**Abstract**

This document is used to identify vulnerabilities that could affect the assets of LearnIt. Each vulnerability is assessed using the NIST cybersecurity framework’s five core functions. The five functions are Identify, Protect, Detect, Respond, and Recover.

Contents

[**Denial of Service or Distributed Denial of Service** 3](#_Toc100313220)

[**Document Control** 4](#_Toc100313221)

# **Denial of Service or Distributed Denial of Service**

**Identify**

Assets at risk:

* + Server hosting web application

Risk Assessment:

If a denial-of-service (DOS) or a distributed denial-of-service (DDOS) attack takes place, then the server hosting the web application can be taken down for a period. This could cause all services of LearnIt to be unavailable to users.

**Protect**

Access Control:

The server will be hosted by a dedicated provider and only authorized personnel will have access to the server. There is no way to protect access to the IP.

Awareness and Training:

Software development staff will be educated on what kind of requests to limit to avoid DOS or DDOS attacks.

Data Security:

Data is not at risk

Protective Technology:

Limiters can be used to stop requests coming from the client when a limit is reached.

**Detect**

Anomalies and Events:

A client sends an abnormal number of requests in a certain amount of time.

Security Monitoring / Detection:

* Log when a client sends an abnormal amount of request
* Monitor server traffic

**Respond / Recover**

Follow the plan outlined in LearnIt Security Response Plan.

Apologies for not adding more to this document. I ended up being very busy with other classes. I figured at least you can get the general idea of what the purpose of this document would be with the one example.

# **Document Control**

|  |  |
| --- | --- |
| Document Name: | Vulnerability Assessment |
| Current Version: 1 |  |
| Plan Owner: LearnIt |  |
| Plan Approver: Hunter Schattie |  |
| Date of Last Review: | 4/8/2022 |