**Incident Response Plan Structure for Catnip Games International**

1. **Introduction**

Purpose: As Catnip Games expands its multiplayer gaming infrastructure, ensuring security is critical to protect player data, maintain game availability, and prevent security breaches. This Incident Response Plan (IRP) provides a structured approach to identifying, managing, and mitigating security incidents, ensuring a quick and coordinated response while maintaining player trust.

**Objectives:**

* Detect and respond to security incidents with minimal impact on game services.
* Automate response workflows using Cortex and MISP.
* Centralize incident tracking and coordination with TheHive.
* Improve collaboration between SOC, development, and infrastructure teams.
* Ensure compliance with data protection regulations (GDPR).
* Align incident response lifecycle to structured playbooks for phishing, malware, and DDoS attacks.

1. **Scope and Applicability**

This plan applies to all Catnip Games systems, networks, and services, including:

* 300 Linux servers across two data centres.
* Sensitive services, including player data, matchmaking, game hosting, and APIs.
* Integration points with third-party services or platforms.

**Types of Incidents Covered:**

* DDoS attacks
* Bot exploits of game mechanics
* Unauthorized data access
* Account compromises
* Social engineering attacks
* Phishing and malware threats

1. **Incident Response Team (Roles and Responsibilities)**

|  |  |
| --- | --- |
| **Team/Role** | **Responsibilities** |
| SOC Analysts | Monitor alerts, perform initial triage, follow playbooks, escalate and initiate investigations |
| Incident Handler | Lead coordinated response, document in TheHive, ensure playbooks are followed |
| Threat Intelligence Team | Enrich alerts with MISP, analyse IOCs, update threat feeds |
| Development Team | Patch code, verify game logic, respond to source code threats |
| Infrastructure Team | Manage Linux security, implement mitigation during DDoS, recover systems |
| Management | Approve escalations, communicate externally, oversee compliance |

1. **Incident Response Lifecycle (Playbook-Based)**

4.1. Preparation

* Set up TheHive for incident case management.
* Configure MISP for threat intelligence sharing.
* Implement Cortex playbooks for automated response (e.g., lock accounts, isolate servers).
* Harden Linux infrastructure (MFA, disable password SSH, firewall).
* Set up Elasticsearch for alerting and log centralisation.
* Review all playbooks quarterly.

4.2. Detection and Analysis

* Alerts from Elasticsearch (login spikes, traffic anomalies) initiate playbooks.
* Use MISP to cross-reference known threats.
* Classify incidents by severity (see Section 5).
* Determine impact (data exposure, service disruption).

4.3. Containment, Eradication, and Recovery

* Execute relevant playbook:
  + **Phishing**: Secure source code, alert DPO, check database for export attempts
  + **Malware**: Isolate server, scan game code, verify matchmaking/game integrity
  + **DDoS**: Mitigate based on L7 or L3/4 pattern, scale or reroute traffic
* Reset affected credentials or lock accounts.
* Restore services, monitor for secondary attacks.

4.4. Post-Incident Activity

* Update MISP with IOCs from incidents.
* Document full lifecycle in TheHive.
* Correlate with beta testing issues if applicable.
* Debrief with development and SOC teams.
* Update playbooks if gaps are found.

1. **Incident Classification and Prioritization**

|  |  |  |  |
| --- | --- | --- | --- |
| Severity | Description | Response Time | Escalation Path |
| Critical | DDoS/malware affecting matchmaking or game data | Immediate | SOC → Management → Dev/Infra |
| High | Targeted phishing, API abuse | 1 hour | SOC → Threat Intel → Dev Team |
| Medium | Suspicious logins, unusual access | 4 hours | SOC → Infra Team |
| Low | Reconnaissance activity | 24 hours | SOC only |

1. **Response Playbooks Summary**

* **Phishing Attack**: If victim is a dev, secure code; if player, verify credentials, update security awareness.
* **Malware Attack**: Isolate affected system, scan for game logic exploitation, update MISP, and run Cortex analysis.
* **DDoS Attack**: Analyse traffic patterns, apply global/regional filtering, route traffic, and begin restoration.

1. **Communication and Escalation Procedures**

* Use Teams for internal coordination.
* Log all activity in TheHive.
* Notify stakeholders and players if needed.

1. **Reporting and Continuous Improvement**

* Use TheHive to automate incident documentation.
* Report weekly to management.
* Metrics: MTTD, MTTR, and mitigation success rate.
* Quarterly playbook reviews and tabletop drills.

1. **Prototype Implementation Steps**

* Deploy TheHive with RBAC.
* Integrate MISP feeds.
* Build and deploy Cortex playbooks.
* Centralise Elasticsearch logs and triggers.

**10.Training and Awareness**

* Train SOC and Dev teams using real scenarios.
* Distribute guides for each playbook.

**11.Legal and Compliance Considerations**

* Ensure all steps meet GDPR.
* Keep documentation audit-ready.