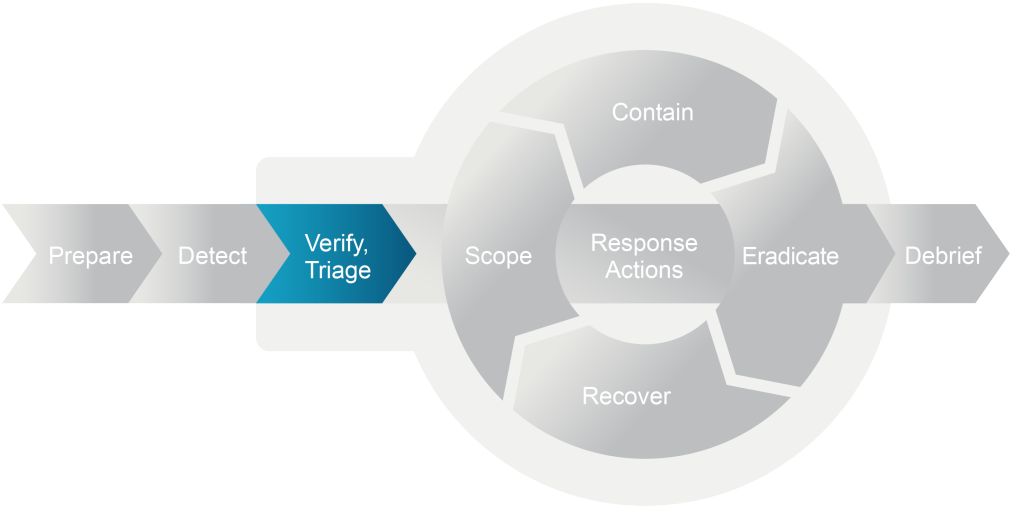
Verify and Triage: Step-by-Step



The following steps provide a condensed reference for verification and triage activities. Each step corresponds to topics covered in the Verify and Triage Activities chapter of *Dynamic Incident Response* (www.dynamicincidentresponse.com), organized for use when validating a potential incident, assessing risk, and working with decision-makers to determine response priorities. Verification serves as a gating function before engaging the broader team: it ensures that the response effort is appropriate for the risk and avoids expending resources on incidents that are not real.

Step 1. Document the Incident Details

Use the incident tracking platform established during preparation. Representative documentation fields include:

- Incident identifier
- Title
- Handler ID
- Summary
- Classification
- Evidence references

Maintain documentation integrity by keeping notes focused on the incident at hand, avoiding contamination that could compromise the documentation's validity as evidence in legal proceedings.

Step 2. Enrich Events of Interest with Cyber Threat Intelligence

Representative activities include:

- Query CTI platforms using technical indicators such as IP addresses, domain names, URLs, or file hashes observed in the environment.
- Cross-reference multiple CTI sources to increase confidence in the assessment.
- Check indicators against the organization's local knowledge base of known false positive sources.

- Pivot to related indicators revealed by CTI platforms and spot-check the environment for them, only to the extent needed to inform the verification decision. Enterprise-wide hunting for the full IOC set is the scope activity's responsibility once the incident is verified.

Step 3. Perform an Initial Risk Assessment

Classify the incident as low, medium, high, or critical (or use another classification system that more closely matches the needs of the organization). Representative considerations include:

- Consider attribution confidence, relevance to the organization, attacker capability, and typical impact from CTI sources when calibrating the risk classification.
- Remember that the absence of threat intelligence does not indicate the absence of a threat.

Step 4. Verify the Incident

Use the information collected during the detect activity and CTI enrichment to select one of three verification outcomes.

- **Continue**: The incident is real. Escalate and engage the broader incident response team and stakeholders.
- **Stop**: The incident is not real. Closing an unusual-but-benign finding is harder than it sounds, and the analyst's confidence should match the strength of the documentation.
  - Document the reasoning: what triggered the alert, what evidence ruled out compromise, and what time window and data sources were examined.
  - Add the benign source to the organization's local false-positive knowledge base so future alerts referencing the same indicator close faster.
  - Notify stakeholders who reported or expected action, including the original reporter and any downstream teams.
  - Close the incident in the tracking platform with a clear classification (false positive, authorized activity, duplicate, or other) for reporting and trend analysis.
- **Defer**: The available information is insufficient. Request additional information from the reporting party or other sources before making a determination.

Step 5. Triage by Presenting to Decision-Makers

Present the verified incident to decision-makers (managers, executives, data owners, legal counsel, or business unit leaders with authority over the response). Representative activities include:

- Use plain language to explain the incident and the potential impact on the organization.
- Provide context by connecting the incident to the organization's policies, procedures, and operations.
- Offer recommendations for response actions based on the risk classification and available incident information.
- Be prepared to answer questions about the incident, its potential impact, and recommended response actions.

Step 6. Work with Decision-Makers on Response Actions and Resource Allocation

Representative activities include:

- Decision-makers should consider the impacted service, the potential impact of the incident on the organization, regulatory exposure, and the resources available for the response effort.
- Response actions may include assigning resources to investigate, engaging legal counsel, or notifying law enforcement.
- Recognize that the analyst's role may shift from technical investigation to coordination support, particularly when regulatory requirements or legal considerations drive the response effort.

Step 7. Review and Improve the Verification and Triage Process

Representative activities include:

- Track false-positive rates at triage as a quality indicator, watching for drift that suggests upstream detection tuning is needed.
- Track outcomes of incidents initially stopped or deferred. If any are reopened later as real incidents, diagnose what was missed and update verification criteria.
- Exercise the verification workflow periodically by rerunning prior incidents through the current process to confirm that risk assessment, CTI enrichment, and decision-maker presentation still work as intended.
- Capture recurring patterns that slow verification, including ambiguous alerts, missing enrichment sources, and unclear escalation paths, and feed improvements back into the Prepare and Detect activities.
- Solicit decision-maker feedback on whether presentations enabled informed decisions, and whether recurring follow-up questions signal gaps in how incidents are framed.