IR Plan, Playbook, and Policy

By Derek Mayen

Introduction and Scope

The Purpose of this document is to:

- Take preventative actions against DoS or DDoS attacks
- List policies to enact for the CSIRT team to combat any sort of known DoS attack
- Enacting the playbook when needed to restore valuable assets such as Servers, Financial Data, etc.

Roles and Responsibilities

- Team Lead/ Manager: Responsible for overseeing the whole security operation and ensuring all assets amongst the company are maintained.

- SOC Analyst: Responsible for Security, setting sensors and thresholds,

- Incident Responder: Responsible for responding to possible threats.

- Log Analyst: Responsible for sifting through raw data to detect threats/ incidents

Incident Response Plan

1. Categorize Incidents : Categorize IoC's (Indicators of Compromise)

2. Identify the Threat : Identify that the company faces a Denial of Service attack (DoS)

3. Notify Proper Management : Notify management or even executives of the situation.

4. Enact Proper Mitigation Methods : Enact proper mitigation methods according to the playbook

Policies to Enact

1. Financial Information Policy
2. Incident Response Policy
3. Data Retention and Destruction Policy
4. Log Retention Policy
5. Captured User Data Policy
6. Unauthorized Access PII Policy
7. Traffic Light Protocol (TLP) Policy

Work Cited

Enaohwo, O. M. (2020, September 24). *How to write a policy. the only guide you need to read!*. SweetProcess. https://www.sweetprocess.com/how-to-write-a-policy/#:%7E:text=A%20policy%20is%20simply%20a,is%20your%20organization's%20action%20plan

A guide to digital forensics and cybersecurity tools. Forensics Colleges. (2022a, May 19). https://www.forensicscolleges.com/blog/resources/guide-digital-forensics-tools

Traffic light protocol (TLP) definitions and usage: CISA. Cybersecurity and Infrastructure Security Agency CISA. (2023, September 29). https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usage

DDoS: Incident response playbooks gallery. Incident Response Consortium. (n.d.). https://www.incidentresponse.org/playbooks/ddos