It develops safe, governed automation patterns that isolate compromised devices, disable accounts, block malicious domains, or initiate ticketing workflows within seconds of detection. Each automation is aligned to agreed guardrails and incorporates appropriate approval steps, error handling, and auditability.

The service establishes a scalable automation foundation that improves consistency, accelerates containment, and enables coordinated response across security and operations teams.

Deliverables

Deliverable	Description
Automation Design Blueprint	Documented design of approved automation patterns, integration points, governance standards, and candidate workflow backlog.
Security and Governance Guardrails	Defined policies for approvals, RBAC, managed identities, Key Vault usage, and change control requirements.
Automation Workflows (Playbooks)	Fully built and tested automated workflows aligned to agreed incident scenarios and approval requirements.
Workflow Documentation Pack	Logic descriptions, diagrams, configuration notes, rollback procedures, and operational guidance.
Automation Repository	Exported workflow artefacts, version tags, change logs, and supporting documentation for customer maintenance.
Handover and Demonstration Sessions	Walkthrough of workflow logic, safe-use guidelines, and governance expectations for ongoing operation.

Dependencies

Delivery of this Service Element requires:

- Microsoft Sentinel and Defender XDR deployed and operational.
- Azure Logic Apps available for workflow development.
- Required connectors and permissions configured and accessible.
- Engagement with SOC, IT operations, and platform owners for use-case validation.
- Agreed incident scenarios and approval requirements established prior to build.

Constraints

This Service Element is subject to the following constraints:

- Automation can only execute pre-approved actions defined within governance guardrails.
- Custom API development or third-party integrations may require additional scoping.
- Multi-tenant or cross-environment deployment is not included unless specified.
- Automation effectiveness is dependent on the quality and consistency of upstream alerting.

Benefits

This service strengthens The Secure Business by enabling rapid, predictable, and safe incident containment through governed automation. It reduces response delays, improves consistency across analysts, and ensures actions are traceable, auditable, and aligned with organisational risk appetite.

Automated workflows allow security teams to focus on complex investigation and decision-making while routine containment steps are performed at machine speed under controlled conditions.

848 Responsibilities

Under this Service Element, 848 will:

- Conduct discovery workshops to identify automation opportunities.
- Review existing detection, response, and integration architecture.
- Design automation frameworks, governance standards, and security guardrails.
- Build, test, and validate approved automated workflows.
- Produce workflow documentation and operational guidance.
- Deliver knowledge-transfer sessions and complete service handover.

Customer Responsibilities

The customer must:

- Provide access to relevant systems, documentation, and technical stakeholders.
- Confirm use-cases, approval models, and action guardrails.
- Ensure required permissions, connectors, and platform features are enabled.
- Participate in testing and validation of workflows.
- Manage ongoing maintenance and governance of automations after handover.

Assumptions

This Service Element is delivered on the basis that:

- The customer maintains an operational Microsoft Sentinel and Defender XDR environment.
- Azure Logic Apps is available and correctly configured.
- Stakeholders are available within agreed timeframes for workshops and reviews.
- Use-case priorities and risk tolerances are defined during discovery.
- The customer manages any post-deployment operational updates unless contracted separately.

Exclusions

This Service Element does not include:

- Live incident response or containment during an active security event.
- Development of custom API connectors or non-Microsoft integrations without prior scoping.
- SOAR platform deployment or environment hardening.
- Remediation or reconfiguration of upstream alerts or data connectors.
- Ongoing operational support or workflow maintenance after handover.

Success Measures

This Service Element is successfully delivered when:

- Approved automation patterns and guardrails designed and documented.
- Fully validated workflows performing agreed containment or response actions.
- Stakeholder sign-off on workflow logic, governance controls, and safe-use guidelines.
- Successful handover with operational teams able to manage and maintain automations.
- Demonstrated reduction in manual effort for validated incident types.

Service Element: Managed Detection & Response (MDR)

Description

Managed Detection & Response (MDR) provides a fully managed 24×7 detection and response capability operated by 848's Security Operations Centre (SOC). The service combines continuous monitoring, advanced analytics, automation workflows, and expert-led containment actions to identify, analyse, and respond to threats in real time.

The service integrates Microsoft Sentinel, Defender XDR, and approved automation patterns to deliver coordinated triage, containment, and incident management. During active incidents, SOC analysts perform hands-on containment activities—such as isolating affected endpoints, disabling compromised accounts, or removing malicious artefacts and work with customer IT teams to restore operational stability.

MDR includes a structured onboarding and readiness assessment to confirm telemetry sources, containment pathways, and operational governance are in place before live service commencement. The outcome is a fully managed detection and response function that reduces dwell time, minimises operational impact, and ensures incidents are handled consistently and effectively.

Deliverables

Deliverable	Description
Integrated Sentinel & Defender MDR Environment	A fully configured and validated monitoring and response environment prepared for 24×7 operation.
Response Authority Matrix	A defined model of pre-approved containment actions, escalation thresholds, and authorisation pathways.
Active Containment Playbooks	Pre-approved response actions enabling rapid containment through analyst-led or automated workflows.
HaloPSA Ticketing & Reporting Setup	Incident tracking, workflow automation, SLA dashboards, and reporting configuration.
Monthly Operational Report	A summary of incidents, containment actions, trends, and operational performance.
Quarterly Executive Summary (where applicable)	A leadership-focused update on threat trends, service performance, and improvement recommendations.

Onboarding Completion Pack	Documentation covering integration outcomes, containment validation, and readiness sign-off.

Dependencies

Delivery of this Service Element requires:

- Microsoft Sentinel and Defender XDR licensing and operational configuration.
- Azure Logic Apps connectivity for automation and containment workflows.
- Customer identity, endpoint, and messaging systems integrated for containment actions.
- Access to customer tenant via delegated access or approved controls.
- Customer ITSM or HaloPSA integration for ticketing and escalation.

Constraints

This Service Element is subject to the following constraints:

- Containment actions are limited to those authorised within the Response Authority Matrix.
- Only Microsoft Sentinel, Defender XDR, and approved integrations are monitored as part of the service.
- Bespoke analytics, non-Microsoft telemetry, or third-party platform integration requires separate scoping.
- MDR does not provide long-term forensics, legal support, or extended remediation services.
- Service performance is dependent on the accuracy, completeness, and timeliness of customer telemetry.

Benefits

This service strengthens The Secure Business by providing a continuous, expert-led detection and response capability that materially reduces the time between compromise, containment, and recovery.

MDR ensures that threats are identified quickly, investigated consistently, and managed in a structured and coordinated manner across technical and business stakeholders.

The service brings clarity, predictability, and resilience to incident management and enables organisations to operate with confidence under sustained cyber pressure.

848 Responsibilities

Under this Service Element, 848 will:

- Deliver continuous monitoring and analysis of Microsoft Sentinel and Defender XDR telemetry.

- Perform triage, investigation, and containment for security events under approved playbooks.
- Maintain detection content, automation workflows, and integration configurations within agreed scope.
- Log, track, and manage incidents using HaloPSA.
- Provide monthly operational reporting and governance updates.
- Conduct onboarding activities to validate telemetry, containment pathways, and authorisation processes.
- Coordinate with customer IT teams during containment and recovery activities.

Customer Responsibilities

The customer must:

- Ensure Microsoft Sentinel, Defender XDR, and Azure Logic Apps licensing is active.
- Provide access to required systems, tenants, and telemetry sources.
- Maintain endpoint, identity, and messaging infrastructure required for containment.
- Review and approve the Response Authority Matrix and containment permissions.
- Respond to escalations, provide required approvals, and support remediation activities.
- Ensure ITSM processes are aligned with MDR escalation pathways.

Assumptions

This Service Element assumes:

- Customer platforms (identity, endpoint, messaging) support automated or analyst-led containment actions.
- All required telemetry sources are available and functioning before MDR commencement.
- Customer provides points of contact for escalation, technical clarification, and incident collaboration.
- The organisation maintains responsibility for remediation beyond initial containment.

Exclusions

This Service Element does not include:

- Long-term forensics, evidence preservation, or digital investigation.
- Business continuity or disaster recovery execution.
- Creation of new detection rules beyond the standard MDR rule pack.
- Integration of third-party SIEM or EDR tools not part of the Microsoft ecosystem.

- Incident response retainer beyond containment (offered as a separate service).
- Remediation beyond initial containment and eradication actions.

Success Measures

This Service Element is successfully delivered when:

- MDR environment onboarded successfully and validated for live 24×7 monitoring.
- Containment actions executed within approved authority pathways.
- Incidents logged, triaged, and managed consistently through HaloPSA workflows.
- Monthly reporting delivered with clear insight into threats and operational trends.
- Increased visibility and reduced dwell time for incidents within monitored environments.
- Demonstrated improvement in customer readiness and response performance over time.

Service Element: Incident Investigation & Lessons Learned

Description

This service provides expert-led investigation of cybersecurity incidents to establish root cause, scope, and business impact using Microsoft Sentinel, Defender XDR, and related Microsoft 365 telemetry. It consolidates technical evidence, stakeholder insights, and event chronology to produce a clear and factual record of what occurred, how it occurred, and what corrective actions are required.

Following the investigation, 848 facilitates a structured Lessons Learned Workshop that engages both technical and business stakeholders to review response performance, highlight any gaps in process or capability, and establish an agreed action plan that strengthens the organisation's readiness for future incidents.

The outcome is a complete, consumable incident review that restores confidence, strengthens organisational resilience, and supports continuous improvement across the Secure Business Respond capability.

Deliverables

Deliverable	Description
Incident Timeline Reconstruction	A chronological reconstruction of the incident using Microsoft Sentinel, Defender XDR, Microsoft 365 audit logs, and available supporting artefacts.
Root Cause and Impact Summary	Clear explanation of the initiating event, methods used by the adversary (where applicable), affected systems, and business impact.
Technical Findings Report	A detailed written report outlining key findings, evidence references, gaps observed in detection or response processes, and validation of containment activities already completed.
Recommendations Tracker	A structured improvement log with prioritised corrective actions across people, process, and technology.
Lessons Learned Workshop	Facilitated session with technical, operational, and business stakeholders to validate findings, identify performance gaps, and agree next steps.
Lessons Learned Summary Pack	Presentation artefact capturing improvement actions, risks identified, and recommended updates to plans, playbooks, or governance.

Dependencies

Delivery of this Service Element requires:

- Access to Microsoft Sentinel, Defender XDR, and Microsoft 365 telemetry for the period covering the incident.

- Access to relevant stakeholders for interviews, including IT operations, security personnel, and business representatives.
- Confirmation from the customer that the incident is contained and systems are stable prior to analysis.
- Any information captured during earlier response actions (tickets, notes, screenshots, emails, logs).

Constraints

This Service Element is subject to the following constraints:

- The service does not include forensic imaging, evidential chain of custody, or legally defensible forensic acquisition.
- Investigation quality and depth depend on available telemetry and log retention within the customer environment.
- The investigation does not include live containment, eradication activities, or recovery actions. These require an Incident Response Retainer.
- External-party liaison (law enforcement, regulators, insurers) is outside the scope of the service.

Benefits

This service provides a structured, factual review of an incident that strengthens the organisation's Secure Business position by identifying root causes, confirming containment, and establishing clear corrective actions that enhance future incident response readiness.

848 Responsibilities

Under this Service Element, 848 will:

- Conduct evidence review using Microsoft Sentinel, Defender XDR, and Microsoft 365 telemetry.
- Reconstruct the incident timeline and validate that containment actions have been successfully completed.
- Interview relevant stakeholders to understand event context, operational impact, and response actions taken.
- Produce the incident findings report, recommendations tracker, and Lessons Learned summary pack.
- Facilitate the Lessons Learned Workshop and guide stakeholders through prioritised improvements.
- Maintain secure handling of all customer data during the engagement.

Customer Responsibilities

The customer must:

- Confirm that the incident is fully contained and systems are safe to analyse.
- Provide administrative access to Microsoft Sentinel, Defender XDR, Microsoft 365, and relevant systems.
- Supply any available incident artefacts, including tickets, screenshots, logs, and communications.
- Ensure the attendance of appropriate stakeholders during interviews and the Lessons Learned Workshop.
- Implement recommended improvements unless separately contracted through other Secure Business services.

Assumptions

This Service Element assumes:

- All work is delivered remotely unless otherwise agreed.
- Adequate telemetry exists within the customer environment to support a meaningful reconstruction of events.
- The incident does not require evidential standards such as chain of custody or legal forensic support.
- Customer systems are accessible and stable at the time analysis begins.

Exclusions

This Service Element does not include:

- Forensic imaging, data recovery, or evidential investigation.
- Live incident response, containment, or system remediation.
- Third-party coordination with law enforcement, insurers, or regulators.
- Full control framework audits beyond the scope of investigation.
- Implementation of corrective actions identified in the Lessons Learned session.

Success Measures

This Service Element is successfully delivered when:

- A complete, verified timeline of the incident is produced and agreed with stakeholders.
- Clear identification of root cause, affected systems, and business impact.
- Delivery of a validated improvement plan with prioritised corrective actions.
- Stakeholder alignment is achieved through the Lessons Learned Workshop.
- The organisation demonstrates strengthened response maturity and increased readiness for future incidents.