

# CI/CD pipeline

**Owner:** Niki

**Reviewer:**

**Contributors:**

**Date Generated:** Sun Sep 15 2024

# Executive Summary

## High level system description

CI/CD pipeline for DevSecOps Labs

## Summary

Total Threats	5
Total Mitigated	0
Not Mitigated	5
Open / High Priority	0
Open / Medium Priority	5
Open / Low Priority	0
Open / Unknown Priority	0

New STRIDE diagram



# New STRIDE diagram

## Developer (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
1	Developer	Spoofing	Medium	Open		A developer commits secrets to version control either accidentally or on purpose. An angry employee with read access to the repository finds the secrets and proceeds to use them to steal end-user data.	Adhere to the principle of "Need to Know" and ensure that production secrets are not shared with individuals who don't have a need to know. Adhere to the principle of "Least Privilege" and ensure secrets and only have the permissions they need.
2	A developers laptop is lost or stolen	Spoofing	Medium	Open		A developers laptop is lost or stolen and the hard drive is not encrypted so an attacker is able to use a toll to bypass authentication and access all of the company code.	Ensure laptop is encrypted. Ensure developers only have access to what they need. Ensure zero trust policies.
3	New STRIDE threat	Spoofing	Medium	Open		A developer adds malicious code to a publicly available package in an unreviewed code check.	Ensure all code is reviewed by the development team and no code can be added without proper checks.
4	New STRIDE threat	Spoofing	Medium	Open		A developer says they are working from home but actually don't even use their computer.	Check the code base for activity, either pull or push. Require developers to log in and authenticate regularly to ensure active development. Randomly require token access to be regenerated.
5	Developer accidentally leaves access to company site via an open port.	Spoofing	Medium	Open		A developer opens a port on some software whilst debugging an issue and forgets to close it before release.	Check for open ports in a test of the software release.

## Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
--------	-------	------	----------	--------	-------	-------------	-------------

## Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
--------	-------	------	----------	--------	-------	-------------	-------------