Incident Response Playbook

When a security incident occurs, a structured response minimizes damage and recovery time. The incident response lifecycle — Preparation, Detection, Containment, Eradication, Recovery, Lessons Learned — provides a framework for handling any security event systematically.

Key Points

- ✓ Follow the IR lifecycle: Prepare, Detect, Contain, Eradicate, Recover, Review
- ✓ Containment is the priority — isolate affected systems to prevent lateral spread
- ✓ Preserve evidence before remediation — image affected systems if possible
- ✓ Communicate through established channels — avoid alerting the attacker
- ✓ Document every action taken with timestamps for post-incident review
- ✓ Escalate based on severity: P1 (critical) requires immediate executive notification
- ✓ Post-incident review is mandatory — learn from every incident to improve defenses

Action Items

1. Locate and review your organization's incident response plan
2. Know your role in the IR plan and the escalation chain
3. Ensure you have offline contact information for key IR team members
4. Participate in tabletop exercises when offered
5. Keep a USB with essential IR tools readily accessible

Quick Reference

Severity Levels:
P1 Critical — Active breach, data exfiltration, ransomware (respond within 15 min)
P2 High — Confirmed malware, compromised account (respond within 1 hour)
P3 Medium — Suspicious activity, policy violation (respond within 4 hours)
P4 Low — Informational, minor policy deviation (respond within 24 hours)