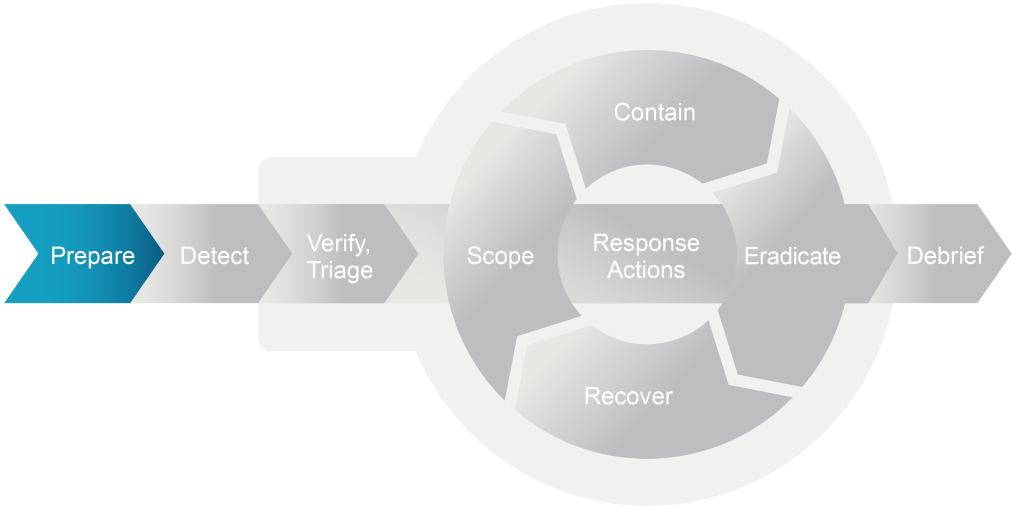
# Prepare: Step-by-Step




The following steps provide a condensed reference for preparation activities. Each step corresponds to topics covered in the Prepare Activity chapter of *Dynamic Incident Response* (www.dynamicincidentresponse.com), organized for use when building organizational readiness, training the incident response team, and strengthening proactive defenses.

## Step 1. Prepare the Organization

1. Develop organizational policies that outline the organization's approach to incident response, including:
    - Company mission and goals for the incident response program.
    - Priorities for the organization before, during, and following an incident.
    - Policy on involving management teams in the organization, including GRC, legal, and public relations.
    - Policy on paying ransom or extortion.
    - Policy on communicating with attackers.
    - Policy on data retention and evidence preservation.
    - Policy on reporting incidents to law enforcement, government, or industry partners.
    - Policy on public disclosure of incidents.
    - Policy on engaging with third-party incident response providers.
    - Containment authorization policies defining who can authorize systems to be taken offline, including tiered authorization levels (SOC/IRT-authorized actions like endpoint isolation, service owner-authorized actions like server or service isolation, executive-authorized actions like shutting down production systems or actions affecting regulated services).
    - Recovery time objectives (RTO) and recovery point objectives (RPO) for critical systems.
    - Evidence retention requirements and chain of custody procedures.
2. Develop management support for incident handling capability, including:
    - Establish relationships with decision-makers before incidents occur.
    - Communicate the value of incident response using industry examples and metrics.
    - Seek management input on policy development.
    - Define communication expectations during incidents.

    - Assign management actionable responsibilities, such as participating in tabletop exercises or breach simulations.
3. Identify critical assets and risk assessment processes, including:
    - Identify systems and services essential to the organization's survival, including revenue-generating operations, customer-facing services, and regulatory compliance systems.
    - Define risk tolerance thresholds for low, medium, high, and critical events.
    - Develop incident classification criteria based on impact factors (systems affected, data sensitivity, business impact, regulatory implications).
    - Document classification matrix for rapid reference during incidents.
    - Review and update criteria annually as the risk landscape evolves.
4. Develop an incident communications plan that addresses channels, contacts, reporting, and emergency messaging, including:
    - Establish communication channels that are secure and reliable:
        - Select a primary communication platform with appropriate security controls.
        - Identify a backup communication channel for use if the primary channel is compromised.
        - Test the communication channels periodically.
        - Document platform access procedures.
    - Document contact information for the team and important stakeholders:
        - Internal contacts (IRT members, IT operations, legal, HR, executives).
        - External contacts (law enforcement, regulators, insurance, retainer providers).
        - Vendor and cloud provider security contacts.
        - Establish a quarterly review process to maintain accuracy.
    - Establish reporting procedures:
        - Define reporting requirements by incident severity.
        - Create report templates for different audiences.
        - Establish service level agreements for initial and ongoing reports.
        - Document distribution lists for each report type.
    - Develop an emergency communication plan:
        - Define notification triggers for different incident types.
        - Establish approval workflows for internal and external communications.
        - Create message templates for common scenarios.
        - Identify constituent audiences (customers, partners, regulators, employees).
        - Establish distribution channels for each audience.
        - Designate and train spokespersons.
        - Document applicable regulatory notification requirements (including GDPR, HIPAA, SEC, PCI DSS, NIS2, DORA, and applicable breach notification laws).
    - Establish external reporting channels for security researchers:
        - Publish a security.txt file (RFC 9116) with contact, encryption, and disclosure policy information.
        - Document internal routing so external security disclosures reach the security team promptly.
5. Establish the incident response team, including:
    - Define team structure and roles (lead, analysts, communications, liaison).
    - Identify primary and backup personnel for each role.
    - Document escalation paths and decision authority.
    - Establish team activation procedures.
6. Identify a platform for incident tracking, including:

- Select a platform appropriate to organization size and needs.
- Configure incident categorization and prioritization.
- Establish access controls and retention policies.
- Train team members on use of the platform.

7. Account for cyber insurance requirements, including:
   - Obtain and review the cyber insurance policy with the IR team.
   - Identify notification timelines, pre-approval requirements, and vendor restrictions.
   - Negotiate to add preferred IR firms to the carrier's approved vendor panel.
   - Include the policy owner on the IRT contact list and in tabletop exercises.
   - Maintain offline access to the policy, carrier contacts, claims phone number, policy number, and procedures for engaging the carrier's approved incident response providers.
   - Protect the policy from disclosure on attacker-accessible systems and during ransom negotiations.
   - Identify independent legal counsel separate from the carrier's breach coach.
8. Implement security awareness training, including:
   - Develop training content covering incident recognition and reporting.
   - Establish training frequency and completion tracking.
   - Implement practical exercises (simulated phishing).
   - Create clear reporting channels for suspicious activity.

## Step 2. Prepare the Incident Response Team

1. Train the incident response team, including:
   - Technical skills (SOAR, digital forensics, network analysis, malware analysis, log analysis, scripting, and automation).
   - Soft skills (communication, documentation, decision-making under pressure, leadership, and negotiation).
   - Incident response procedures and playbook execution.
   - Company policies and escalation procedures.
   - Schedule ongoing training to maintain and develop skills.
2. Develop and validate system backup and recovery procedures, including:
   - Document current backup architecture and coverage.
   - Verify backup protection against ransomware (immutable, air-gapped, separate authentication).
   - Implement backup integrity monitoring and failure notifications.
   - Test restoration procedures and measure against RTO/RPO targets.
   - Document backup access procedures for incident response.
3. Cultivate relationships with essential personnel, including:
   - Identify contacts in IT operations, SOC, help desk, legal, HR, public relations, and business units.
   - Consider developing a RACI matrix to clarify roles during incident response.
   - Include essential contacts in exercises and preparation activities.
   - Establish communication preferences and escalation procedures.
   - Build relationships through regular interaction.
4. Develop playbooks for common incidents, including:
   - Identify incident types most likely to affect the organization.
   - Create detailed, actionable procedures for each type.
   - Include decision points, tool references, and communication triggers.

- Review and update playbooks after each exercise or incident in which they were used.

5. Prepare resources for response actions, including:
   - Configure forensic workstations with the necessary tools, including cloud-based workstations for organizations with significant cloud infrastructure.
   - Acquire and test evidence collection tools.
   - Establish secure evidence storage with appropriate capacity.
   - Prepare a jump bag for on-site response.
6. Prepare access to systems, including:
   - Establish break-glass accounts secured with hardware tokens or a credential vault, with alerting on use and periodic testing.
   - Document access request procedures for incident response.
   - Pre-authorize access where possible to reduce response delays.
   - Document vendor and cloud provider support procedures.
7. Conduct tabletop exercises and incident response drills, including:
   - Schedule regular exercises (monthly tabletop discussions, quarterly technical drills, annual full-scale exercises that combine tabletop discussion with technical execution).
   - Develop realistic scenarios based on relevant threats.
   - Include participants from all departments involved in the response.
   - Test authorization levels and containment decisions in addition to technical procedures.
   - Rotate team members through different roles to build depth.
   - Document findings and track improvement implementation.
8. Maintain preparation documentation on a regular review cycle, including:
   - Review contact lists quarterly with verification of current information.
   - Exercise each playbook at least once per year and conduct a separate review on an offset schedule.
   - Review policy documents annually aligned with broader governance cycles.
   - Develop an annual exercise plan that maps each playbook to a scheduled exercise date.
   - Assign specific individuals responsible for keeping documents current and include document review in their performance expectations.

## Step 3. Proactive Prevention and Detection

1. Implement Cyber Threat Intelligence (CTI) capabilities, including:
   - Identify appropriate intelligence sources (commercial, ISAC, government, OSINT).
   - Establish processes to review and operationalize intelligence.
   - Integrate IOCs into detection systems using standardized formats (STIX 2.1).
   - Use intelligence to prioritize defenses and inform response.
   - Evaluate CTI platforms to centralize intelligence management, correlate indicators across sources, and support investigation pivots during active incidents.
2. Develop processes for software management, including:
   - Implement risk-based patch management with defined timelines.
   - Maintain configuration management with version control.
   - Track software inventory including version information.
   - Maintain Software Bill of Materials (SBOM) data to identify systems affected by vulnerabilities in third-party components.
   - Discover and document shadow IT through billing and expense report reviews.

    - Track end-of-life software and establish migration or compensating control plans.
    - Establish exception handling for systems that cannot be patched.
3. Apply system hardening processes, including:
    - Disable unnecessary services and remove default accounts and credentials.
    - Adopt security benchmarks (CIS, DISA STIGs) appropriate to environment.
    - Deploy endpoint controls and forward logging data to a central collection point.
    - Implement application allowlisting where feasible.
    - Automate hardening through infrastructure-as-code or scripting where possible.
    - Regularly review and update hardening baselines.
    - Monitor for configuration drift from hardened baselines as an indicator of unauthorized changes.
    - Document exceptions with compensating controls.
4. Implement endpoint security monitoring, including:
    - Deploy EDR across servers, workstations, and cloud instances.
    - Configure appropriate detection rules and tune for the environment.
    - Establish alert review and investigation processes.
    - Enable response capabilities (isolation, evidence collection).
5. Deploy enhanced endpoint telemetry where EDR coverage has gaps, including:
    - Deploy a supplemental telemetry agent across endpoints lacking sufficient native or EDR-provided event detail.
    - Adopt a community-maintained configuration as a baseline and tune for the environment.
    - Forward telemetry events to a central collection point for correlation and retention.
    - Validate telemetry capture using adversary simulation tests.
6. Implement network security monitoring, including:
    - Deploy monitoring at critical network points (egress, segment boundaries).
    - Configure appropriate detection rules for network threats.
    - Ensure visibility into both north-south and east-west traffic.
    - Establish alert review and investigation processes.
7. Invest in detection engineering, including:
    - Develop detection rules tied to specific attacker techniques, mapped to MITRE ATT&CK.
    - Test and validate detection rules using adversary simulation tools.
    - Tune rules to reduce false positives based on the organization's environment.
    - Track detection coverage against the ATT&CK matrix to identify gaps.
    - Maintain detection rule lifecycle: retire outdated rules, update for environment changes, and document rule intent and logic.
8. Establish a threat hunting program, including:
    - Maintain a catalog of hunt hypotheses tied to MITRE ATT&CK tactics and techniques.
    - Identify target data sources for each hypothesis (proxy, DNS, process creation, authentication).
    - Define cadence for each hypothesis based on risk priority and data freshness.
    - Track hypothesis, data source, cadence, last-run date, threat hunting analyst, and findings in an audit table.
    - Promote hunt findings into automated detection rules to feed the detection engineering program.
9. Catalog critical data, systems, and infrastructure, including:
    - Maintain an accurate inventory of hardware, software, data assets, cloud resources, and third-party connections.
    - Identify and document critical assets essential to organizational survival.

    - Classify assets by business criticality.
    - Document network architecture and dependencies.
    - Maintain both local offline copies and access to authoritative sources maintained by owning teams.
    - Implement processes to maintain inventory accuracy.
10. Monitor the attack surface, including:
    - Continuously discover and evaluate externally visible assets (internet-facing services, cloud resources, domains, certificates, exposed APIs).
    - Compare discovered assets against the internal asset inventory to identify gaps.
    - Feed ASM findings into hardening and vulnerability management processes.
    - Evaluate ASM tools appropriate to the organization's size and external footprint.
11. Assess security posture through adversary simulation, including:
    - Schedule regular vulnerability scanning and configuration assessment against security benchmarks.
    - Conduct periodic penetration testing and application security testing.
    - Use adversary simulation and purple teaming to validate detection coverage against known attack techniques (e.g., MITRE ATT&CK, Atomic Red Team).
    - Prioritize remediation using CVSS severity alongside EPSS exploitation probability, asset criticality, exposure, and threat intelligence about active exploitation.
    - Evaluate Breach and Attack Simulation (BAS) platforms for continuous, automated validation of detection capabilities between manual assessments.
    - Track remediation progress and escalate persistent vulnerabilities that exceed acceptable risk thresholds.
12. Collect and retain logging information, including:
    - Identify critical log sources and ensure they are collected.
    - Configure systems to capture security-relevant events.
    - Define retention periods based on investigation and compliance needs, distinguishing between logs retained for active detection and those retained for compliance.
    - Store compliance-only logs in lower-cost archives and reserve SIEM capacity for sources with active detection use cases.
    - Periodically review and remove SIEM log sources that have no associated detection or investigation use cases.
    - Protect logs from tampering and implement a central collection point.