

TECHNICAL PRODUCT BRIEF

Managed Security Operations

Validate the operating model behind security monitoring.

Why customers use this service

Review source health, triage, investigation and escalation workflows to identify telemetry gaps, inconsistent decisions and actions that may not reach accountable owners.

What we assess

Source onboarding	Expected telemetry, ownership and usable context.
Ingestion health	Missing, delayed or malformed security data.
Detection workflow	How supported alerts enter triage and investigation.
Triage quality	Consistent priority, context and disposition decisions.
Investigation evidence	Timelines, artefacts and reasoning supporting conclusions.
Escalation and handoff	Triggers, authority and accountable customer actions.
Case lifecycle	Status, closure, exceptions and linked remediation.
Operational reporting	Source health, activity, outcomes and unresolved risk.

Engagement outcome

An operating-model review with source and workflow evidence, material gaps, prioritised actions and validation outcomes.

How the engagement works

How we test or review

Damocles reconciles expected sources with ingestion health, samples detections and traces representative alerts through triage, investigation, escalation, customer action and closure. Operational records support service review but monitoring cannot guarantee detection of every attack.

Testing and review perspectives

Source owner and onboarding contact

Confirms expected telemetry, collection method, ownership and source-side health during onboarding and gap review.

Included when: Used for source inventory and ingestion accountability.

Access: Source inventory, owners, expected event types and maintenance context.

Limitations: Cannot establish SOC handling after ingestion.

Monitoring or SOC analyst

Reviews ingestion state, detection output and representative alerts in the monitoring platform.

Included when: Used for health, detection and triage procedures.

Access: Platform access, parser state, last-event time, detections and alerts.

Limitations: Sampled alerts cannot prove every attack is detectable.

Investigation and escalation analyst

Builds timelines, preserves evidence and applies severity and escalation procedures to representative cases.

Included when: Used for investigation and handoff assessment.

Access: Case records, queries, evidence stores, escalation matrix and contacts.

Limitations: A sample does not establish handling of every incident type.

Customer action owner and service reviewer

Tracks customer-owned actions, closure evidence, reporting and service-improvement decisions.

Included when: Used for communication, closure and periodic review.

Access: Action register, reports, service measures, attendees and decisions.

Limitations: Service review cannot eliminate telemetry or detection limitations.

Customer access or evidence typically required

Source inventory, owners, expected event types and maintenance context.; Platform access, parser state, last-event time, detections and alerts.; Case records, queries, evidence stores, escalation matrix and contacts.; Action register, reports, service measures, attendees and decisions.

What you receive

An operating-model review with source and workflow evidence, material gaps, prioritised actions and validation outcomes.

Detailed technical coverage

Source onboarding

What is assessed	Damocles checks an expected telemetry source through ownership, collection method, parsing, event receipt and onboarding acceptance.
Perspective / access	Source owner and onboarding contact. Assessment requires source inventory, monitoring access, sampled detections, alerts, cases, escalation records, actions and service reports, selected specifically for source onboarding.
Evidence	Evidence records the source state, event timestamp, parser status, detection, alert, query, investigation timeline, escalation or action record relevant to source onboarding.
References	Incident Response Recommendations and Considerations for Cybersecurity Risk Management Revision 3
Applicability	Applies to Source onboarding when the operational process and representative records fall within the managed service period.
Limitations	The conclusion is limited to the sampled source onboarding; sampling cannot prove every event or attack is detected; customer and provider responsibilities remain bounded.

Source inventory

What is assessed	Damocles reconciles the customer-approved source inventory with platform entries, owners, expected event types and current status.
Perspective / access	Customer action owner and service reviewer. Assessment requires source inventory, monitoring access, sampled detections, alerts, cases, escalation records, actions and service reports, selected specifically for source inventory.
Evidence	Evidence records the source state, event timestamp, parser status, detection, alert, query, investigation timeline, escalation or action record relevant to source inventory.
References	Incident Response Recommendations and Considerations for Cybersecurity Risk Management Revision 3
Applicability	Applies to Source inventory when the operational process and representative records fall within the managed service period.
Limitations	The conclusion is limited to the sampled source inventory; sampling cannot prove every event or attack is detected; customer and provider responsibilities remain bounded.

Ingestion health

What is assessed	Damocles compares expected cadence with last-event time, transport state, parsing status and source-side health for sampled sources.
Perspective / access	Source owner and onboarding contact. Assessment requires source inventory, monitoring access, sampled detections, alerts, cases, escalation records, actions and service reports, selected specifically for ingestion health.
Evidence	Evidence records the source state, event timestamp, parser status, detection, alert, query, investigation timeline, escalation or action record relevant to ingestion health.
References	Incident Response Recommendations and Considerations for Cybersecurity Risk Management Revision 3
Applicability	Applies to Ingestion health when the operational process and representative records fall within the managed service period.
Limitations	The conclusion is limited to the sampled ingestion health; sampling cannot prove every event or attack is detected; customer and provider responsibilities remain bounded.

Telemetry gaps

What is assessed	Damocles identifies missing, delayed, filtered or unusable telemetry and records the affected detection and investigation use cases.
Perspective / access	Source owner and onboarding contact. Assessment requires source inventory, monitoring access, sampled detections, alerts, cases, escalation records, actions and service reports, selected specifically for telemetry gaps.
Evidence	Evidence records the source state, event timestamp, parser status, detection, alert, query, investigation timeline, escalation or action record relevant to telemetry gaps.
References	Incident Response Recommendations and Considerations for Cybersecurity Risk Management Revision 3
Applicability	Applies to Telemetry gaps when the operational process and representative records fall within the managed service period.
Limitations	The conclusion is limited to the sampled telemetry gaps; sampling cannot prove every event or attack is detected; customer and provider responsibilities remain bounded.

Detection content

What is assessed	Damocles reviews selected detection logic, data dependencies, scope, suppression, tuning history and known blind spots.
Perspective / access	Source owner and onboarding contact. Assessment requires source inventory, monitoring access, sampled detections, alerts, cases, escalation records, actions and service reports, selected specifically for detection content.
Evidence	Evidence records the source state, event timestamp, parser status, detection, alert, query, investigation timeline, escalation or action record relevant to detection content.
References	Incident Response Recommendations and Considerations for Cybersecurity Risk Management Revision 3
Applicability	Applies to Detection content when the operational process and representative records fall within the managed service period.
Limitations	The conclusion is limited to the sampled detection content; sampling cannot prove every event or attack is detected; customer and provider responsibilities remain bounded.

Alert triage

What is assessed	Damocles samples representative alerts and records enrichment, severity, disposition, timing and analyst rationale.
Perspective / access	Source owner and onboarding contact. Assessment requires source inventory, monitoring access, sampled detections, alerts, cases, escalation records, actions and service reports, selected specifically for alert triage.
Evidence	Evidence records the source state, event timestamp, parser status, detection, alert, query, investigation timeline, escalation or action record relevant to alert triage.
References	Incident Response Recommendations and Considerations for Cybersecurity Risk Management Revision 3
Applicability	Applies to Alert triage when the operational process and representative records fall within the managed service period.
Limitations	The conclusion is limited to the sampled alert triage; sampling cannot prove every event or attack is detected; customer and provider responsibilities remain bounded.

Investigation workflow

What is assessed	Damocles reconstructs representative investigation timelines from alerts, queries, evidence, hypotheses and analyst decisions.
Perspective / access	Monitoring or SOC analyst. Assessment requires source inventory, monitoring access, sampled detections, alerts, cases, escalation records, actions and service reports, selected specifically for investigation workflow.
Evidence	Evidence records the source state, event timestamp, parser status, detection, alert, query, investigation timeline, escalation or action record relevant to investigation workflow.
References	Incident Response Recommendations and Considerations for Cybersecurity Risk Management Revision 3
Applicability	Applies to Investigation workflow when the operational process and representative records fall within the managed service period.
Limitations	The conclusion is limited to the sampled investigation workflow; sampling cannot prove every event or attack is detected; customer and provider responsibilities remain bounded.

Escalation

What is assessed	Damocles compares sampled escalation decisions and timing with severity, responsibility, contact and handoff requirements.
Perspective / access	Source owner and onboarding contact. Assessment requires source inventory, monitoring access, sampled detections, alerts, cases, escalation records, actions and service reports, selected specifically for escalation.
Evidence	Evidence records the source state, event timestamp, parser status, detection, alert, query, investigation timeline, escalation or action record relevant to escalation.
References	Incident Response Recommendations and Considerations for Cybersecurity Risk Management Revision 3
Applicability	Applies to Escalation when the operational process and representative records fall within the managed service period.
Limitations	The conclusion is limited to the sampled escalation; sampling cannot prove every event or attack is detected; customer and provider responsibilities remain bounded.

Customer communications

What is assessed	Damocles reviews representative customer notifications for timing, content, channel, acknowledgement and follow-up.
Perspective / access	Source owner and onboarding contact. Assessment requires source inventory, monitoring access, sampled detections, alerts, cases, escalation records, actions and service reports, selected specifically for customer communications.
Evidence	Evidence records the source state, event timestamp, parser status, detection, alert, query, investigation timeline, escalation or action record relevant to customer communications.
References	Incident Response Recommendations and Considerations for Cybersecurity Risk Management Revision 3
Applicability	Applies to Customer communications when the operational process and representative records fall within the managed service period.
Limitations	The conclusion is limited to the sampled customer communications; sampling cannot prove every event or attack is detected; customer and provider responsibilities remain bounded.

Investigation evidence

What is assessed	Damocles verifies that sampled investigations retain queries, events, notes, timestamps and decision evidence needed for review.
Perspective / access	Source owner and onboarding contact. Assessment requires source inventory, monitoring access, sampled detections, alerts, cases, escalation records, actions and service reports, selected specifically for investigation evidence.
Evidence	Evidence records the source state, event timestamp, parser status, detection, alert, query, investigation timeline, escalation or action record relevant to investigation evidence.
References	Incident Response Recommendations and Considerations for Cybersecurity Risk Management Revision 3
Applicability	Applies to Investigation evidence when the operational process and representative records fall within the managed service period.
Limitations	The conclusion is limited to the sampled investigation evidence; sampling cannot prove every event or attack is detected; customer and provider responsibilities remain bounded.

Action ownership

What is assessed	Damocles traces remediation and containment actions to named customer or provider owners, due dates and acceptance evidence.
Perspective / access	Customer action owner and service reviewer. Assessment requires source inventory, monitoring access, sampled detections, alerts, cases, escalation records, actions and service reports, selected specifically for action ownership.
Evidence	Evidence records the source state, event timestamp, parser status, detection, alert, query, investigation timeline, escalation or action record relevant to action ownership.
References	Incident Response Recommendations and Considerations for Cybersecurity Risk Management Revision 3
Applicability	Applies to Action ownership when the operational process and representative records fall within the managed service period.
Limitations	The conclusion is limited to the sampled action ownership; sampling cannot prove every event or attack is detected; customer and provider responsibilities remain bounded.

Closure criteria

What is assessed	Damocles checks sampled closures for disposition, evidence, customer acknowledgement, residual actions and reopen criteria.
Perspective / access	Source owner and onboarding contact. Assessment requires source inventory, monitoring access, sampled detections, alerts, cases, escalation records, actions and service reports, selected specifically for closure criteria.
Evidence	Evidence records the source state, event timestamp, parser status, detection, alert, query, investigation timeline, escalation or action record relevant to closure criteria.
References	Incident Response Recommendations and Considerations for Cybersecurity Risk Management Revision 3
Applicability	Applies to Closure criteria when the operational process and representative records fall within the managed service period.
Limitations	The conclusion is limited to the sampled closure criteria; sampling cannot prove every event or attack is detected; customer and provider responsibilities remain bounded.

Operational reporting

What is assessed	Damocles reviews operational reports for source health, alerts, investigations, timing, actions, trends and stated limitations.
Perspective / access	Source owner and onboarding contact. Assessment requires source inventory, monitoring access, sampled detections, alerts, cases, escalation records, actions and service reports, selected specifically for operational reporting.
Evidence	Evidence records the source state, event timestamp, parser status, detection, alert, query, investigation timeline, escalation or action record relevant to operational reporting.
References	Incident Response Recommendations and Considerations for Cybersecurity Risk Management Revision 3
Applicability	Applies to Operational reporting when the operational process and representative records fall within the managed service period.
Limitations	The conclusion is limited to the sampled operational reporting; sampling cannot prove every event or attack is detected; customer and provider responsibilities remain bounded.

Service review

What is assessed	Damocles walks through service-review inputs, attendees, decisions, actions and subsequent improvement tracking.
Perspective / access	Customer action owner and service reviewer. Assessment requires source inventory, monitoring access, sampled detections, alerts, cases, escalation records, actions and service reports, selected specifically for service review.
Evidence	Evidence records the source state, event timestamp, parser status, detection, alert, query, investigation timeline, escalation or action record relevant to service review.
References	Incident Response Recommendations and Considerations for Cybersecurity Risk Management Revision 3
Applicability	Applies to Service review when the operational process and representative records fall within the managed service period.
Limitations	The conclusion is limited to the sampled service review; sampling cannot prove every event or attack is detected; customer and provider responsibilities remain bounded.

Service boundaries and exclusions

What is assessed	Damocles records monitored sources, hours, responsibilities, exclusions, response authority and customer dependencies.
Perspective / access	Source owner and onboarding contact. Assessment requires source inventory, monitoring access, sampled detections, alerts, cases, escalation records, actions and service reports, selected specifically for service boundaries and exclusions.
Evidence	Evidence records the source state, event timestamp, parser status, detection, alert, query, investigation timeline, escalation or action record relevant to service boundaries and exclusions.
References	Incident Response Recommendations and Considerations for Cybersecurity Risk Management Revision 3
Applicability	Applies to Service boundaries and exclusions when the operational process and representative records fall within the managed service period.
Limitations	The conclusion is limited to the sampled service boundaries and exclusions; sampling cannot prove every event or attack is detected; customer and provider responsibilities remain bounded.

Detection limitations

What is assessed	Damocles documents known telemetry, detection, timing and response limitations and states that monitoring cannot guarantee detection of every attack.
Perspective / access	Source owner and onboarding contact. Assessment requires source inventory, monitoring access, sampled detections, alerts, cases, escalation records, actions and service reports, selected specifically for detection limitations.
Evidence	Evidence records the source state, event timestamp, parser status, detection, alert, query, investigation timeline, escalation or action record relevant to detection limitations.
References	Incident Response Recommendations and Considerations for Cybersecurity Risk Management Revision 3
Applicability	Applies to Detection limitations when the operational process and representative records fall within the managed service period.
Limitations	The conclusion is limited to the sampled detection limitations; sampling cannot prove every event or attack is detected; customer and provider responsibilities remain bounded.

Methodologies and standards

Incident Response Recommendations and Considerations for Cybersecurity Risk Management Revision 3 — Guides incident-response preparation, exercise analysis and improvement reporting.

Security and Privacy Controls for Information Systems and Organizations Release 5.2.0 — Provides Release 5.2.0 control context only where a verified mapping is declared.

Information Security Manual June 2026 — Provides ASD ISM control context only for the declared mapping and observed behaviour.

Prudential Standard CPS 234 Information Security effective 1 July 2019 — Provides supporting regulatory context for the entity's broader control-testing program.

Standards and control mappings

Prudential Standard CPS 234 Information Security effective 1 July 2019 — supporting-evidence

References: CPS 234 paragraphs 35-36

Assessed: The authorised technical scope as one input to the regulated entity's systematic testing program.

Evidence: Dated scope, coverage, findings, remediation and limitations.

Applicability: Only for an APRA-regulated entity that places the engagement within its control-testing program.

Limitations: Does not assess annual program coverage, independence governance, Board reporting or obligations outside scope.

What you receive: report and evidence

Authorised scope and rules of engagement

Records authorised scope and rules of engagement produced from the authorised Managed Security Operations work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Coverage matrix

Records coverage matrix produced from the authorised Managed Security Operations work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Retest and residual-risk record

Records retest and residual-risk record produced from the authorised Managed Security Operations work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Source inventory and health record

Records source inventory and health record produced from the authorised Managed Security Operations work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Investigation timeline

Records investigation timeline produced from the authorised Managed Security Operations work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Escalation and action record

Records escalation and action record produced from the authorised Managed Security Operations work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Service review record

Records service review record produced from the authorised Managed Security Operations work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Scope and safety limitations

- Only expressly authorised assets, identities, locations and activities are assessed.
- Higher-risk, disruptive, destructive and third-party activity requires separate written authority.
- Point-in-time evidence cannot establish continuous operation or conditions outside the engagement.

Assurance boundary

Damocles maps assessed coverage and observations to agreed objectives as traceable technical evidence. The review is not a certification, does not establish complete compliance, and does not confirm controls outside the authorised scope.

Review metadata

Owner: Technical Assurance

Last reviewed: 2026-08-10

Next review due: 2026-12-10

Scope this engagement with Damocles Security
damocles.com.au/contact

Assurance boundary

Damocles maps assessed coverage and observations to agreed objectives as traceable technical evidence. The review is not a certification, does not establish complete compliance, and does not confirm controls outside the authorised scope.

This brief supports engagement scoping. The authorised scope, rules of engagement and applicable agreement govern delivery.