Qualtrics ID	To be copied on ChatGPT-Threat description, assumptions, STRIDe threat type, and Affected components
STOLEN-AUTH-INFO	**Scenario:** updating a remote repository on GitHub **Threat description:** Spoofing a remote repo admin by stealing the authentication credentials via a social engineering attack **Assumptions**:The attacker carries out a successful social engineering attack (attackers communicate legitimately with others, manipulating and exploiting human qualities to achieve their attack) and gets authentication credentials. The credentials are valid. **STRIDE threat type**: Spoofing **Affected components:** The remote code repository
LEAKED-CONFIG-FILE	**Scenario:** updating a remote repository on GitHub **Threat description:** An attacker uses leaked (e.g. on Github) configuration file to interact with the remote repo, potentially jeopardize running code and submitting malicious code **Assumptions:** The attacker finds the leaked information, The attacker can (remotely) interact with the remote repository **STRIDE threat type:** Information disclosure **Affected components:** Victim's server
DOS-SERVER	**Scenario:** updating a remote repository on GitHub **Threat description:** An attacker submit malicious code can crash the server running the code, causing a Denial of Service (DoS) **Assumptions:** The attacker submits malicious code that can cause Denial of Service (DoS) to remote repo. The server has pulled and been running the code submitted by the attacker **STRIDE threat type:** Denial of Service **Affected components**: Victim's server
MALICIOUS-CODE-GITHUB	**Scenario:** updating a remote repository on GitHub **Threat description:** An attacker submit malicious code to the project on GitHub and get a shell of the server running the code **Assumptions:** The attacker can submit code to remote repo. The server has pulled and been running the malicious code submitted by the attacker **STRIDE threat type:** Elevation of privilege **Affected components:** Victim's server
ELEVATION-PRIVILEDGED-ACCESS	**Scenario:** updating a remote repository on GitHub **Threat description**: The attacker uses the malicious code to gain root access to the server **Assumptions:** The attacker can submit code to remote repo. The server has pulled and been running the code submitted by the attacker. Code run as root on the server **STRIDE threat type:** Elevation of privilege **Affected components:** Victim's server

DOS-REMOTE-REPO	**Scenario:** updating a remote repository on GitHub **Threat description:** The attacker submits the same fake push request to other remote code repositories, causing a Denial of Service attack **Assumptions**: Permission management is properly implemented in the remote (GitHub) provided repository hosting service to differentiate user access to the code repository. An attacker has the right to submit a bogus push request to a remote repository **STRIDE threat type:** Denial ofservice **Affected components:** Other remote code repositories
DISCLOSE-THIRD-PARTY	**Scenario:** updating a remote repository on GitHub **Threat description:** Not only can the attacker use these third-party services, but the attacker can also push code to the remote code repository where the yml file is located **Assumptions:** An attacker can browse the project's yml file. The developer has left the keys to the third-party services they need to use in the yml file that configures GitHub Actions **STRIDE threat type:** Information Disclosure **Affected components:** Third-party services, The remote code repository
ELEVATION-PRIVILEDGED-REPO	**Scenario:** updating a remote repository on GitHub **Threat description:** The attacker can launch a push request to a repository on GitHub and can delete the repository **Assumptions**: The attacker has gained push access to the code repository on GitHub **STRIDE threat type:** Elevation of privilege **Affected components:** The remote code repository
ELEVATION-PRIVILEDGED-CODE	**Scenario:** updating a remote repository on GitHub **Threat description:** An unauthenticated and non privileged attacker can still submit custom code into the remote repo to prepare the first step of another attack, e.g. turning off logging service or cause a Denial of Service **Assumptions:** The attacker can reach the remote repo (e.g. through internet) **STRIDE threat type:** Elevation of privilege and tampering **Affected components:** The remote code repository
EXPLOIT-HTTP-PROTOCOL	**Scenario:** updating a remote repository on GitHub **Threat description:** If an attacker compromises a http protocol on GitHub, the attacker can steal other users' identities by using HTTP by running a man in the middle attack **Assumptions:** GitHub uses the HTTPS protocol. The attacker has compromised the HTTP protocol on GitHub **STRIDE threat type:** Spoofing **Affected components:** GitHub eengine