Playbook & Policies for Ubisoft

Introduction, Scope, and Overview

The purpose of this document is to effectively outline and implement the policies, to take preventative action against any Denial of Service (DoS) or Distributed Denial of Service(DDoS) attacks that could face the gaming company 'Ubisoft' and its assets. These policies will help the CSIRT team combat any sort of known DoS attack, and effectively implement the playbook to help restore services back to valuable assets such as the servers, financial data, etc.

Roles and Responsibilities

There are various needs for roles amongst all aspects of the company, especially for server maintenance and financial security. The individuals assigned to these roles are responsible for its security and maintenance. This will also be where we will activate 'Prepare' stages of the Denial of Service playbook which will be linked in the citation page at the end of this document. The prepare stage of the playbook outline that we must define the core teams that will handle each stage of the mitigation process, as well as who will be responsible for the monitoring of each aspect of security across different areas of the company.

- **Team Lead / Manager:**

The Team lead will be responsible for overseeing the whole security operation and ensure that the connection between all assets of the company are maintained. The Team lead will be in charge of ensuring all team members will be working as efficiently as possible to ensure that any analysis on the system will be properly investigated for any suspicious activity.

- **SOC Analyst**:

The SOC analysts will be in charge of security for all of the company's assets, such as setting up sensors for the server to provide log analysts with the data to review the logs of the server to see if there are any IoC's of a DoS attack. SOC analysts will also be providing security measures to the financial aspect and the logistics aspects of the company. Financial being the online stores customers use to digitally download video games, as well as shipment of physical games to third party vendors for physical distribution. As for the logistics side of things, ensuring that vendors for the third party companies are able to track their shipments of their required stock, and be able to submit request for restock, requires that the servers integrity be maintained,

- **Incident Responder**

The incident responder will be in charge of responding to possible threats and assessing the scope of threats to determine the best course of action to respond to the possible threat.

-**Log Analyst**

A log analyst will be in charge of sifting through the raw data and analyzing it to look for possible IoC's. After discovering any IoC, their job is to then escalate the situation to upper management to then have the appropriate course of action taken. This is especially important for a gaming company such as ubisoft as they have to maintain and monitor live server connections for longer periods of time as more people connect to their servers throughout the day.

Incident Response Plan for Ubisoft

1. Categorize any incident
2. Identify the threat
3. Notify the proper management
4. Enact the proper mitigation process
5. Post-Recovery

1. **Categorize any incident:** When an IoC is detected, it should be categorized in order of priority, and whether or not it will need to be escalated. Categorizing the incident will lead to identifying the possible threat easier, and allow communication to be more efficient between the necessary parties. This is where the Incident responder should look at the 'Detect' stage of the Denial of Service playbook. This is where the Incident responder will activate this stage of the playbook to help gather information to identify the possible threat. From capturing packet data information to conducting scans.
2. **Identify the threat:** After categorizing IoC's, they can be identified. For example, when there seems to be an overwhelming amount of traffic or an unusual amount of traffic that cannot be explained, this could be an indicator of an IoC. This is where the SOC analyst should look at the 'Analyze' stage of the Denial of Service playbook. After activating this stage of the playbook, the SOC analyst will be able to analyze the collected data and determine whether or not the threat can be solved amongst the security team, or to be escalated beyond to higher management to help determine mitigation methods that would bypass their security controls.
3. **Notify the proper management:** Communication between security teams is quintessential when trying to combat possible threats. Notifying proper management and escalating cases of possible IoC's will allow for the proper actions to be taken and a scope to be set to take action if this is indeed a threat to the company. This is where the SOC analyst and team lead should look at the 'Contain' and 'Eradicate' stages of the Denial of Service playbook. After activating this stage of the playbook, The SOC analyst and Team lead will then form plans of action to contain the compromised data. After containing the incident, the security team will then activate the 'Eradicate' stage in which they will confirm and report the incident, send communications of the incident through the proper channels, and begin basic mitigation processes.

4. **Enact the proper mitigation process:** After a threat has been escalated, and a scope has been set, it will then be time to enact the proper steps outlined in the playbook. This will allow the precautionary measures to be taken to avoid or prevent the attacks. This is where the SOC analyst should look at the ‘Recover’ and ‘Post-Incident Handling’ stages of the Denial of Service playbook. When the incident report has been closed, then the security team will activate the ‘Recover’ stage of the playbook in which they will update the holes in the system or network that need to be patched, I.e updating firewalls. After recovery, then the last stage to be activated is the ‘Post-Incident Handling’ stage. In this stage, the security team will then review the incident that occurred where discussions will take place about any updates to policy, preparation, and security measures.

Policies to Enact

1. **Financial Information Policy:** All financial information should be secured and only accessed by authorized personnel only. Keeping this financial information secure will prevent the company's financial information from being compromised by a threat. Financial information of a company should be retained for at least 6 years. According to the CRA (Canada Revenue Agency), Financial data of any company should be retained for at least 6 years. For security purposes, they should be stored on a separate server located inside the main office, in accordance with the CRA, only to be accessed through authorized personnel such as accountants, managers, and executives.
2. **Incident Response Policy:** When encountering an incident that could be an IoC,the incident response teams will enact the necessary protocols to prevent the IoC from becoming an attack. Analyzing all the possible IoC’s when monitoring the servers will provide a more secure environment and efficiency when it comes to responding to possible threats. Incidents and the actions taken against them, should be well documented for purposes of retaining what processes have been taken and who they have been approved by, for future use when updating security practices and policy changes.
3. **Data Retention & Destruction Policy:** Identifying systems that may have been compromised and systems that have not been affected. Isolating infected systems from healthy systems and securing network traffic to unaffected systems. Identifying the contents within the affected system, and developing an action plan to recover breached data. As outlined in the information policy, data retention should be kept for at least 6 years, but can be kept for as long as they are active. If a user account has been inactive for 6 months it will then be eligible for deactivation in which the user will be notified of its deactivation.

4. **Log Retention Policy:** Documenting internal and external authorized access to systems, this information may include time, personal identifiers (ie login information), devices used, operating systems, IP addresses, and location. Retaining these logs will help identify IoC's such as unauthorized users by cross referencing legitimate logs, with suspected fraudulent logs. Log data for Ubisoft should be retained for 6 months or more as there are millions of users connecting to ubisoft servers, this will allow for logs to be analyzed further back in case of an incident and for any other possible discoveries to be made.
5. **Captured User Data Policy:** In the event of unauthorized access to personal user information is captured or identified, escalate to upper management on next steps which may invoke the company playbook to mitigate the threat. This escalation may involve further escalation on the origins of the data breach. When encountering captured user data, ensure that users comply with all security methods of verification such as a Multi-Factor Authentication Method (MFA) of a security code, to establish a change in personal information to the user account. Any incident of compromised user data should be documented well in accordance with the 'incident response policy'.
6. **Unauthorized PII Access Policy:** Escalate to appropriate superiors as well as proper law enforcement for any case of PII (Personally Identifiable Information) breach. Frequent Data audits should be performed regularly to meet compliance with SOP.
7. **Traffic Light Protocol (TLP) Policy:** Identify TLP colour code to determine the level of discretion. Identify appropriate departments, individuals, and organizations who have authorization to potentially sensitive information. Once TLP code is identified, proceed with a direct need to know basis when handling information. Some information may be confidential or restricted.

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

Agency, C. R. (2023, July 28). *Government of Canada*. Canada.ca. https://www.canada.ca/en/revenue-agency/services/tax/businesses/topics/keeping-records/where-keep-your-records-long-request-permission-destroy-them-early.html

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

Suggested sops. OpenClinica Reference Guide. (2021, February 25). https://docs.openclinica.com/oc4/knowledge-articles/suggested-sops/#:~:text=The%20following%20list%20of%20Standard%20Operating%20Procedures%20%28SOPs%29,a%20recommended%20minimum%20set%20of%20data%20management%20procedures.