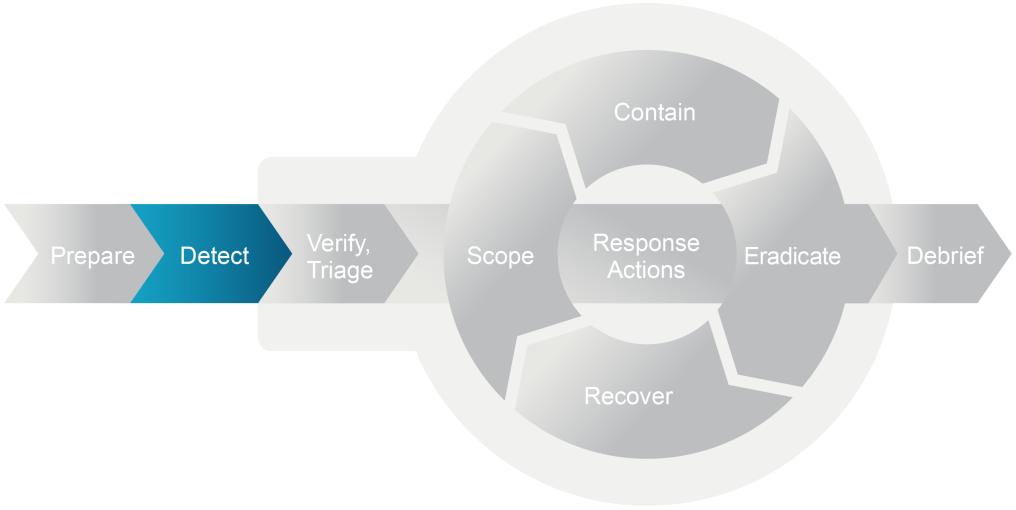
Detect: Step-by-Step



The following steps provide a condensed reference for detection activities. Each step corresponds to topics covered in the Detect Activity chapter of *Dynamic Incident Response* (www.dynamicincidentresponse.com), organized for use when establishing detection sources, hunting for threats, and refining detection capabilities.

Step 1. Select and Combine Detection Methodologies

Representative activities include:

- Use signature-based detection for efficient, high-confidence identification of known threats.
- Apply behavioral detection to identify threats that evade signatures, including mass file encryption, unusual access patterns, living-off-the-land techniques, and insider misuse.
- Scope behavioral baselines to business units or functional groups so meaningful anomalies stand out from normal activity.
- Layer ML-based detection for scoring and correlation at scale, using human-in-the-loop workflows to preserve analyst judgment on final classification.
- Map detection logic to MITRE ATT&CK techniques rather than specific indicators so rules remain effective as attackers modify tools.

Step 2. Operate Detection Data Sources

Representative activities include:

- Review EDR telemetry for process injection, credential dumping, persistence, and suspicious parent-child process chains.
- Analyze network monitoring data for C2 beaconing, lateral movement, and anomalous data volumes.
- Query SIEM platforms for attack patterns spanning multiple log sources.
- Apply SOAR automation to respond to high-confidence alerts.
- Monitor log source health to confirm critical feeds are delivering data as expected.

Step 3. Adapt Detection to Cloud-Native Environments

Representative activities include:

- Query cloud provider flow logs, control plane events, and Kubernetes audit logs for suspicious activity.
- Use eBPF kernel monitoring and container runtime socket telemetry to identify suspicious container activity.
- Use service mesh telemetry for east-west traffic visibility between services.
- For serverless and microservices workloads, collect function telemetry and watch for abnormal invocation patterns, unexpected outbound connections, unusual access to secrets or environment variables, and deviations from baseline execution characteristics.
- Unify telemetry across on-premises, hybrid, and multi-cloud environments to enable cross-environment correlation.

Step 4. Implement Data Reduction and Prioritization Strategies

Representative activities include:

- Apply detection-driven collection: define detection use cases first, then identify required data sources.
- Filter high-volume, low-value logs at the source before SIEM ingestion.
- Implement tiered data retention with hot, warm, and cold storage to balance accessibility and cost.
- Dispose of data that no longer supports a detection or forensic use case rather than degrading quality through aggregation or sampling.
- Correlate multiple low-confidence signals into high-confidence alerts.
- Apply statistical analysis to identify anomalous patterns such as periodic beaconing.

Step 5. Conduct Active Threat Hunting

Threat hunting in detect runs as a standing program, distinct from the IOC-driven enterprise sweep that scope runs during a verified incident.

Representative activities include:

- Operate threat hunting as a documented program with rotating hypotheses, tracked cadence, and auditable last-run dates.
- Prioritize hunting for TTPs and behavioral indicators over low-level indicators like hashes or IP addresses (Pyramid of Pain).
- Search for beaconing patterns, lateral movement, data staging, and living-off-the-land techniques.
- Run standing IOC sweeps against current and recent telemetry using IOCs from threat intelligence feeds. Incident-specific IOC sweeps belong to the scope activity once an incident is verified.

- Analyze encrypted traffic metadata (TLS client fingerprints, connection patterns, certificate attributes).
- Deploy TLS inspection for internal systems where policy permits to provide richer visibility for hunting and investigation.
- Document findings and new IOCs discovered during hunting.

Step 6. Monitor Passive Detection Sources

Representative activities include:

- Review automated alerts from security tools.
- Monitor employee reports of suspicious activity.
- Acknowledge employee reports promptly and supportively, even for false alarms, to sustain reporting culture.
- Track observations from system administrators and help desk personnel during routine operations.
- Validate third-party notifications using multiple factors (infrastructure legitimacy, IOC cross-reference, report quality) rather than source reputation alone.

Step 7. Respond to Detection Events

Representative activities include:

- Apply a false-positive prefilter using the local knowledge base before escalating, ruling out alerts that match documented benign sources without sending them to verify and triage.
- Document the EOI for handoff with the alert source, observation timestamps, affected assets, and technical indicators collected during detection.
- Escalate the documented EOI to verify and triage. Verification of whether the incident is real, CTI enrichment, and the continue/stop/defer decision belong to that phase.
- For EOIs originating from external researchers, acknowledge the report and establish the channel for ongoing updates.

Step 8. Continuously Improve Detection Capabilities

This step captures phase-specific feedback only; broader organizational changes are handled in debrief Step 8.

Representative activities include:

- Track detection metrics (MTTD, alert volume, false positive rate).
- Conduct purple-team exercises to test detection coverage against adversary evasion techniques.
- Update detection rules based on new threats and TTPs.
- Address detection gaps identified during incident response.
- Monitor for log tampering, disabled audit policies, and gaps in log data as indicators of adversary evasion.
- Retrain and recalibrate ML-based detection models to address model drift, validating training data for quality and avoiding contamination from mislabeled examples.
- Retain test environments for validating changes to detection logic before production deployment.
- Capture detection expertise in knowledge management systems for future reference.

- Review threat intelligence on attacker tooling and evasion methods.
- Surface staffing and sourcing decisions (analyst training investment, MSSP supplementation) to debrief Step 8 rather than acting on them within the detect activity.