mvw CYBERSECURITY SERVICES

# MVW SOC SERVICE DEFINITION

MVW CYBERSECURITY SERVICES

JANUARY 2026

Prepared for:

mvw CYBERSECURITY SERVICES

# TABLE OF CONTENTS

# 1. THIS DOCUMENT

This document is the MVW Service Definition for our Security Operations Centre version January 2026.

This document serves as the overarching service definition for the MVW Security Operations Centre. Whilst specific implementation will vary depending on the client-specific scope and agreement, this document defines the key areas of the service and identifies where variation may occur.

Prepared by MVW Cybersecurity Services on January 2026.

## 1.1 ABOUT MVW TECHNOLOGY LIMITED

MVW Technology Limited are a technology consultancy and managed service provider who specialise in delivering a Modern Workplace and IT Infrastructure services.

Our focus in this field enables us to remain in touch with the evolution of end-user and infrastructure technologies and apply innovative and effective solutions to meet business needs, whilst aligning to operational, security and regulatory requirements.

Our senior consultants each have over 25 years of experience each in top tier organisations including leading investment and retail banks.

## 1.2 VERSION HISTORY

| VERSION | DATE | AUTHOR | UPDATES |
|---|---|---|---|
| 2601 | 09 Jan 2026 | James Rayner | Updated document to support G-Cloud |

## 2. SERVICE

Managed security monitoring and incident handling using Microsoft Sentinel. The service operates inside the client tenant. Telemetry stays in the client environment.

Baseline service scope:

- Continuous monitoring of Sentinel incidents and alerts
- Triage and investigation with evidence recorded in each Sentinel incident
- Severity assignment using a three-level priority scale, HIGH to LOW, determined by severity indicated within the Sentinel platform and associated incident generated
- Escalation by email by default, with phone alerts where agreed upon
- Ongoing tuning of core detections to reduce noise
- Connector and ingestion health checks for key data sources
- Monthly reporting aligned to the selected service tier

Service boundaries:

- The service manages Sentinel operations and agreed upon content only
- The service does not include advanced remediation or complex environment wide changes
- The service does not include full forensic acquisition or malware reverse engineering unless added under a separate statement of work or included specifically in the

# 3. SERVICE TIERS

The following section outlines the three tiers offered by MVW and where variations lie along with suitability for different organisations.

## 3.1 TIER 1 CORE (FOUNDATIONAL)

Recommended for: organisations typically < 50 users and/or early-stage security maturity.

Focus: foundational monitoring and standardised coverage.

Included:

- Standard deployment of core Sentinel analytics/detections and baseline incident workflow
- 24/7 triage and investigation within agreed scope
- Tuning of baseline rules to reduce noise
- Monthly report delivered by email
- Standard communications & escalation (email, phone alert if required)

Constraints (Core):

- Custom detection engineering limited to minor tuning, bespoke use-cases typically delivered via SOW or uplift to Tier 2/3
- Reporting focused on Sentinel incidents/alerts and core operational metrics

## 3.2 TIER 2 ENHANCED (COMPREHENSIVE COVERAGE & GOVERNANCE)

Recommended for: growing organisations or regulated sectors needing stronger oversight and sector alignment.

Focus: sector-specific detections and broader security reporting.

Included (in addition to Tier 1):

- Monthly governance & review call with stakeholders from both sides
- Deployment of sector-specific analytics/detections aligned to the client's risk profile and sector threats
- Reporting across a wider dataset where integrated: identities, vulnerabilities, and devices
- Increased tuning cadence and structured improvement backlog

Constraints (Enhanced):

- Bespoke detections/playbooks supported within agreed allowances. Complex engineering may require a SOW.

## 3.3 TIER 3 OPTIMISED (COLLABORATIVE & INTEGRATED CAPABILITY)

Recommended for: mature security functions requiring deep integration and continuous optimisation.

Focus: significant cross-collaboration and integration into threat detection engineering.

Included (in addition to Tier 2):

- Integration into the client's threat detection engineering lifecycle (backlog reviews, use-case design, acceptance criteria)
- Joint optimisation of detections, automation, and operational workflows
- Expanded continuous improvement programme
- Potential to deliver additional cybersecurity engagements (separately contracted), such as threat-hunting campaigns, IR readiness, tabletop exercises, and detection validation

Note: Additional engagements are delivered as separate statements of work (SOWs) or pre-agreed packages. Tier 3 provides the operating model and collaboration structure to enable them efficiently.

# 4. RESPONDING TO INCIDENTS

## 4.1 REMEDIATION RECOMMENDATIONS ONLY (OPTIONAL)

MVW investigates and provides detailed recommended remediation steps but does not execute changes. This option helps where clients are required to retain full operational control.

## 4.2 EXECUTING STANDARD RESPONSES (OPTIONAL)

Where agreed within the contract, MVW may execute pre-approved, standard response actions. This allows the SOC to act quickly in response to observed incidents.

Examples of standard actions, note these must be explicitly listed and approved:

- Device isolation
- Password resets / account disabling
- Session/token revocation
- Malicious email removal/quarantine and block
- IOC blocking (hash/IP/domain) in approved tooling
- Disable email inbox rules such as forwarding or email deletion

Explicitly excluded (not included unless separately contracted):

- Advanced bespoke remediation and complex environmental changes
- Full forensics (acquisition, reverse engineering) and legal/regulatory management
- Ransomware negotiations

## 4.3 DEFAULT APPROVAL FLOW

MVW can vary this model per client. The following is the default approach:

- HIGH: MVW may execute pre-approved standard actions immediately, with explicit pre-approval in the contract
- MEDIUM: During Core business hours – client approval required prior to execution, Out of hours – MVW may execute pre-approved standard actions if explicitly stated

- Only actions in the signed specifically mentioned in the contract can be actioned
- All actions must be fully logged and recorded in the Sentinel incident (and Freshdesk if used)

If authority/access is unavailable, MVW reverts to advice-only and escalates to the client. Recommended remediation steps will be appropriately detailed in email reporting, via Teams or over the phone.

# 5. DATA BACKUP AND DISASTER RECOVERY

Microsoft Sentinel and the underlying Log Analytic Workspace are hosted in the client environment, telemetry retention and platform resilience are primarily governed by the client's Azure architecture and Microsoft availability. MVW provides operational continuity and restoration capability.

## 5.1 MANAGED CONTENT BACKUP

MVW maintains an export/backup approach for managed configuration items, such as:

- Analytics rules (including sector-specific and custom rules)
- Automation rules
- Playbooks (Logic Apps) definitions (where MVW-managed)
- Watchlists and agreed configuration artefacts
- Tuning and suppression rationale, runbooks, and operating procedures

## 5.2 RESTORATION SUPPORT

- Restoration of baseline offering, with high priority analytics and detections running.
- Reapplication of tuning and exception logic
- Verification of ingestion → detection → incident → escalation pipeline

## 5.3 BUSINESS CONTINUITY

- 24/7 analyst coverage, handovers, and surge management
- Alternative communications if primary channels are unavailable
- Documented escalation pathways for major incidents

# 6. ONBOARDING & OFFBOARDING SUPPORT

MVW will assist with both onboarding and offboarding of the solution, whilst specific process may differ depending on the client, their current state and requirements, the broad approach is detailed below. Prior to service signoff, MVW will provide details of dependencies and milestones.

## 6.1 ONBOARDING

Discovery & Design:

- Confirm scope, priority assets, log sources, severity model, escalation and communications
- Confirm response model (advice-only vs authorised execution) and approval catalogue
- Confirm ITSM approach: Sentinel-only vs Freshdesk

Technical Enablement:

- Configure GDAP + Azure Lighthouse access with least privilege
- Validate data connectors and ingestion health
- Deploy baseline analytics/detections (plus sector-specific for Tier 2/3)
- Configure automations/playbooks as contracted
- Configure Freshdesk integration if required

Operational Readiness:

- Finalise runbooks, notification templates, and stakeholder contacts
- Hypercare tuning period (commonly 2–6 weeks)

## 6.2 OFFBOARDING

- Remove MVW access (GDAP/Lighthouse, RBAC, PIM/JIT roles)
- Removal of MVW IP (analytics, automations etc)
- Deliver handover pack (see Section 12)
- Knowledge transfer sessions
- Optional parallel run (as agreed)

# 7. SERVICE CONSTRAINTS

## 7.1 MAINTENANCE WINDOWS & CHANGE CONTROL

- SOC monitoring continues 24 x 7 x 365
- Detection/automation changes follow agreed change control
- Planned changes scheduled during agreed windows, emergency changes allowed for any critical issues with post-change reporting

## 7.2 CUSTOMISATION & THREAT DETECTION ENGINEERING BOUNDARIES

- Tier 1 focuses on standard detections and tuning
- Tier 2 includes sector-specific analytics and enhanced reporting, with additional continuous improvements
- Tier 3 enables integration into detection engineering and may support additional engagements (separately contracted), often working alongside dedicated security functions within the client

## 7.3 DEPENDENCIES

- Coverage and quality of onboarded telemetry sources
- Client approvals (where required) for MEDIUM actions
- Reliable cross-tenant access configuration and identity governance
- Appropriate access and permissions in the environment to facilitate onboarding and ongoing management of the solution

# 8. SERVICE LEVELS (PERFORMANCE, AVAILABILITY, SUPPORT HOURS)

## 8.1 SUPPORT HOURS

- 24 × 7 × 365 monitoring and incident handling for all tiers
- Governance and reviews align to tier (Tier 1 email report, Tier 2/3 monthly call)

## 8.2 TARGET RESPONSE TIMES (EXAMPLE SLO)

| SLO TITLE | DESCRIPTION | SLO |
|---|---|---|
| SOC Availability | The time during which the SOC is monitoring customer environment | The SOC will provide a 24x7 service. |
| Incident Response | The speed at which incident produced within the SOC is acknowledged and responded to by an analyst<br><br>*Severity defined in Sentinel for each alert/incident* | High severity incidents: 99% within 1 hour<br><br>Medium severity incidents 99% within 4 hours<br><br>Low severity incidents 99% within 8 hours |
| Customer Raised Incident Acknowledgement | The speed at which incidents raised by a customer are picked up by a member of the SOC | Acknowledged within 1 hour. |
| Customer Use Case Request Acknowledgement | The speed at which a request for the development of a use case is acknowledged by a member of the SOC | Acknowledged within 1 working day |
| Customer Use Case Successful Development | The number of use case development requests from customers that are completed | Completed within 10 working days |
| Additional Service Request Acknowledgement | The speed at which a request for additional service(s) are acknowledge by a member of the MVW team, for example requests for additional data source integration | Acknowledged within 2 working days |

## 8.3 COMMUNICATIONS & ESCALATIONS

- Escalations from MVW to client: Email by default, Phone alert if required by client for HIGH/MEDIUM and documented in the escalation matrix
- Client communications to MVW SOC: Teams chat, phone, or email
- Ticketing: Sentinel incidents by default, Freshdesk used where the client requires ITSM ticketing
  Note: Response-time SLOs apply to MVW SOC operations. Platform uptime is governed by Microsoft and the client's tenant configuration.

# 9. AFTER-SALES SUPPORT (MONTHLY REPORTING & GOVERNANCE)

## 9.1 MONTHLY REPORTING BY TIER

- Tier 1 (Core): Monthly report delivered by email
- Tier 2 (Enhanced): Monthly governance & review call and in-depth reporting
- Tier 3 (Optimised): Monthly governance & review call with expanded stakeholder collaboration and in-depth reporting

## 9.2 MONTHLY REPORT CONTENT (BASELINE)

- Incident volumes by severity/category/source
- MTTA/triage/handling metrics and SLO performance
- Notable incidents (HIGH/MEDIUM summaries)
- Top noisy detections and tuning actions
- Ingestion/connectors health highlights and telemetry gaps
- Improvement backlog (prioritised)

## 9.3 ENHANCED/OPTIMISED REPORTING EXTENSIONS (TIER 2/3)

- Identity-related risk trends (e.g., sign-in anomalies, risky users) where integrated
- Device posture trends (endpoint health indicators, prevalent threats) where integrated
- Vulnerability trend summaries (top critical vulnerabilities, exposure areas) where integrated
- Sector-aligned threat themes and recommended detection improvements

# 10. TECHNICAL REQUIREMENTS

## 10.1 CLIENT ENVIRONMENT REQUIREMENTS

- Microsoft Sentinel enabled on a Log Analytics workspace in the client tenant
- Required licensing and data sources enabled (client responsibility)
- Connectivity for ingestion (agents/APIs/syslog as applicable)
- Identity readiness for GDAP/Lighthouse cross-tenant access

## 10.2 ACCESS & SECURITY REQUIREMENTS

- Least privilege RBAC aligned to tasks (incident operations vs content management)
- MFA enforced for MVW personnel
- Prefer PIM/JIT elevation for privileged tasks (where supported)
- Administrative and response actions auditable via logs and incident/ticket notes

## 10.3 ITSM REQUIREMENT (OPTIONAL)

- If ITSM is required: Freshdesk will be used
- Otherwise: incidents are handled and tracked in Sentinel as the system of record

# 11. OUTAGE AND MAINTENANCE MANAGEMENT

## 11.1 PLANNED MAINTENANCE

- Documented change record with scope, risk, rollback, and validation
- Scheduled within agreed windows
- Post-change verification of ingestion and detection operation

## 11.2 UNPLANNED OUTAGES / SERVICE DEGRADATION

- Identify and declare impact (connector failures, ingestion drop, playbook failure, access issues)
- Notify stakeholders via agreed channels
- Prioritise restoration of critical sources and detection pathways

## 11.3 MONITORING THE MONITORING

- Alerts for ingestion failures/drops (critical connectors)
- Playbook failure alerting
- Health checks for critical detections
- Operational dashboards

## 12. HOSTING OPTIONS AND LOCATIONS

- Hosting: Client-hosted Microsoft Sentinel + Log Analytics Workspace (one per client)
- Location/data residency: determined by the client's chosen Azure region
- MVW does not host client telemetry as part of this service model (unless separately contracted)

## 13. ACCESS TO DATA (UPON EXIT)

Because the service operates inside the client tenant, the client retains ownership and access to all telemetry, incidents, and configurations.

MVW provides an offboarding handover pack including:

- Connector inventory and ingestion status
- Removal of MVW intellectual property such as analytics
- Runbooks, escalation matrix, and response action catalogue
- Monthly reporting pack for agreed period
- MVW will revoke all access (GDAP/Lighthouse/RBAC/PIM) and provide transition support (timeboxed)

# 14. SECURITY

## 14.1 IDENTITY & ACCESS SECURITY

- Least privilege RBAC and role separation (operations vs engineering where appropriate)
- MFA mandatory
- JIT elevation preferred for privileged tasks
- Named accounts only with no shared accounts
- Periodic access reviews and immediate revocation for leavers

## 14.2 DATA HANDLING

- Data remains in the client tenant with MVW accesses configured as only what is required for investigation and response
- Any extracted artefacts follow the client's data classification and retention rules
- Reporting minimises sensitive content unless explicitly agreed

## 14.3 MVW SECURITY INCIDENT NOTIFICATION

If an MVW-side incident could affect client confidentiality or service integrity, MVW will notify the client per agreed timelines with an impact assessment and corrective actions.

# 15. ANNEX A  RESPONSE ACTION CATALOGUE (TEMPLATE)

Attach this annex to the contract to enable explicit pre-approval and clear boundaries. For each approved action, define:

- Action name
- Tools permitted (e.g., Defender for Endpoint / Entra ID / Exchange actions)
- Severity eligibility (HIGH / MEDIUM)
- Approval rule (HIGH pre-approved immediate, MEDIUM in-hours approval, MEDIUM out-of-hours pre-approved execution if authorised)
- Preconditions / safety checks (entity validation, criticality checks, service account handling)
- Execution steps (high level)
- Rollback procedure (if feasible)
- Notification requirement (who, how, and within what time)
- Audit logging requirements (Sentinel incident notes, Freshdesk ticket if used, and tool audit logs)

## 16. ANNEX B  TIER SUMMARY (ONE-PAGE VIEW)

- Core: foundational SOC coverage for smaller/less mature organisations, standard detections, monthly email report
- Enhanced: sector-specific detections + broader identity/device/vulnerability reporting, monthly governance call
- Optimised: integrated with client detection engineering, deep collaboration, enables additional cyber engagements

END OF DOCUMENT