

# Security Incident Severity Matrix

## Severity Levels Overview

Incidents classified by severity to ensure appropriate response. Severity based on: Impact, scope, data sensitivity, business criticality.

P1 (Critical), P2 (High), P3 (Medium), P4 (Low). Severity determines response time and escalation.

### P1 - Critical Incidents

Definition: Severe impact to business operations or data. Active data breach or ransomware. Customer-facing systems down. Widespread system compromise.

Response Time: 15 minutes. Escalation: Immediate to incident commander and CISO. Notification: Executive team, legal, PR.

Examples: Active data exfiltration, ransomware encryption, complete system outage, confirmed APT.

### P2 - High Incidents

Definition: Significant impact to operations or data. Potential data breach. Important systems impaired. Multiple systems compromised.

Response Time: 1 hour. Escalation: Senior security analyst and manager. Notification: Department heads, IT leadership.

Examples: Malware infection, unauthorized access to sensitive data, DDoS attack, significant vulnerability exploitation.

### P3 - Medium Incidents

Definition: Moderate impact. Single system compromised. Minor data exposure. Degraded performance.

Response Time: 4 hours. Escalation: Security analyst. Notification: Affected department, IT team.

Examples: Phishing attempt, policy violation, minor malware, unsuccessful attack attempt, suspicious activity.

## P4 - Low Incidents

Definition: Minimal impact. Informational alerts. Potential security concerns. No immediate threat.

Response Time: Next business day. Escalation: None unless pattern emerges. Notification: Security team only.

Examples: Failed login attempts, low-risk vulnerability, security awareness issue, minor policy violation.

## Impact Assessment Factors

Confidentiality: Data exposure or theft. Integrity: Data modification or corruption. Availability: System or service disruption.

Scope: Number of systems, users, or customers affected. Duration: Length of impact or exposure.

Data Sensitivity: Classification level of affected data.

## Business Impact Criteria

Revenue impact: Lost sales, transaction processing disruption. Reputation: Customer trust, brand damage, media attention.

Regulatory: Compliance violations, reporting requirements. Legal: Potential lawsuits, contractual breaches.

Operational: Productivity loss, recovery costs.

## **Severity Escalation**

Incidents may be escalated to higher severity as investigation reveals greater impact.

Escalation triggers: Broader scope than initially assessed, sensitive data involved, prolonged duration, regulatory implications.

Document escalation rationale.

## **Severity Downgrade**

Incidents may be downgraded if impact less severe than initially assessed.

Downgrade only after thorough investigation confirms lower impact. Document downgrade justification.

Maintain audit trail of severity changes.

## **Response Time SLAs**

P1: Acknowledge 15 min, Initial assessment 30 min, Containment 2 hours.

P2: Acknowledge 1 hour, Initial assessment 2 hours, Containment 8 hours.

P3: Acknowledge 4 hours, Initial assessment 8 hours, Containment 24 hours.

P4: Acknowledge next business day, Assessment 3 days, Resolution 5 days.

## **Communication Requirements**

P1: Hourly updates to stakeholders. Status page updates. Executive briefings.

P2: Updates every 4 hours. Stakeholder notifications. Management briefings.

P3: Daily updates. Affected parties notified. Standard reporting.

P4: Update on resolution. Documented in ticket. Monthly summary reporting.

## **Severity-Based Resources**

P1: Full incident response team, external experts if needed, dedicated resources.

P2: Senior analysts, manager involvement, additional resources as needed.

P3: Assigned analyst, standard resources.

P4: Analyst as available, standard tools.

## **Post-Incident Review Requirements**

P1/P2: Mandatory post-incident review within 48 hours. Root cause analysis. Lessons learned. Action items.

P3: Review if recurring or significant learning opportunity.

P4: Documented in ticket, no formal review unless pattern identified.