Tissue Analytics Computer Security Incident Response Team (CSIRT) Charter and Incident Response Process

Author: Joshua Budman, CTO
Date Published: 5/31/17
Version: 1.0

Purpose

Tissue Analytics has developed the following document in order to serve as a charter for the Computer Security Incident Response Team (CSIRT). This document will discuss the criteria TA uses in order to select the CSIRT, as well as the practices they must follow in responding to various incidents. The overall goal of the CSIRT is to ensure a swift response to any incident jeopardizing TA's software components, hardware components and clients' data. It is also intended to ensure that the probability of a similar event occurring in the future is reduced.

CSIRT Team Selection

In order to be eligible for the CSIRT, individuals must be TA technical management personnel. Refer to the **Tissue Analytics Organizational Chart** for the various management roles in the company. Individuals on this team must have experience applying the incident response process, detailed in the **Incident Response Process,** and logging incidents using the **Incident Response Reporting Template.** The quantity of individuals nominated to respond to specific incidents is chosen based on the severity of the incident reported. Once the team has been selected, the incident response process can be initiated.

Incident Response Process

Once the CSIRT faction has been selected, the incident response process can be initiated. The first step of the incident response process is to identify the source component of the incident. The source components can be broken into the following:

1. Mobile
2. Server/Back-End Processes
3. Database
4. Web

Once the system component associated with the incident has been identified, the CSIRT will examine the nature of the incident/breach and log the incident using the **Incident Response Template.**

After the incident has been logged, the CSIRT is responsible for engaging the software development team and IT management. The CSIRT alerts the relevant personnel by issuing a ticket on Jira, the agile development planning tool TA uses. This Jira ticket will be issued in a board based on the system component identified as the source of the issue. It will be designated as the highest priority due to the fact that it is an incident and not a bug fix. There are a few scenarios of incidents that require distinct responses:

1. Suspected breach in one or more system components
2. Suspected vulnerability in one or more system components

3. Data loss or contamination in one or more system components

Incident response processes for each of these scenarios are explained in detail below.

Suspected Breach
If a breach is suspected, the CSIRT team is responsible for working with TA software developers and IT management to identify the client account(s) associated with this breach. First, TA software developers will shut down all software resources allocated to this account. This includes removal of access from all users associated with this account. TA will alert the client(s) affected by the breach within 24 hours of the breach's occurrence. All other customers will be notified of this breach within 30 days of the breach per HIPAA requirements.

Once the nature of the breach is identified, TA will initiate its **Secure Development Life Cycle Process** to address the breach at its source and fix it. All clients will be alerted once the SDLC for this breach has been completed and the issue has been resolved.

Suspected Vulnerability
If a vulnerability is suspected, the CSIRT is responsible for identifying the components associated with said vulnerability and logging a Jira ticket detailing this vulnerability. This incident must also be logged via the **Incident Response Template.** Based on the severity of the vulnerability, TA may choose to shutdown the system component and re-initiate the SDLC similar to the protocol for a suspected breach. The client will not necessarily be alerted of the vulnerability unless there is proof that it does result in a breach.

Data Loss or Contamination
In this case, the CSIRT is responsible for identifying the following information regarding the data: 1). The reason for the data loss/contamination, 2). The client(s) affected by this data contamination and 3). The nature of the data lost/contaminated. If the reason for the data issue is related to a suspected breach or suspected vulnerability, the relevant processes outlined above are pursued. If not, the reason for the data loss must be documented using the **Incident Response Template.** Next, a Jira ticket will be created based on the incident reported by the CSIRT and the SDLC will be initiated in order to repair the problem that caused the data issue. Possible mitigations for data loss/contamination include server hardening and audit log monitoring. Audit log monitoring is made possible as TA logs all database interactions. Once the issue is resolved, TA will report the issue and resolution to the client. This report should include all of the data recovered, repaired or restored and any data that could not be recovered, repaired or restored.

Revision History

Date of Change	Version Number	Responsible	Summary of Change