Non-compliant Servers and Applications — Non-compliant servers and applications are servers and applications with unpatched high severity operating system or application vulnerabilities detected more than 90 days prior to the report generation.

High-Severity Vulnerabilities — Operating System or Application Vulnerabilities classified as Level 4 or Level 5 Severity by the Campus Vulnerability Scanner "Qualys".

Operating System Vulnerabilities — Operating system vulnerabilities are found in operating system programs, which are delivered by the vendor (i.e. Microsoft, Red Hat Linux)

Application Vulnerabilities — Application vulnerabilities are found in programs added to the operating system, such as Adobe, Apache, etc.

Vulnerability Exceptions — Vulnerability exceptions are documented and/or mitigated systems which have been formally reviewed by campus administration. More work on this one.

Servers Without Exceptions — Servers without exceptions are non-compliant servers which have not been formally documented.

**Server Vulnerability Status**

Legend

Green — Servers free of high-severity Operating System or Application Vulnerabilities.

Yellow — Servers which contain Operating System or Application Vulnerabilities not exceeding 60 days from detection.

Pink — Servers which contain Operating System or Application Vulnerabilities which exceed 60 days from detection, and are at a higher risk of becoming non-compliant.

Red — Servers which contain Operating System or Application Vulnerabilities which exceed 90 days from detection, and become non-compliant.

High Severity (Urgent & Critical) Vulnerabilities — Intruders can easily gain control of the host, which can lead to the compromise of an entire network. These vulnerabilities may include full read and write access to files, remote execution of commands, and presence of backdoors.

**PCI Compliance**

<table>
<thead>
<tr>
<th>Area</th>
<th>Compliant</th>
<th>Non-compliant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Associated Students (AS)</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Research Foundation (RF)</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Stateside</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>University Foundation (UF)</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
**Web Application Vulnerability Status**

- Total Web Apps: 443
- Web Apps with High Severity Vulnerabilities: 8
- Web Apps with Exceptions: 4
- Web Apps without Exceptions: 4

**Compromised Accounts**

- Internally Notified: 35
- Externally Notified: 1

**Online Awareness Training**

- Total Enrolled (Month): 132
- Total Completed (Month): 127

**PS/SA Security**

- Accounts Created: 16
- Accounts Modified: 27
- Passwords Reset: 2

Note: Metrics are respective to account modifications made by SA Security, specific to the PeopleSoft Student Administration SA module.

**Accounts Created**— New accounts created for employees with authorized access within SA PeopleSoft module

**Accounts Modified**— Authorized role or permission list modifications made for users within SA PeopleSoft module

**Passwords Reset**—Manual account password resets performed