848

Detect

Service Definition

Secure Business

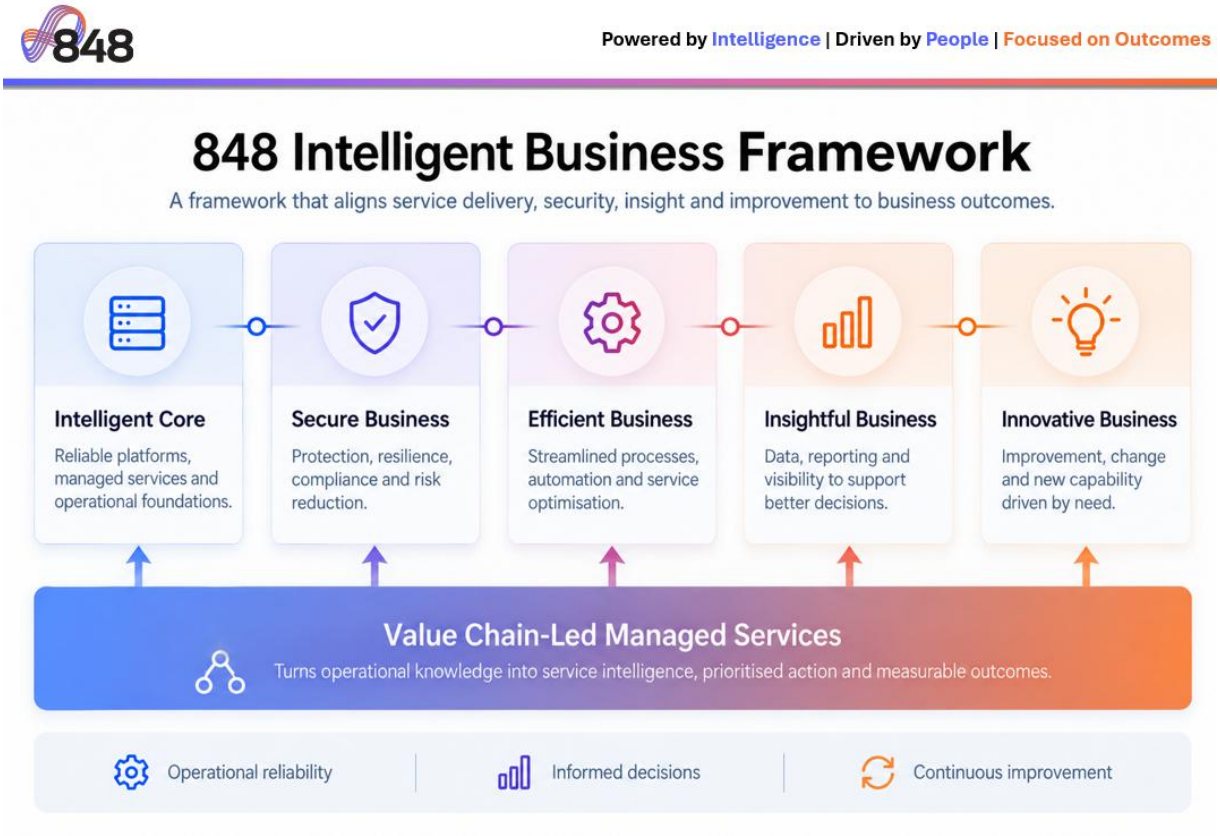
Version 0.6 | September 2026

Driven by **people.** Powered by **intelligence.** Value chain **led.**

1. Service Overview

Security teams need to recognise which signals require attention and understand where visibility is missing. A growing volume of alerts offers limited assurance when data sources are incomplete or detection rules create excessive noise. Detect establishes and improves the monitoring capability needed to identify suspicious activity and direct it to the right people.

Detect sits within The Secure Business, part of 848's Intelligent Business Framework. The framework connects technology investment to the way the organisation operates, makes decisions and delivers services. Each engagement addresses the selected outcome while considering its place in the wider customer environment.



From business need to usable capability

The service connects telemetry to a usable detection process. Reliable ingestion makes activity visible; analytic content gives that activity meaning; clear triage and escalation routes turn findings into operational decisions. Customers can select enablement work or a managed monitoring element according to the capability they already have.

Within the wider portfolio, Protect supplies safeguards and Respond defines or delivers the action taken when an incident is confirmed. Detect provides the link between them. Its findings also inform security improvement priorities, helping platform and service owners understand recurring exposure across the customer environment.

2. Scope and Service Boundaries

Customers select the elements that support their intended outcome. The scope identifies what 848 will deliver and the work retained by customer teams or suppliers.

Service	Outcome
Monitoring platform enablement	Sentinel or an expressly agreed equivalent is designed and configured with selected data connectors. Ingestion checks establish the available monitoring coverage; live SOC operation is a separate element.
Detection analytics and optimisation	Analytic rules and correlation logic are reviewed or developed for agreed use cases. Tuning and coverage analysis help reduce irrelevant alerts and explain remaining detection gaps.
XDR and threat intelligence integration	Selected Defender XDR signals and intelligence feeds are connected to enrich detection context. Bespoke connectors and non-Microsoft integrations require explicit scope.
SOC operations framework	Triage models and escalation workflows define how alerts should be handled. Performance measures and reporting expectations support operational ownership; staffing and live monitoring are separate.
Managed security operations	The selected managed SOC arrangement monitors and validates events, investigates alerts and escalates findings. Coverage hours and response responsibilities are agreed for the commissioned service; hands-on remediation and recovery are separate.
Detection testing and simulation	Controlled simulations test agreed detection scenarios and identify missed or misleading signals. Full penetration testing, destructive testing and remediation are outside this element.
Dashboards and reporting	Selected Sentinel workbooks or Power BI reports present security and SOC measures for the intended audience. Data sources and reporting logic are documented for use after delivery.
Advanced detection analytics	Microsoft-native behavioural and anomaly capabilities are enabled for agreed use cases. This covers platform capabilities, with external machine-learning models and custom training pipelines separately scoped.
Threat landscape reporting	Contextual threat reporting relates external activity to the organisation’s exposure and priorities. Findings inform defensive planning and operational review.

Dependencies and exclusions

Enablement and managed operation are commissioned separately. The service depends on the quality and availability of connected telemetry. Tool deployment does not itself provide continuous analyst coverage, and managed monitoring does not automatically include system recovery, patching or forensic investigation. Hours, escalation expectations and authorised actions belong in the agreed service arrangements.

3. How 848 Delivers the Service

Delivery follows the selected scope, using the customer's operating context to guide the work. The sequence below explains how evidence and decisions progress towards the agreed outputs. Customer review and knowledge transfer form part of that progression.

Set the detection objectives

848 reviews the threats and services that matter to the customer. Security owners confirm the monitoring boundary and existing response arrangements. The review identifies the telemetry and use cases required to support those objectives.

Establish usable visibility

For selected enablement work, 848 configures the design and connects agreed sources. Ingestion and data quality checks show where monitoring is reliable and where prerequisites remain unresolved. Customer platform owners assist with access and source configuration.

Validate and interpret signals

848 develops or tunes the commissioned analytics and validates their behaviour. Where managed operations are selected, analysts monitor activity and investigate alerts using the available context. Findings are prioritised and escalated through the agreed operational routes.

Review coverage and operational readiness

848 explains detection findings and remaining gaps to the receiving team. Reporting and selected simulations help the customer review coverage. Enablement work concludes with handover; managed operation continues through its agreed reporting and improvement cycle.

4. Service Delivery and Management

4.1. Deliverables and Outcomes

The outputs give the customer a usable record of the work and the information needed to act on it. The selected elements determine which deliverables apply; findings and limitations remain visible alongside the results.

Deliverable	Use for the customer
Monitoring configuration and coverage	Shows connected sources, analytic content and known visibility limitations for the selected work.
Detection findings and operational records	Provides validated alerts, test findings or reporting according to the commissioned element.
Operational framework and guidance	Explains triage, escalation and reporting responsibilities, together with the relevant configuration knowledge.

4.2. Working with 848

Customer security owners confirm priorities and response authority. Platform owners maintain telemetry prerequisites. The nominated response team receives escalations and undertakes actions outside the managed SOC boundary.

Participant	Responsibility
848 delivery team	Performs the selected work, explains findings and documents the relevant outputs. Coordinates review and knowledge transfer with the customer.
Customer service owner	Confirms the intended outcome and scope. Makes customer decisions and identifies who can resolve dependencies or approve changes.
Customer specialists and suppliers	Provide relevant information and agreed access. Complete retained activity and participate in review or validation where their systems or processes are involved.
Receiving team	Reviews the relevant outputs and takes ownership of the activities that continue after handover.

4.3. Service Assurance

Validation checks source ingestion and selected detection behaviour. Managed reviews consider alert handling and reporting against the agreed coverage. Gaps in telemetry or untested scenarios remain visible in the findings.

Review focus	What is checked
Scope alignment	The delivered work and outputs address the agreed requirements and selected service elements.

Review focus	What is checked
Evidence and validation	Findings or test results show the basis for conclusions, including known limitations and unresolved dependencies.
Customer acceptance	Relevant owners review the outputs and understand any open actions before accepting the commissioned work.

4.4. Onboarding

Onboarding establishes the conditions needed for useful delivery. The customer and 848 confirm what the engagement should achieve and check that the people and information needed for the selected work will be available.

Preparation	What needs to be established
Outcome and scope	Confirm the selected elements, boundaries and expected outputs, together with the customer's priorities.
Information and access	The agreed SIEM and security licences must be available. Connected sources need working telemetry and suitable permissions. Customer contacts and escalation routes must be confirmed before managed monitoring starts.
Participants and decisions	Identify the service owner, relevant specialists and receiving team. Confirm review participants and escalation routes.
Delivery readiness	Agree the applicable schedule and customer prerequisites. Confirm any operational constraints affecting access, validation or handover.

4.5. Operating and Improving

Reporting can identify noisy rules, coverage gaps and recurring threat patterns. The customer prioritises further tuning or engineering work; continuous optimisation is provided only within the selected managed scope.

4.6. Handover and Exit

An enablement handover transfers configuration and operating guidance. Exit from managed monitoring must identify the receiving monitoring and response owners so coverage and escalation responsibilities are understood.

Handover item	Purpose
Agreed outputs	Provide the final documents or configuration material relevant to the selected service.
Findings and open actions	Preserve the evidence, limitations and remaining work for the customer or receiving provider.
Knowledge and ownership	Explain how the outputs should be used and confirm who owns the next operational or improvement activity.

5. Why 848

848 helps organisations improve how technology supports the way they operate, make decisions and deliver services. Our focus is not on deploying technology for its own sake, but on connecting technology investment to measurable business outcomes.

Our services are aligned through The Intelligent Business Framework, which brings together five outcome areas: The Intelligent Core, The Secure Business, The Efficient Business, The Insightful Business and The Innovative Business. This provides a consistent way to move from technology foundations and security through to operational efficiency, data-led decision-making and innovation, without treating each requirement as an isolated project.

848 combines consulting, engineering and managed service capability within one UK-based team. That matters because the people who design and implement change understand how technology must operate once it enters live service. Architecture, cloud, security, data, Power Platform, Dynamics 365, Microsoft 365 and managed services can therefore be considered as connected parts of the customer environment rather than separate technical towers.

Our Microsoft capability is supported by established partner credentials and practical delivery experience across Microsoft Azure, Microsoft 365, Power Platform, Dynamics 365, Fabric, Sentinel, Defender, Intune, Entra ID and Purview. 848 is a Microsoft Solutions Partner for Security and a Microsoft Direct CSP, giving our teams direct access to Microsoft technologies, programmes and commercial capability.

Service quality and security are supported by recognised organisational standards. 848 holds ISO/IEC 27001, ISO 9001, Cyber Essentials and Cyber Essentials Plus, with security-cleared capability available where required. These controls sit behind the way we manage information, quality, access, risk and service delivery across customer engagements.

What differentiates 848 is the connection between delivery and improvement. Through Value Chain-Led Managed Services, service information is converted into practical intelligence about how technology and services perform across users, teams, suppliers, systems and hand-offs. Service Flow Analysis extends that view by identifying friction, delay, rework, unclear ownership and recurring service issues across end-to-end journeys. The result is a clear improvement backlog based on real operational evidence rather than assumption.

We also place a strong emphasis on internal capability. Knowledge transfer, clear ownership and practical handover are built into our services so that customers understand what has been delivered, how it works and how it should evolve. Where 848 remains involved, improvement continues through review, prioritisation and measurable service outcomes rather than static support.

For customers, the result is a partner able to move from strategy through design, implementation, validation, operation and improvement while maintaining a consistent view of the wider business outcome. 848 brings together the people, Microsoft capability and service intelligence needed to make technology easier to operate, easier to improve and more valuable over time.