**Inspo:** [**https://www.hackthebox.com/blog/writing-incident-response-report-template#1\_executive\_summary**](https://www.hackthebox.com/blog/writing-incident-response-report-template#1_executive_summary)

**Executive Summary**

**Incident ID:**

**Severity:   
Status:   
  
Incident Overview: (describe time, place, what happened)**

**→ Affected systems**

**→Immediate Response and by which team members**

**Key Findings:  
  
Immediate Actions: (who is taking care of what)**

**Impact Overview:**

**→Clients:**

**→Organization Staff:   
→Partners:   
→Regulatory Bodies**

**→Internal Teams & Core Functionalities**

**→Services Disrupted**

**Technical Analysis**

**Affected Systems:   
  
→(distro) &**

**Evidence Sources & Analysis:  
  
(insert screenshots and captions, or detail the order of events)**

**Indicators of Compromise (IOCs):**

**→ IP & Hash**

**Root Cause Analysis:**

**(paragraph description of what enabled this to happen)**

**Timeline of Events:**

**→initial compromise**

**→C2 instances if any**

**→Exfiltration and data**

**→arbitrary code execution**

**→Lateral movement**

**→Malware deployment**

**→unauthorized access**

**→containment times**

**→Eradication times**

**→ Recovery times**

**How We Detected the Events:**

**Response & Recovery Analysis:**

**→ Immediate Actions**

**→ Revocation of Access**

**→ Containment Strategy**

**→ Short Term:**

**→ Long Term:**

**→ Eradication Measures**

**→ Post Incident Monitoring**

**→ Post Incident Actions**