OSS Cybersecurity Internal Team Working Agreement

Purpose

This document serves to outline the working guidelines and principles governing the OSS Cybersecurity Internal Support team to better foster collaboration and communication to achieve our primary objectives:

1. Maintaining the active security posture of Open-Source w/ SLU with documentation, auditing, and incident response
2. Provide cybersecurity training/education to our developers, contributors, and organization partners
3. Contribute to widely used Open-Source security tools to aid the wider Open-Source community

Team Members

Client: Daniel Shown (providing high level direction/communicating wants & needs)

Tech Lead: Samuel Kann (understanding and breaking down client requests into work for developers, leading developers and managing schedules)

Developers: Anne Henehan, Dennis Sheynkerman, Samuel Kann (implementing work and providing support to internal and external project)

Communication

Acceptable forms of communication for announcements, meeting schedules, and other non-confidential information include verbal communication, email, GitHub, and Slack channel #oss_cybersecurity. For handling confidential audits and vulnerability discussion, conversations must take place on the internal GitHub and internal #oss_cybersecurity_internal Slack channel. No confidential information shall be shared outside of these channels unless it's a secure, enclosed, isolated space. It is expected that response time for any vulnerability discussion is prompt, and all members of the team should respond to a notification of a vulnerability within 24 hours.

Work Process

Work over the course of the semester will loosely follow the cybersecurity roadmap outlined here: https://oss-slu.github.io/oss_cybersecurity/SOSS_Roadmap_Sp26.pdf. Work time frames will be enforced unless extreme extenuating circumstances. Deviations from the roadmap will be discussed

publicly for the sake of transparency for organizational partners.

To help facilitate collaboration while working, we will be meeting twice a week. The first meeting will be Mondays at 4:10PM in the Busch Student Center room 253 for our standard class meeting time, the other meeting time will be a short touch base meeting on Wednesdays at 11:00 AM to go over initial blockers for work. Should one member of the team be unable to convene for this meeting time, communication will be made in the Slack with as much forward notice as possible.

Documentation

Work toward the roadmap, including security documentation and SAML integration as well as any incident response and vulnerability analysis or any other work performed will be documented to the satisfaction of the client. Whether or not the documentation is disclosed publicly or privately will be the determination of the program director and the tech lead.

Policy

All members of the security team will abide by all University policies, and the organization's security policy for reporting, handling incidents, disclosure, and best practices. No member of the security team will engage in behavior that jeopardizes the security posture of Open Source w/ SLU or the broader university.

Modifications

A request to modify this document can be made at any point through any public communication channel, however any modification needs to be approved by all developers of the team. The client has ultimate final veto power and any changes to this document must be communicated to them no later than 24 hours after a change was agreed upon.

This document is valid until March 6, or at the completion of GitHub Issue 6, whichever is later. A review meeting will be conducted at that point to review the contents of the document and to ensure the expectations are being met.

Acknowledgement

By digitally signing this document, I acknowledge I will abide by the terms of this team agreement, and should the need arise to change this document I will work with the team to identify areas that need to be addressed and help in codifying a new policy to abide by.