MICHIGAN STATE
U N I V E R S I T Y

Project Plan
Cybersecurity Management System

The Capstone Experience

Team Aptiv

Ashtaan Rapanos
Clayton Peters
Dillon Brown
Wei Jiang
Winton Qian

Department of Computer Science and Engineering
Michigan State University

Spring 2018

From Students…
*…to Professionals*

Functional Specifications

- Application to help with automation of Aptiv's cybersecurity processes
  - TARA, Vulnerability/Penetration Assessments, Mitigation Remediation, Incident Response
- 4 Trackers for analysis and visualization of information collected by system
  - Threat/Risks, Vulnerabilities, Incidents, Mitigations
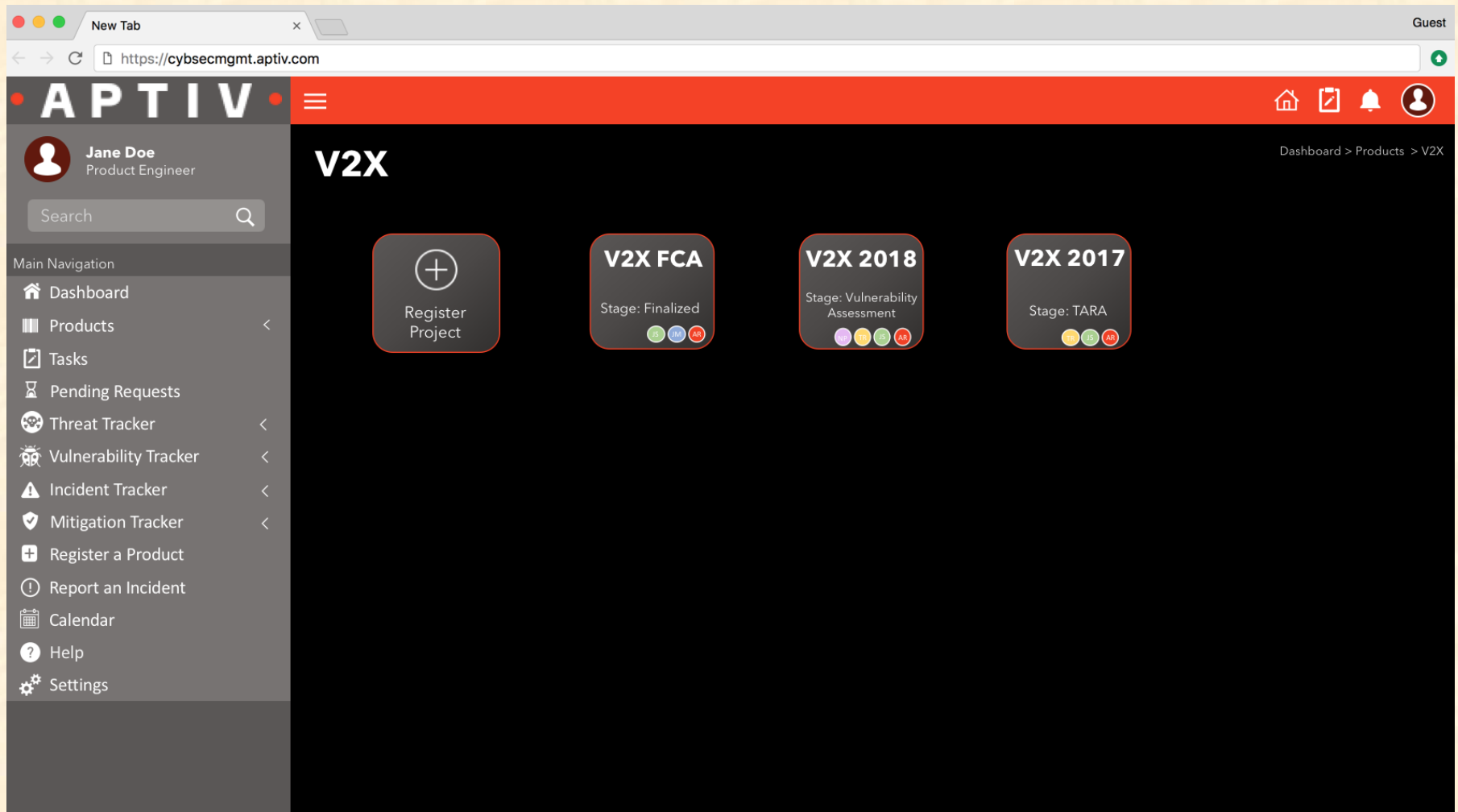- Task management

Design Specifications

- ASP.NET (C#) Web Application
- Simple interface for all users
  - Dashboard
  - Project Pages
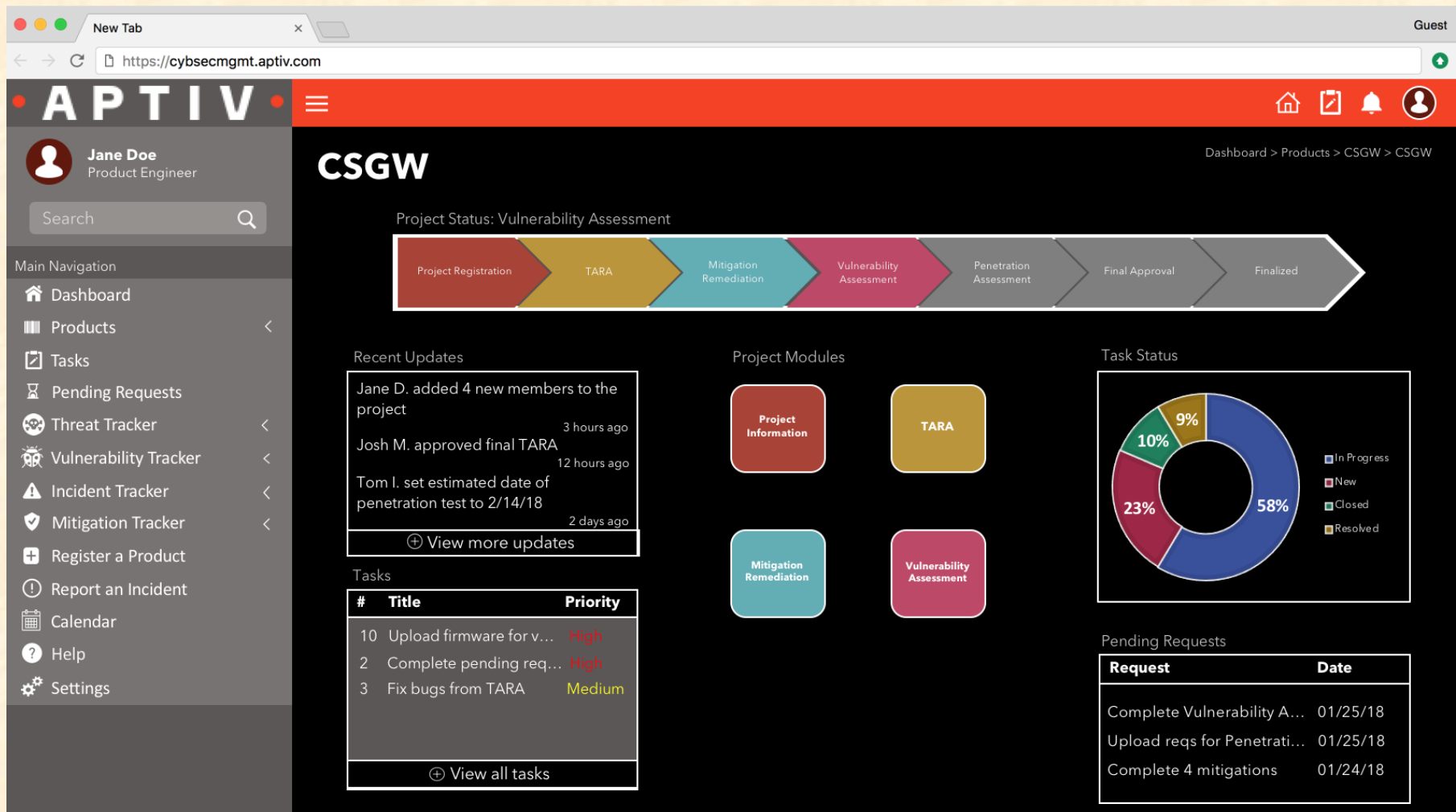 - Cybersecurity Process Modules
  - Data Trackers
  - Task Manager

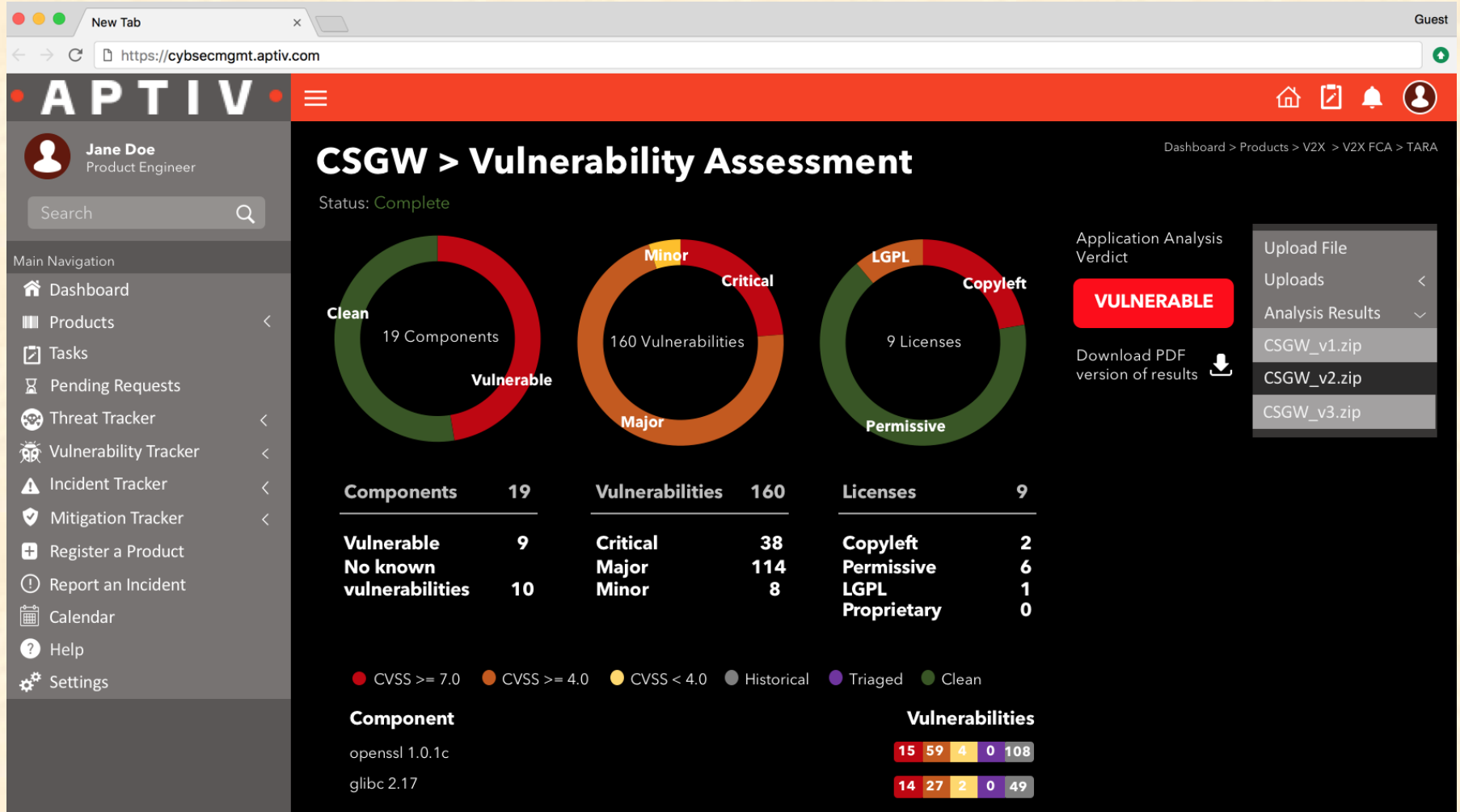# Screen Mockup: Product Dashboard
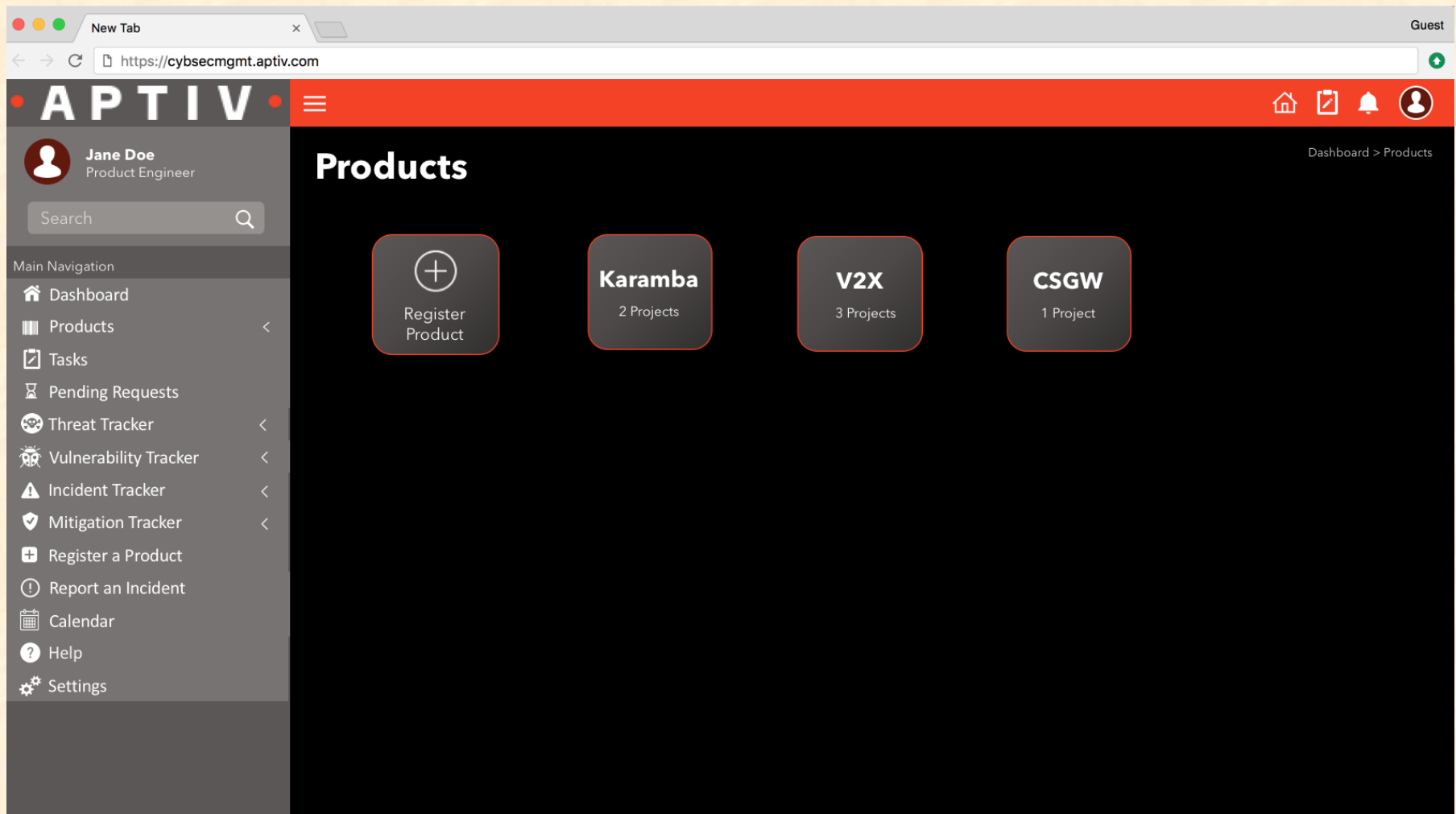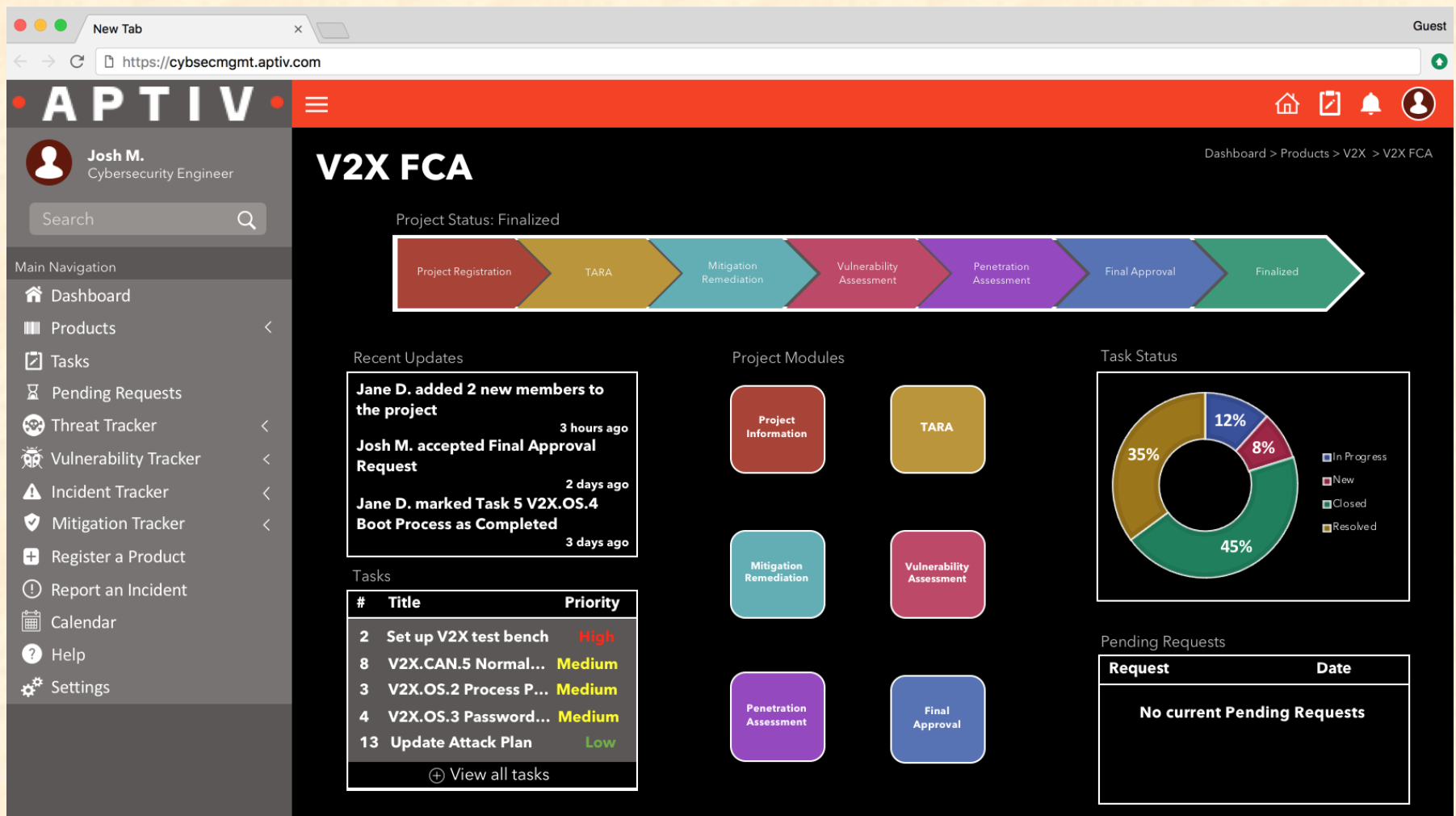
Screen Mockup: Project Dashboard
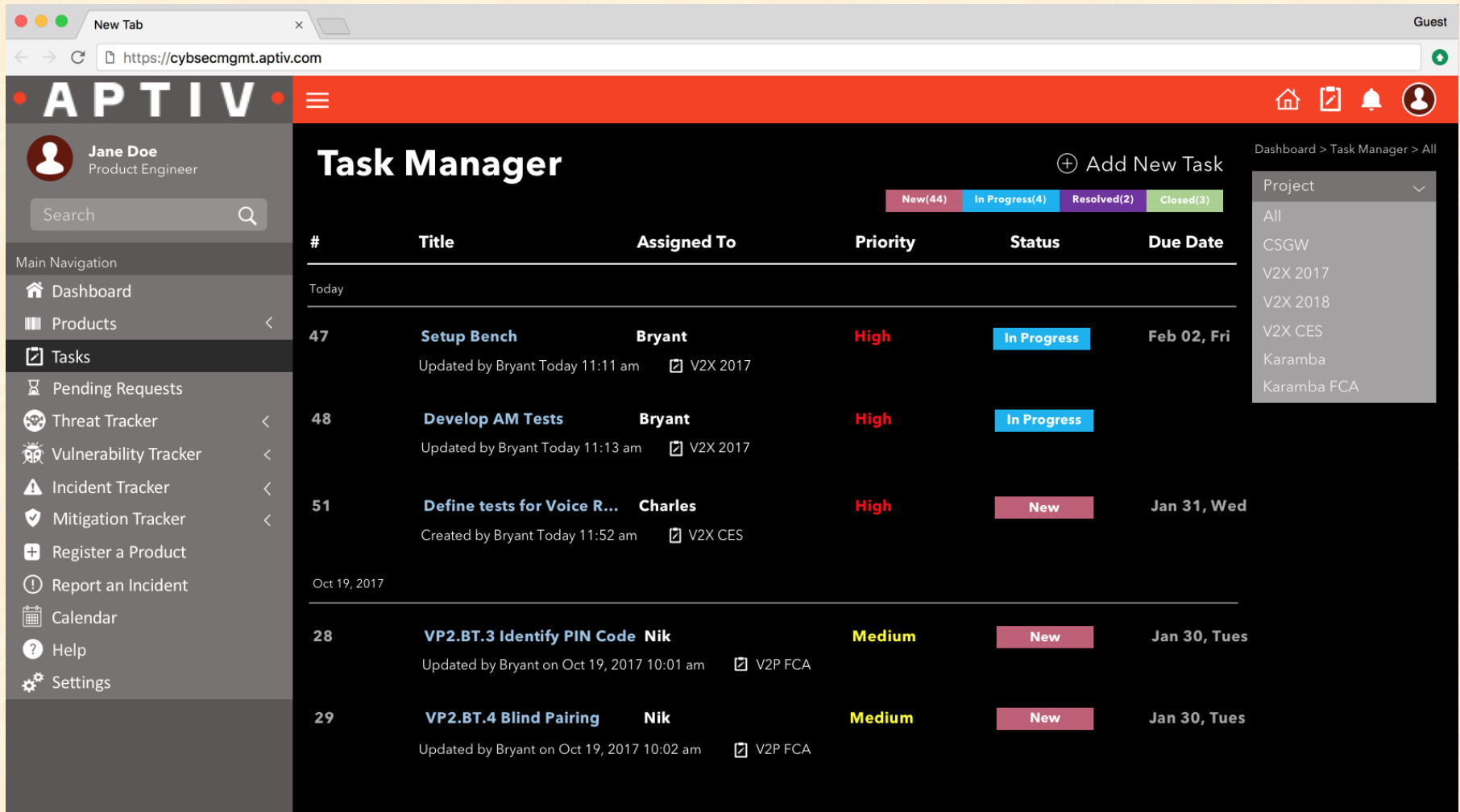
Screen Mockup: Incomplete Project Page

Screen Mockup: Vulnerability Assessment Module

Screen Mockup: Completed Project Page

Screen Mockup: Task Manager

Screen Mockup: Incident Tracker

Technical Specifications

- Microsoft Active Directory
  - User authentication to define role in system
- Microsoft Azure
  - Hosting SQL database and web application
- Many-to-many Database
  - Stores all cybersecurity data input into system
  - Used for tracker visuals and analysis
- Protecode API
  - Detect vulnerabilities in source code

System Architecture
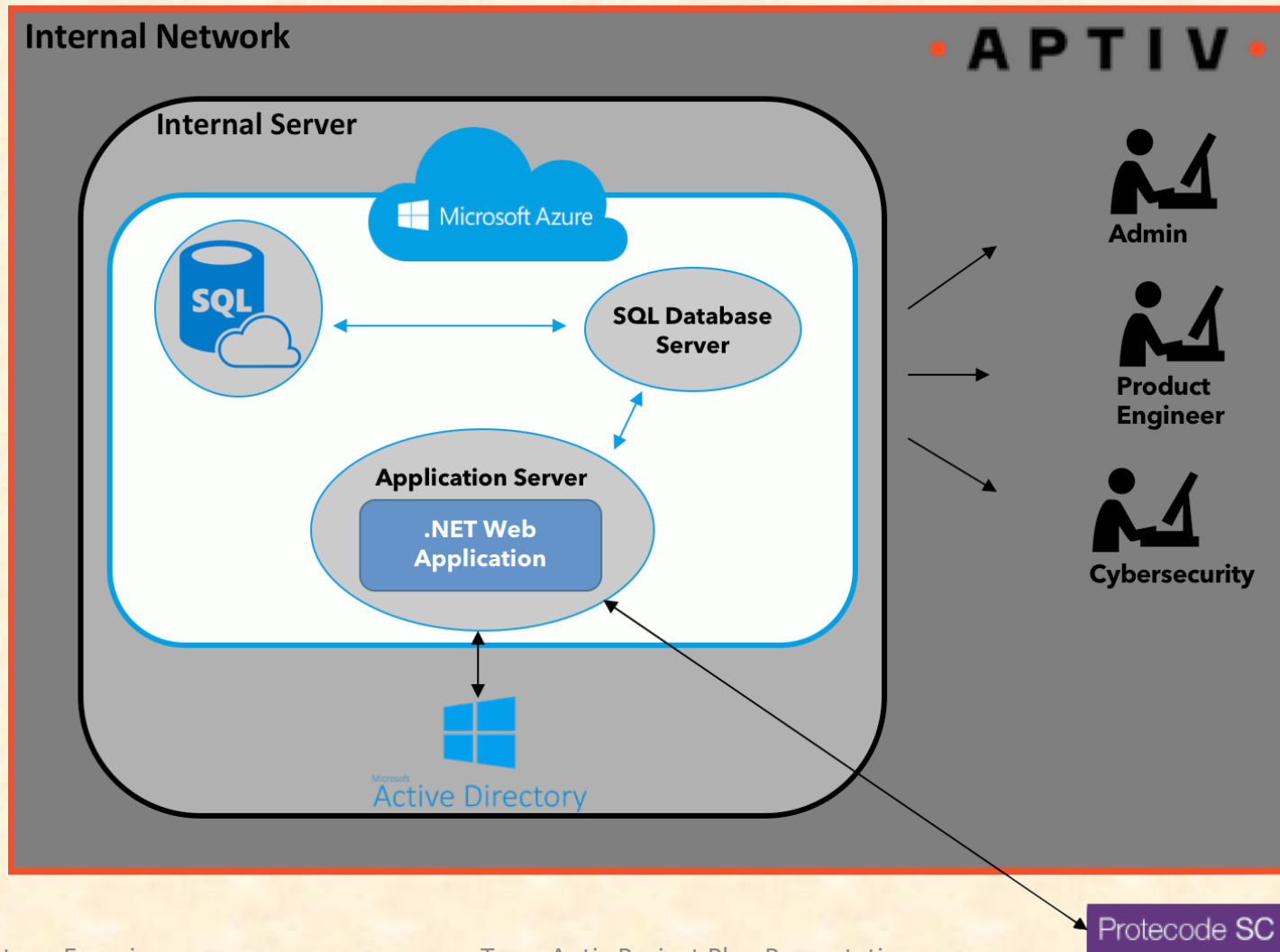
System Components

- Hardware Platforms
  - Microsoft Azure server
- Software Platforms / Technologies
  - Visual Studio
  - ASP.NET (C#)
  - Javascript
  - HTML/CSS
  - MS SQL Database
  - Microsoft Active Directory
  - Protecode API
  - Jenkins

Risks

- Application Security
    - Application/Database will hold all of Aptiv's data (schematics, software, vulnerabilities, etc.) for all products
    - Mitigation: Implementing best practice security measures as the system is developed, and perform dynamic code analysis on code developed using Protecode
- Database Implementation
    - Application uses complex data structures and holds vast amounts of data
    - Mitigation: Proper schema created and implemented to ensure only those authenticated can access data and the data is quickly accessible
- Knowledge of Client Procedure
    - To fully design the functionality for the application a complete understanding of all of Aptiv's cybersecurity processes, inputs, outputs, and integration is needed
    - Mitigation: Weekly conference calls with client and constant communication if needed allows for questions and clarifications on project model
- Scalability
    - Aptiv has 147,000 employees and develop hundreds of products a year; the application must be able to handle hundreds of users logged in and accessing data
    - Mitigation: Application hosted on Microsoft Azure, MS SQL database hosted on Microsoft Azure; cloud servers have ability to scale immediately and automatically

Questions?

? ? ? ?

? ?

? ?

?