Project Title: Annual Security Inventory (ASI) Application

Submitted By
David Gracey
Deputy CIO, Enterprise Solutions - University of California, Riverside
david.gracey@ucr.edu
951-827-7367

Team Members
Sumita Roy-Chowdhury, Primary Application Developer
Brandon Ayers, Application Architect
Jeremy Fisher, Technical Infrastructure Lead

Project Summary
The Annual Security Inventory (ASI) application was developed to more effectively manage the inventory of sensitive information stored and processed on computer systems across campus. Documenting the institution’s electronic information resources allows the campus to identify areas of risk, determine where additional security measures are needed, and ensure compliance with University of California information security policies and standards.

Project Narrative
Prior to implementing the ASI application, campus IT departments were required to fill out standalone documents and send via email their security plans, system names, and IP addresses of systems containing sensitive data to the responsible administrative official and the central IT organization (Information Technology Solutions). The emails were then archived for later retrieval and review in the event an audit was needed, or a system was compromised. The goal of the Annual Security Inventory project was to improve the way this information is gathered, organized, stored, and retrieved.

The previous, email-based solution for managing the security inventory was fraught with issues. Some departments did a good job of reporting the sensitive information contained within their computer systems and the security controls in place. Others provided incomplete or inconsistent information at best. There was a desire to improve both the quality of the information being provided by individual campus IT organizations as well as central oversight to ensure complete and accurate inventories were being provided consistently across the institution.

A centralized database and corresponding web-based application was designed to capture the relevant information security details for each campus system including, but not limited to, the types of protected...
data contained therein (e.g. Social Security Number, Driver’s License Number, Credit Card Number), whether each data element is encrypted, whether physical and host-based security measures are in place, information about database and file system access controls, details about system backups and disaster recovery plans, and so on. Business rules were implemented within the application to avoid incomplete submissions. Logic was added to ensure all required questions are answered and valid values are selected for each data field. System roles and workflows were implemented to ensure the report for each system or environment is entered by the department, reviewed by the organization, routed to Information Technology Solutions for final review, and ultimately approved.

The ASI application had a positive impact on customers. The user experience features a simple and easy-to-navigate interface, stepping the user through the data collection process for each of their computer systems. For convenience, each year’s inventory is pre-populated based upon the reports submitted the previous year. This allows departments to focus on specifying what is new, what has changed, and what no longer exists rather than the busywork of re-entering a lot of the same or similar information year after year.

UCR’s Chief Information Security Officer indicates the ASI application is much easier and more convenient to use than completing the security inventory on email or paper. Historical data can be referenced to populate current year’s security inventory which accelerated completing the survey. The Information Security Office has the functionality to provide suggestions and remediation guidelines on completed assessments to assist clients with improving their security posture. The application has integrated routing from department to organization, to Information Security Office making it a more efficient workflow. Several UC campuses including Santa Barbara, Santa Cruz, and Berkeley have shown interest in using the ASI application considering there is an appreciation for the work to have the application be multitenant.

The success of the project is measured by the accuracy and completeness of the Annual Security Inventory. Reports were built within the system to reveal which reports have been submitted by which campus departments, and which reports are still pending. This allows the Information Security Office to engage with campus units as needed to ensure 100% compliance with reporting requirements including adherence to BFB-IS-3 University of California policy for electronic information security.

The ASI application has broken-down silos between campus IT organizations. There is now a free flow of information security data across the institution.

**Project Timeline**

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>September 2015</td>
<td>Planning and Design</td>
</tr>
<tr>
<td>October 2015</td>
<td>Development</td>
</tr>
<tr>
<td>November 2015</td>
<td>Testing and Deployment</td>
</tr>
<tr>
<td>July 2018</td>
<td>Update to support policy BFB-IS-3: Electronic Information Security</td>
</tr>
<tr>
<td>January 2019</td>
<td>Multi-Tenancy Architecture Review</td>
</tr>
<tr>
<td>August 2019</td>
<td>Application Hosting for Additional UC Campus Locations</td>
</tr>
</tbody>
</table>
Technology Highlights

- Architected to host multiple tenants.
- ASI uses Single Sign-on (CAS) for authentication and the campus Enterprise Access Control System (EACS) for authorization.
- ASI is built with GRAILS. The GRAILS (Groovy on Rails) programming language and technology stack. This high-productivity development framework enables UCR to build web applications like ASI in a very short timeframe.
- It is built for Mobile platforms. ASI implementation is developed with Responsive Web Design. Thus, it is mobile-friendly and optimized for various mobile devices (e.g., tablets, smartphones).
- Common Infrastructure. ASI leverages existing infrastructure (e.g., virtual machines, storage, and database) thereby allowing developers to focus on development and not on back-end configuration details.
- ASI takes advantage of a suite of application development tools that allows for rapid development.
  - The GRAILS (Groovy on Rails) programming language and technology stack
  - Development IDE supporting Java, and Model View Controller (MVC)
  - Common infrastructure (e.g., virtual machines, storage, and database)
  - Puppet to automatically provision Virtual Machines
  - Jenkins to create new builds
  - Rundeck for deployment
  - Apache Fuse Enterprise Service Bus (ESB) to provide web service integration for:
    - User authorization
    - Person information
    - Accountability structure (orgs and depts.)
  - Responsive design allowing the application to resize itself dynamically for optimal display regardless of device
- ASI leverages existing infrastructure (e.g., virtual machines, storage, and database) allowing developers to focus on development and not on backend configuration details
ASI Screen-Shots

Main Menu dynamically presents tiles corresponding to the user’s authorizations (the illustration below shows options for the application administrator):

Welcome, John

ITS Security Reviewer Options:

- View 2015 Inventory
- View Historical Info
- Admin Console

The application guides the user through the process of gathering required information for each system (page 1):
The application guides the user through the process of gathering required information for each system (page 2):
The application guides the user through the process of gathering required information for each system (page 3):

### General Environment Information

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Hostname</th>
<th>Machine Type</th>
<th>DNS Access</th>
<th>OS</th>
<th>Vendor</th>
<th>Patch</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.25.222</td>
<td>daylight</td>
<td>Virtual</td>
<td>2023-08-01 12:00</td>
<td>SUSE</td>
<td>IBM x3850 M4</td>
<td>1.5</td>
</tr>
<tr>
<td>192.168.25.225</td>
<td>daylight2</td>
<td>Virtual</td>
<td>2023-08-01 12:00</td>
<td>SUSE</td>
<td>IBM x3850 M4</td>
<td>1.5</td>
</tr>
<tr>
<td>192.168.25.226</td>
<td>daylight3</td>
<td>Virtual</td>
<td>2023-08-01 12:00</td>
<td>SUSE</td>
<td>IBM x3850 M4</td>
<td>1.5</td>
</tr>
<tr>
<td>192.168.25.227</td>
<td>daylight4</td>
<td>Virtual</td>
<td>2023-08-01 12:00</td>
<td>SUSE</td>
<td>IBM x3850 M4</td>
<td>1.5</td>
</tr>
<tr>
<td>192.168.25.228</td>
<td>daylight5</td>
<td>Virtual</td>
<td>2023-08-01 12:00</td>
<td>SUSE</td>
<td>IBM x3850 M4</td>
<td>1.5</td>
</tr>
</tbody>
</table>

Environment Inventory Notes:

### General Environment Administrator

Is the environment administrator a vendor? No

Contact Name: Lambert Teammme Contact Email: william@edu Contact Number: (805) 357-2019

### Environment System Administrator

Is the environment system administrator a vendor? No

Contact Name: Lambert Teammme Contact Email: william@edu Contact Number: (805) 357-2019

### Database/File System Information

The following section pertains to the database administration on the environment.

#### Storage Type Information

Please describe the underlying technology used to store and access protected data. Examples include: relational databases (e.g., Oracle, SQL Server, MySQL, PostgreSQL), Microsoft Access, custom applications/development mechanism, flat file database or network shares (e.g., Office documents on a central file share), Oracle databases and NFS mounts.

#### Database/File System Administration

Is the administration of the database, file system, or other storage mechanism described above provided by a vendor? No

Contact Name: C. G. Khaneil Contact Email: c.g.khanoeil@edu Contact Number: (860) 979-1203

#### Database/File Access Controls

How many people have access to database/files containing Person Protected Information (PPI), Medical information, or Sensitive Information within this environment? 5

Has the Data Steward authorized all of the people with such access? Yes

Do any of the people with access use a shared password? Yes

Are logs kept of all database/file accesses? No

Please describe the logging procedure and any authentication/authorization controls. Include log location, retention period, frequency of review and the contact information for the person responsible for the review. glsadm for Oracle database accesses. Local auditing, remote auditing is to central log server, OISDE IDES, and ELK analysis. OIS Security Team can provide further review relevant security data.
Overview of systems inventoried within a single IT organization for a specific year (with option to drill-down to view details for each system):

<table>
<thead>
<tr>
<th>#</th>
<th>Department</th>
<th>Environment</th>
<th>Test ID</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>001</td>
<td>Sun Control</td>
<td>US Change</td>
<td>01180021</td>
<td>Complete</td>
</tr>
<tr>
<td>002</td>
<td>Web Services</td>
<td>US Change</td>
<td>01180021</td>
<td>Complete</td>
</tr>
<tr>
<td>003</td>
<td>IT Services</td>
<td>US Change</td>
<td>01180021</td>
<td>Complete</td>
</tr>
<tr>
<td>004</td>
<td>Finance</td>
<td>US Change</td>
<td>01180021</td>
<td>Complete</td>
</tr>
<tr>
<td>005</td>
<td>Human Resources</td>
<td>US Change</td>
<td>01180021</td>
<td>Complete</td>
</tr>
<tr>
<td>006</td>
<td>Customer Service</td>
<td>US Change</td>
<td>01180021</td>
<td>Complete</td>
</tr>
<tr>
<td>007</td>
<td>Human Resources</td>
<td>US Change</td>
<td>01180021</td>
<td>Complete</td>
</tr>
<tr>
<td>008</td>
<td>Customer Service</td>
<td>US Change</td>
<td>01180021</td>
<td>Complete</td>
</tr>
</tbody>
</table>