UptimeRobot

Incident Response Readiness Checklist

1. Preparation

- An Incident Response Team (IRT) is established with clearly defined roles and responsibilities
- Communication protocols and escalation procedures are documented
- Legal, compliance, and regulatory requirements (e.g., GDPR, HIPAA, PCI-DSS) are reviewed and incorporated
- Employees receive regular security awareness training and phishing simulations
- Cybersecurity tools (SIEM, EDR, IDS/IPS) are configured and monitored
- Incident response playbooks are developed for common attack scenarios (e.g., ransomware, DDoS, insider threats)
- Contact lists for internal teams, law enforcement, and external response partners are maintained and updated

2. Detection & Analysis

- Security monitoring tools detect and log potential threats in real-time
- An incident classification system is in place to categorize threats by severity
- Threat intelligence feeds are integrated to track emerging cyber threats
- Analysts follow a structured approach to investigating security alerts
- Logging and forensic tools are configured to collect relevant data for analysis
- Automated detection and alerting mechanisms are tested regularly for accuracy
- Indicators of compromise (IoCs) are updated and shared with relevant teams

3. Containment, Eradication & Recovery

- Predefined containment strategies (e.g., network segmentation, account lockdown) are documented
- Isolated backups are regularly tested for fast recovery in case of ransomware attacks
- Systems are patched and updated to remove vulnerabilities post-incident
- Recovery processes include data integrity checks and validation before restoration
- Business Continuity Plan (BCP) is aligned with incident recovery efforts
- Redundant infrastructure and failover mechanisms are in place for critical systems
- Multi-factor authentication (MFA) and access controls are reassessed post-incident

4. Post-Incident Activity

- Incident post-mortems are conducted to analyze root causes and improve future response efforts
- Lessons learned are used to update the IRP and security controls
- IRP is regularly tested through tabletop exercises and live simulations
- Incident response drills include key stakeholders beyond the IT team
- Reports are generated for executive teams, regulators, and key decision-makers
- Security policies and procedures are updated based on incident insights
- Continuous improvement processes are in place to refine detection and response capabilities