🛡️ Incident Response Plan (IRP): Crypto Ransomware Attack on Confidential Football Plays

---

📌 1. Incident Overview

- Incident Type: Crypto Ransomware Attack
- Target: Confidential football play files (critical intellectual property)
- Impact: Files encrypted, system locked
- Ransom Demand: $100 million in Bitcoin to an offshore Switzerland wallet
- Risk Level: Critical (Data loss, extortion, reputational threat)

🔍 2. Detection Method: SIEM-Based Threat Detection

Method: Security Information and Event Management (SIEM)

1. Log Collection – Aggregates system logs from endpoints, file servers, and user accounts.

2. Anomaly Detection – Identifies unusual encryption activity (e.g., rapid file renaming, file extensions like `.locked` or `.crypt`).

3. Correlation Rules – Flags:

    - Sudden access to the confidential playbook folder
    - Spikes in CPU/network activity
    - Unauthorized access from external IPs

4. Alert Trigger – Security alert issued for investigation based on file behavior and command-line activity.

🛑 3. Containment Strategy: Network Isolation & Host Quarantine

Immediate Steps

- Disconnect affected system from all networks (LAN, Wi-Fi, VPN).

- Disable compromised user account and revoke session tokens.
- Block outbound traffic to known ransomware IPs and C2 servers.
- Isolate infected machine in a quarantined VLAN or sandbox for forensic review.

Extended Containment

- Audit access logs for lateral movement to other systems or file shares.
- Suspend remote access for all non-essential users.
- Notify internal stakeholders, including IT, leadership, and legal teams.
- Preserve system image for forensic and legal purposes.

🧹 4. Eradication: Malware Removal & Vulnerability Patching

1. Identify Ransomware Strain

- Use tools like ID Ransomware or static analysis of ransom note.

- Sample identifiers: encryption extensions, note format, language, wallet address.

2. Remove Ransomware

- Use approved antivirus or EDR solution to isolate and remove executable.

- Search for persistence mechanisms (e.g., scheduled tasks, registry entries).

3. Patch Entry Point

- Patch vulnerabilities (RDP, unpatched software) used in the attack.

- Reset passwords for affected accounts and admins.

4. Threat Hunt

- Scan the environment for IoCs (Indicators of Compromise) and other infected nodes.

- Ensure no backdoors remain.

💾 5. Recovery: System Restoration & File Integrity Check

1. **Restore from Clean Backups**
    - Validate backup is pre-infection and offline.
    - Scan backup before restoring to production.
2. **Rebuild System**
    - Format infected system and reinstall OS from a trusted image.
    - Restore critical applications and securely transfer clean football play files.
3. **Monitor Post-Recovery**
    - 24–48 hour monitoring of restored systems for abnormal activity.
    - Run vulnerability scans and endpoint detection audits.
4. **Communicate**

- Notify affected stakeholders and, if necessary, law enforcement.
- Prepare public/internal statement, if breach details risk exposure.

🧠 6. Ransomware Identification: CryptoLocker Variant

- Name: Likely a CryptoLocker derivative or similar strain.
- Behavior: Encrypts local and network drive files using RSA-2048 or AES-256 encryption.
- Delivery Method: Phishing attachment or exploit via remote desktop protocol (RDP).
- Unique Indicators:
  - File extensions: `.footballplay.locked`
  - Ransom note titled: `READ_ME_NOW.txt`
  - Demands cryptocurrency payment and warns of public file leak.

- **Response Note: Do not pay the ransom unless legally advised and all options are exhausted.**

📓 7. Post-Incident Actions

- **Conduct full post-mortem within 7 days.**
- **Update incident documentation and threat detection rules.**
- **Provide training refreshers on phishing awareness.**
- **Improve backup rotation and testing.**
- **Share threat intelligence with trusted networks (ISAC, law enforcement, etc.).**