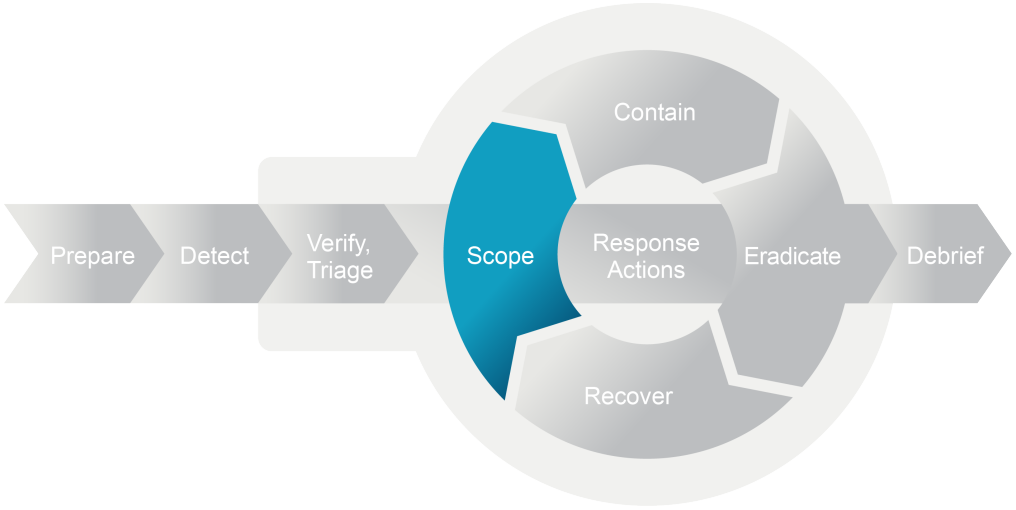
Scope: Step-by-Step



The following steps provide a condensed reference for scoping activities. Each step corresponds to topics covered in the Scope Activity chapter of *Dynamic Incident Response* (www.dynamicincidentresponse.com), organized for use when determining the full extent of compromise across the environment.

Step 1. Identify Indicators of Compromise from Detection and Verification

Categorize the IOCs handed off from verify and triage into the canonical inventory used for sweeps. Representative IOC categories include:

- File-based indicators (hashes, filenames, file paths).
- Network indicators (IP addresses, domains, URLs, signatures).
- Process and service indicators (process names, command-line arguments).
- Registry and configuration indicators (registry keys, configuration changes).
- Account-based indicators (unauthorized accounts, suspicious usage patterns).
- Behavioral indicators (temporal patterns, data movement, lateral movement).

Step 2. Conduct Enterprise-Wide Hunting for Identified IOCs

This is the IOC-driven sweep during a verified incident, distinct from the standing hypothesis-driven hunting program owned by detect. Representative activities include:

- Search centralized log analysis tools (SIEM, log aggregation systems).
- Leverage EDR platforms to search across managed endpoints.
- When EDR is not available, use inventory management tools, active scanning, network scans, or custom scripts to probe for IOCs.
- Apply threat-hunting platforms that combine endpoint, network, and logging data to provide overlapping analysis coverage.

Step 3. Apply Progressive Scoping Methodology

Representative activities include:

- Prioritize critical assets (domain controllers, file servers, databases, systems with sensitive data).
- Expand laterally to systems connected to known-compromised hosts.
- Conduct an environmental sweep across all systems.

Step 4. Reconstruct the Attack Timeline

Scope owns the canonical attack-progression timeline; subsequent activities annotate it (eradicate adds eradication-sequencing markers; debrief consolidates into the final narrative). Representative activities include:

- Identify the initial compromise and the patient zero system.
- Map lateral movement through authentication logs and file access patterns.
- Identify the persistence mechanism deployment timeline.
- Determine when sensitive data was accessed or exfiltrated.

Step 5. Document Scoping Findings

Representative activities include:

- List all compromised systems identified.
- Record IOCs discovered during scoping.
- Create a timeline visualization of the attack's progression.
- Note any visibility gaps or systems requiring additional investigation.

Step 6. Address Scoping Challenges

Representative activities include:

- Identify and document visibility gaps (unmanaged systems, limited logging, IoT, and ICS devices).
- For systems with limited logging, use alternative evidence sources such as network flow data and authentication logs from connected systems.
- For ICS and industrial devices without centralized logging (for example, programmable logic controllers), rely on network flow data as the primary source of evidence.
- Watch for anti-forensic techniques (log deletion, timestomping, encryption and obfuscation, living off the land).

- Use counter-strategies, including log manipulation detection, alternative timestamp sources, behavioral analysis, and command-line argument review.
- Apply cloud-specific scoping tools and techniques for cloud and hybrid environments, including cloud provider audit logs and container runtime security.
- Scope cloud environments quickly. Ephemeral resources can deallocate and take evidence with them if scoping is delayed.
- Manage scale and complexity through prioritization and automation.
- Document false positive sources for future reference.

Step 7. Prepare Scoping Results for Containment, Eradication, and Recovery

Hand off the scoped system list, the canonical IOC inventory (Step 1), and the attack-progression timeline (Step 4) so each downstream activity can build on settled artifacts rather than re-derive them.