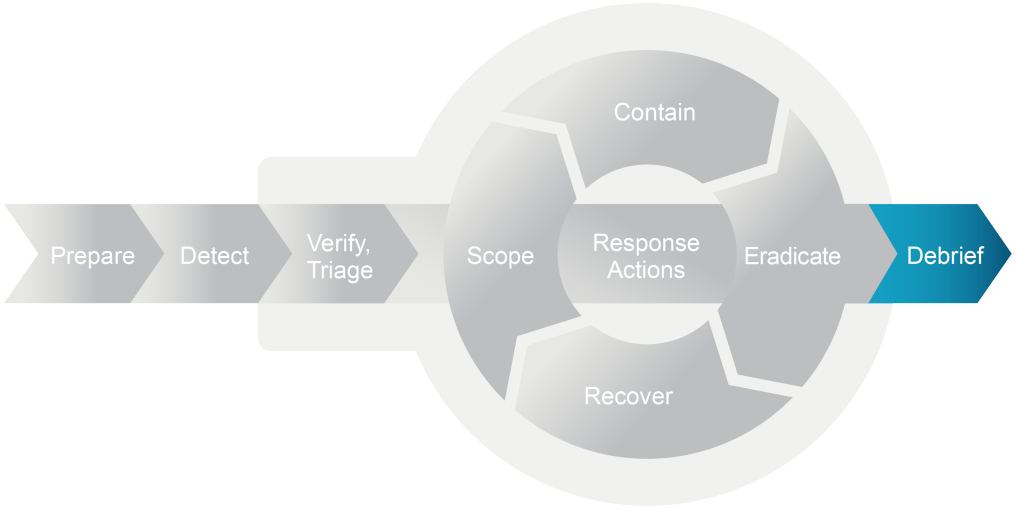
Debrief: Step-by-Step



The following steps provide a condensed reference for debrief activities. Each step corresponds to topics covered in the Debrief Activity chapter of *Dynamic Incident Response* (www.dynamicincidentresponse.com), organized for use when documenting the incident, capturing lessons learned, and driving organizational improvement. The debrief serves three primary objectives: documenting what happened, understanding root causes and contributing factors, and transforming the experience into organizational improvement.

Step 1. Determine Debrief Scope and Documentation Requirements

1. Assess transition readiness, including:
   - Confirm response actions loop has concluded with no new IOCs discovered.
   - Verify that organizational decision-makers have approved the transition to debrief.
   - Ensure critical systems have been restored and validated.
   - Document any residual risks accepted by leadership.
2. Determine documentation depth based on incident characteristics, including:
   - Review organizational thresholds for formal documentation (system count, data exposure, regulatory notification, response duration).
   - Assess whether the incident triggered external notification requirements.
   - Consider potential litigation, regulatory inquiry, or law enforcement involvement.
   - Consult with legal counsel on documentation and retention requirements.
3. Select appropriate debrief approach:
   - Lightweight debrief: Ticket-based documentation with team lead sign-off for contained incidents.
   - Formal debrief: Comprehensive documentation with AAR and executive reporting for significant incidents.
   - Phased debrief: Capture essential information immediately and defer deeper analysis when personnel or time are constrained, guided by the organization's risk tolerance.
   - Document the rationale for the selected approach in incident records.
4. Address legal and regulatory considerations, including:
   - Consult legal counsel on documentation practices that protect the organization while supporting

legitimate learning objectives.
    - Consider whether attorney-client privilege structures are appropriate for sensitive incident analysis, recognizing that scope and durability vary by jurisdiction.
    - Identify regulatory frameworks that impose specific documentation and retention requirements.
    - Balance the need for thorough learning documentation against litigation and disclosure risk.

Step 2. Manage Temporary Assets Created During Response

1. Review forensic evidence for retention decisions, including:
    - Inventory all forensic artifacts collected (disk images, memory captures, network captures, log archives).
    - Consult legal counsel on retention requirements based on potential litigation or regulatory obligations.
    - Identify artifacts with ongoing value for threat intelligence, training, or future investigations.
    - Document retention decisions and destroy artifacts not required for retention.
2. Address temporary accounts and elevated access, including:
    - Review incident documentation for all temporary accounts created during the response.
    - Disable or delete temporary accounts unless there is a compelling operational need.
    - Revoke elevated access granted to responders during the incident.
    - Document account disposition in incident records with timestamps.
3. Evaluate temporary monitoring configurations, including:
    - Assess whether temporary monitoring addresses previously undetected attack vectors.
    - Evaluate operational impact (performance overhead, alert volume) of retained monitoring.
    - Coordinate with security operations on the permanent integration of valuable configurations.
    - Remove monitoring configurations that impose excessive burden without proportionate value.
    - Document decisions on monitoring retention or removal.

Step 3. Consolidate Incident Documentation

1. Gather documentation from all sources, including:
    - Collect notes from ticketing systems, chat channels, shared documents, and email threads.
    - Request individual responder notes while memories remain fresh.
    - Compile forensic analysis reports, tool outputs, and investigation findings.
    - Gather communication records, including stakeholder updates and decision documentation.
2. Validate and refine the incident timeline, including:
    - Walk through the timeline with important responders to verify accuracy.
    - Fill in gaps identified during documentation review.
    - Reconcile conflicting timestamps or accounts of events.
    - Document confidence levels for timeline elements based on the quality of the evidence.
3. Document important decisions made during the response, including:
    - Record significant decisions with alternatives considered and rationale for chosen approach.
    - Capture decisions that later proved suboptimal with an analysis of what information would have improved outcomes.
    - Note any disagreements among responders and how they were resolved.
    - Preserve decision documentation for future reference and potential legal proceedings.

Step 4. Capture Incident Metrics

1. Calculate detection and response metrics, including:
    - Mean Time to Detect (MTTD): Elapsed time from incident start to detection.
    - Mean Time to Respond (MTTR): Elapsed time from detection to resolution.
    - Time to Containment: Elapsed time from detection to attacker activity stopped.
    - Time to Eradication: Elapsed time from containment to persistence removal complete.
    - Time to Full Recovery: Elapsed time from detection to all systems restored.
    - Total Incident Lifecycle: Complete duration from initial compromise to verified resolution (combines MTTD and MTTR).
2. Document scope and impact metrics, including:
    - Number of systems affected (servers, workstations, cloud resources).
    - Number of user accounts compromised or requiring credential reset.
    - Data exposure scope (record count, data classification, regulatory categories).
    - Business impact (operational disruption duration, revenue impact if applicable).
3. Record resource utilization, including:
    - Personnel hours invested in response activities.
    - External consulting or support services engaged.
    - Tool and infrastructure costs incurred.
    - Any ransom payments or extortion costs (if applicable).
4. Preserve metrics for organizational improvement, including:
    - Record metrics in a consistent format for comparison across incidents.
    - Compare metrics against organizational baselines where available.
    - Identify trends indicating improvement or degradation in response capabilities.
    - Feed metrics into security program planning and resource justification.

Step 5. Conduct After-Action Review

1. Schedule and prepare for the AAR, including:
    - Schedule a session within one to two weeks of incident closure, while the details remain fresh.
    - Invite representatives from all teams involved in the response.
    - Prepare a timeline visualization and an important findings summary for the presentation.
    - Establish a blameless postmortem culture with ground rules emphasizing process improvement over individual blame. Focus discussion on systemic weaknesses such as inadequate controls, unclear procedures, and resource constraints rather than individual actions. Handle individual performance concerns separately from the debrief.
2. Facilitate discussion around core AAR questions:
    - What was supposed to happen? (Review incident response plan, playbooks, established procedures).

- What actually happened? (Walk through timeline, decisions, and actions taken).
- Why did differences occur? (Distinguish plan failures from execution failures).
- What can we do better? (Develop specific, actionable recommendations).
- What worked well? (Identify successful aspects to retain or expand).

3. Capture and prioritize recommendations, including:
   - Document all improvement suggestions from participants.
   - Categorize recommendations by implementation timeline (immediate, short-term, long-term).
   - Assign owners to each recommendation with expected completion dates.
   - Prioritize based on risk reduction value and implementation feasibility.
4. Document AAR outcomes, including:
   - Record participants, discussion summary, and important findings.
   - Document recommendations with assigned owners and timelines.
   - Note any unresolved questions requiring further investigation.
   - Schedule follow-up reviews to verify the implementation of the recommendations.

Step 6. Develop Incident Reports (When Required)

1. For lightweight documentation (contained incidents), including:
   - Add a debrief summary section to the incident ticket.
   - Document what happened, what worked well, and improvement actions.
   - Record participants in the debrief discussion.
   - Obtain incident lead and management sign-off.
   - Close the incident with documented approval.
2. For formal documentation, establish the report's purpose and audience, including:
   - Identify the primary audience and the decisions the report should inform.
   - Determine the distribution scope (internal-only, or shared with external parties).
   - Assess evidentiary requirements (forensic standards vs. operational documentation).
   - Review compliance obligations that impose specific documentation requirements (HIPAA, PCI DSS, GDPR).
   - Decide on format approach (single comprehensive document or separate reports for different audiences).
3. For formal documentation (significant incidents), develop an executive summary report, including:
   - Keep the report concise (one to three pages) for executive readability.
   - Include incident overview, business impact, important findings, and metrics.
   - Present recommendations with resource requirements in business terms, using a structured framework (opportunity, benefit, cost, time, resources) to support decision making.
   - Specify decisions required from leadership.
   - Reference the technical report for detailed information.
4. For formal documentation (significant incidents), develop a technical incident report, including:
   - Document the complete timeline with attacker activity and response actions.
   - Include attack analysis mapped to frameworks (e.g., MITRE ATT&CK, if applicable).
   - Catalog affected assets, compromised identities, and indicators of compromise.
   - Document root cause analysis findings and contributing factors.
   - Provide comprehensive recommendations with implementation guidance.
   - Include appendices with detailed artifacts, queries, and supporting evidence.

Step 7. Present Findings and Recommendations to Stakeholders

1. Prepare and schedule the presentation session, including:
    - Schedule a session promptly after consolidating documentation (within one to two weeks of incident closure).
    - Invite decision-makers with authority to approve resources and policy changes.
    - Prepare presentation materials summarizing findings, impact, and recommendations.
    - Designate facilitator and note-taker roles.
2. Conduct the presentation session, including:
    - Walk through the incident timeline and important findings.
    - Present business impact and risk exposure in terms relevant to leadership.
    - Review recommendations with implementation timelines and resource requirements.
    - Reserve time for discussion and stakeholder questions.
    - Capture decisions, approvals, and action items during the session.
3. Document and distribute session outcomes, including:
    - Distribute a summary of decisions and action items within twenty-four to forty-eight hours.
    - Record recommendations approved, modified, or deferred.
    - Document resource commitments secured during the session.
    - Confirm accountability assignments for approved recommendations.

Step 8. Drive Organizational Improvement

1. Integrate lessons learned into organizational processes, including:
    - Update incident response plans and playbooks based on findings.
    - Revise detection rules and monitoring configurations to address visibility gaps.
    - Develop training scenarios based on the incident for future responder preparation.
    - Share relevant threat intelligence with industry partners and ISACs (as appropriate).
2. Track recommendation implementation, including:
    - Enter approved recommendations into security project tracking systems.
    - Establish milestone dates for implementation progress.
    - Assign accountability for each recommendation to specific individuals.
    - Communicate implementation expectations to responsible parties.
3. Conduct follow-up reviews, including:
    - Schedule 30/60/90-day reviews to assess implementation progress.
    - Include leadership representation in follow-up reviews to maintain visibility.
    - Address obstacles or resource constraints preventing implementation.

    - Escalate stalled recommendations to the appropriate decision-makers.
4. Close the debrief activity, including:
    - Verify all immediate recommendations have been implemented or are on track.
    - Confirm long-term recommendations are incorporated into planning cycles.
    - Archive incident documentation according to retention policies.
    - Update organizational metrics and trend tracking with incident data.