

MICHIGAN STATE

UNIVERSITY

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

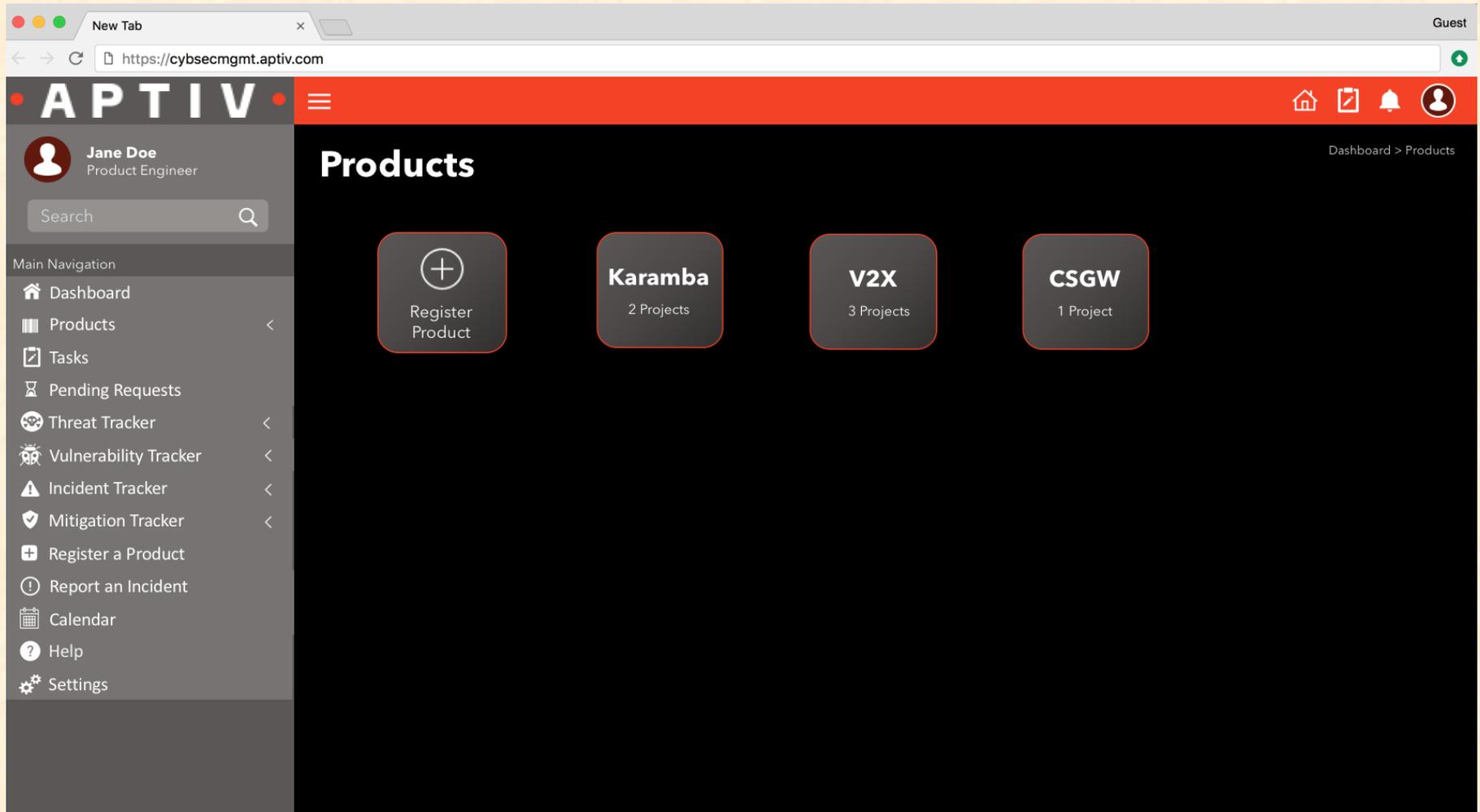
- Application to help with automation of Aptiv's cybersecurity processes
 - TARA, Vulnerability/Penetration Assessments, Mitigation Remediation, Incident Response
- 4 Trackers for analysis and visualization of information collected by system
 - Threat/Risks, Vulnerabilities, Incidents, Mitigations
-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

Design Specifications

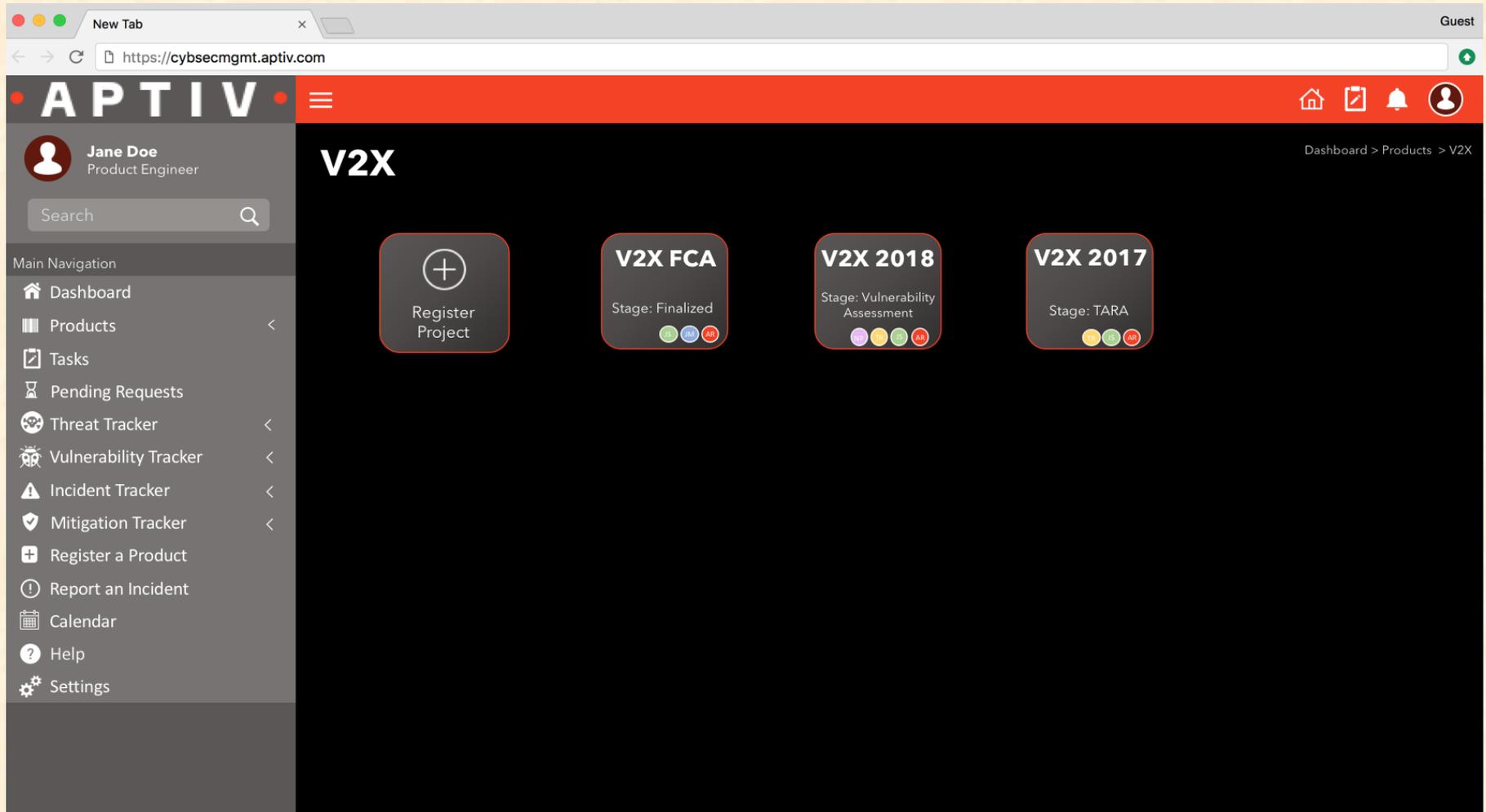
- ASP.NET (C#) Web Application
- Simple interface for all users
 - Dashboard
 - Project Pages
 - Cybersecurity Process Modules
 - Data Trackers
 - Task Manager



Screen Mockup: Product Dashboard



Screen Mockup: Project Dashboard



Screen Mockup: Incomplete Project Page

The screenshot shows a web browser window with the URL <https://cybsecmgmt.aptiv.com>. The page header features the APTIV logo and a user profile for Jane Doe, Product Engineer. The breadcrumb trail is Dashboard > Products > CSGW > CSGW. The main content area is titled "Project Status: Vulnerability Assessment" and includes a progress bar with stages: Project Registration, TARA, Mitigation Remediation, Vulnerability Assessment, Penetration Assessment, Final Approval, and Finalized. The current stage, Vulnerability Assessment, is highlighted in pink. Below the progress bar are three sections: "Recent Updates" with a list of actions and timestamps, "Project Modules" with four colored boxes for Project Information, TARA, Mitigation Remediation, and Vulnerability Assessment, and "Task Status" with a donut chart showing 58% In Progress, 23% New, 10% Closed, and 9% Resolved. At the bottom right, there is a "Pending Requests" table.

Project Status: Vulnerability Assessment

Project Registration → TARA → Mitigation Remediation → **Vulnerability Assessment** → Penetration Assessment → Final Approval → Finalized

Recent Updates

- Jane D. added 4 new members to the project 3 hours ago
- Josh M. approved final TARA 12 hours ago
- Tom I. set estimated date of penetration test to 2/14/18 2 days ago

[View more updates](#)

Project Modules

- Project Information
- TARA
- Mitigation Remediation
- Vulnerability Assessment

Task Status

Task Status	Percentage
In Progress	58%
New	23%
Closed	10%
Resolved	9%

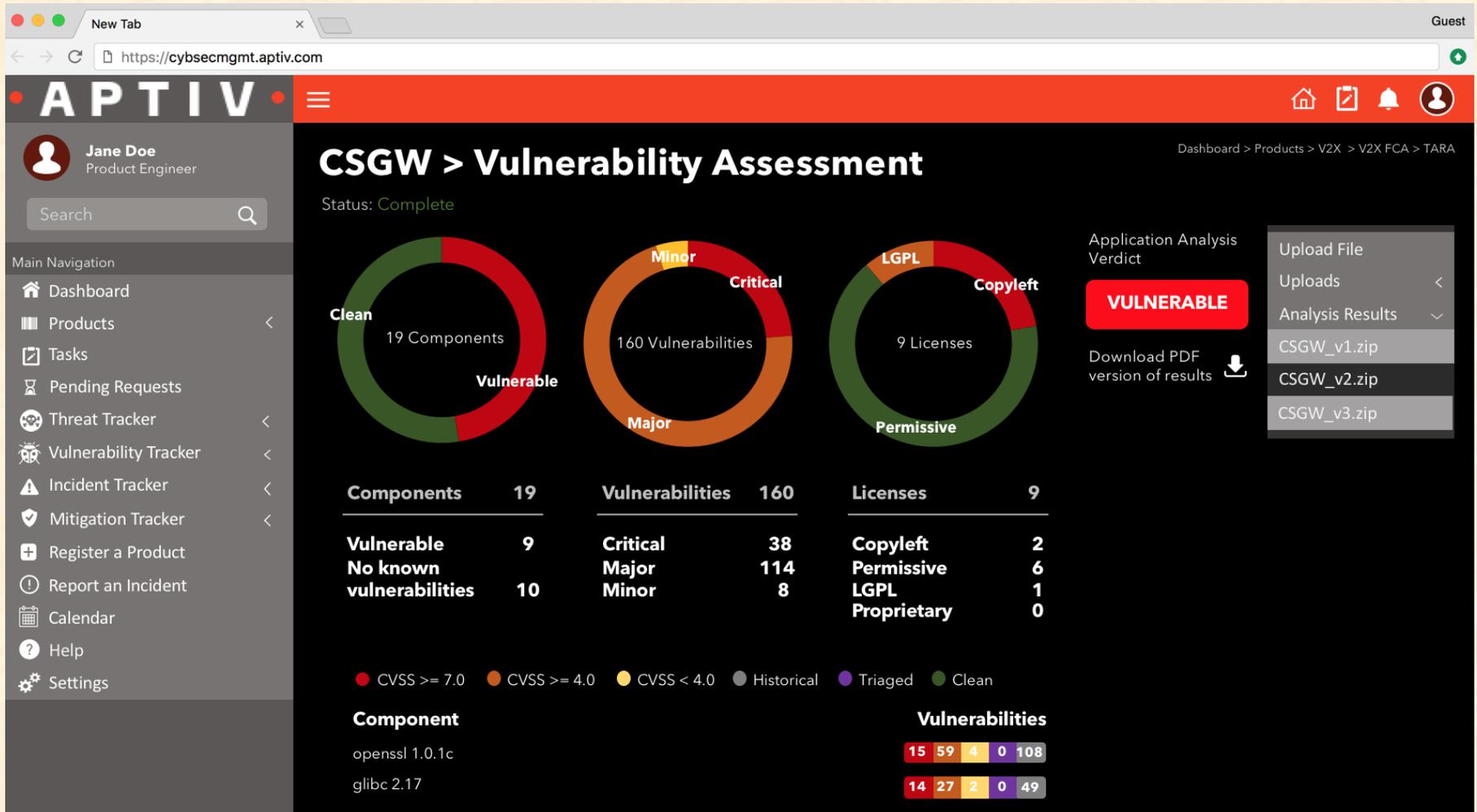
Pending Requests

Request	Date
Complete Vulnerability A...	01/25/18
Upload reqs for Penetrati...	01/25/18
Complete 4 mitigations	01/24/18

Main Navigation

- Dashboard
- Products
- Tasks
- Pending Requests
- Threat Tracker
- Vulnerability Tracker
- Incident Tracker
- Mitigation Tracker
- Register a Product
- Report an Incident
- Calendar
- Help
- Settings

Screen Mockup: Vulnerability Assessment Module



Screen Mockup: Completed Project Page

APTIV | Guest

Josh M. Cybersecurity Engineer

Search

Main Navigation

- Dashboard
- Products
- Tasks
- Pending Requests
- Threat Tracker
- Vulnerability Tracker
- Incident Tracker
- Mitigation Tracker
- Register a Product
- Report an Incident
- Calendar
- Help
- Settings

V2X FCA

Project Status: Finalized

Project Registration → TARA → Mitigation Remediation → Vulnerability Assessment → Penetration Assessment → Final Approval → Finalized

Recent Updates

- Jane D. added 2 new members to the project 3 hours ago
- Josh M. accepted Final Approval Request 2 days ago
- Jane D. marked Task 5 V2X.OS.4 Boot Process as Completed 3 days ago

Tasks

#	Title	Priority
2	Set up V2X test bench	High
8	V2X.CAN.5 Normal...	Medium
3	V2X.OS.2 Process P...	Medium
4	V2X.OS.3 Password...	Medium
13	Update Attack Plan	Low

View all tasks

Project Modules

- Project Information
- TARA
- Mitigation Remediation
- Vulnerability Assessment
- Penetration Assessment
- Final Approval

Task Status

Donut Chart:

- 35% (Resolved)
- 45% (Closed)
- 12% (In Progress)
- 8% (New)

Pending Requests

Request	Date
No current Pending Requests	



Screen Mockup: Task Manager

The screenshot shows a web browser window with the URL <https://cybsecmgmt.aptiv.com>. The page features a red header with the APTIV logo and navigation icons. A left sidebar contains a user profile for Jane Doe (Product Engineer) and a main navigation menu with options like Dashboard, Products, Tasks, Pending Requests, Threat Tracker, Vulnerability Tracker, Incident Tracker, Mitigation Tracker, Register a Product, Report an Incident, Calendar, Help, and Settings. The main content area is titled 'Task Manager' and includes a search bar, a '+ Add New Task' button, and a summary bar showing task counts: New(44), In Progress(4), Resolved(2), and Closed(3). A table lists tasks with columns for #, Title, Assigned To, Priority, Status, and Due Date. A 'Project' dropdown menu is open on the right, showing options like CSGW, V2X 2017, V2X 2018, V2X CES, Karamba, and Karamba FCA.

#	Title	Assigned To	Priority	Status	Due Date
Today					
47	Setup Bench <small>Updated by Bryant Today 11:11 am</small>	Bryant <small>V2X 2017</small>	High	In Progress	Feb 02, Fri
48	Develop AM Tests <small>Updated by Bryant Today 11:13 am</small>	Bryant <small>V2X 2017</small>	High	In Progress	
51	Define tests for Voice R... <small>Created by Bryant Today 11:52 am</small>	Charles <small>V2X CES</small>	High	New	Jan 31, Wed
Oct 19, 2017					
28	VP2.BT.3 Identify PIN Code <small>Updated by Bryant on Oct 19, 2017 10:01 am</small>	Nik <small>V2P FCA</small>	Medium	New	Jan 30, Tues
29	VP2.BT.4 Blind Pairing <small>Updated by Bryant on Oct 19, 2017 10:02 am</small>	Nik <small>V2P FCA</small>	Medium	New	Jan 30, Tues



Screen Mockup: Incident Tracker

The screenshot displays the APTIV Incident Tracker interface. The top navigation bar is red with the APTIV logo and a hamburger menu. The user profile for Jane Doe, Product Engineer, is visible in the top left. The main content area is titled 'Incident Tracker > Grid View' and contains a table of incidents. A 'Sort By' dropdown menu is open, showing options for sorting by Product, Product Line, Contact, Creation Date, Close Date, and Severity. The table has columns for Incident Name, Contact Name/Email, Products(s), Product Line, Creation Date, Download Attachments, and Description. The incidents listed are Incident1 through Incident11.

Incident Name	Contact Name/Email	Products(s)	Product Line	Creation Date	Download Attachments	Description	Severity
Incident1	Jane Doe, jane.doe@aptiv.com	V2X 2018, V2X 2017	AD OEM	1/23/18	Download		High
Incident2	Jane Doe, jane.doe@aptiv.com	V2X CES	AD OEM	6/21/17	Download		High
Incident3	Jane Doe, jane.doe@aptiv.com	V2X CES	AD OEM	3/13/17	Download		High
Incident4	Jane Doe, jane.doe@aptiv.com	CSGW	C&S	3/13/17	Download		High
Incident5	Jane Doe, jane.doe@aptiv.com	V2P Ford	UX	12/20/17			High
Incident6	Jane Doe, jane.doe@aptiv.com	V2X FCA, V2X CES, V2X 2018	AD OEM	1/10/18	Download		Medium
Incident7	Jane Doe, jane.doe@aptiv.com	Karamba Carwall	Safety	8/2/17			Medium
Incident8	Jane Doe, jane.doe@aptiv.com	V2X 2018, V2X 2017	AD OEM	9/17/17	Download		Medium
Incident9	Jane Doe, jane.doe@aptiv.com	CSGW	C&S	11/12/17	Download		Medium
Incident10	Jane Doe, jane.doe@aptiv.com	Karamba Carwall	Safety	12/13/17	Download		Low
Incident11	Jane Doe, jane.doe@aptiv.com	V2P Ford	UX	8/7/17			Low

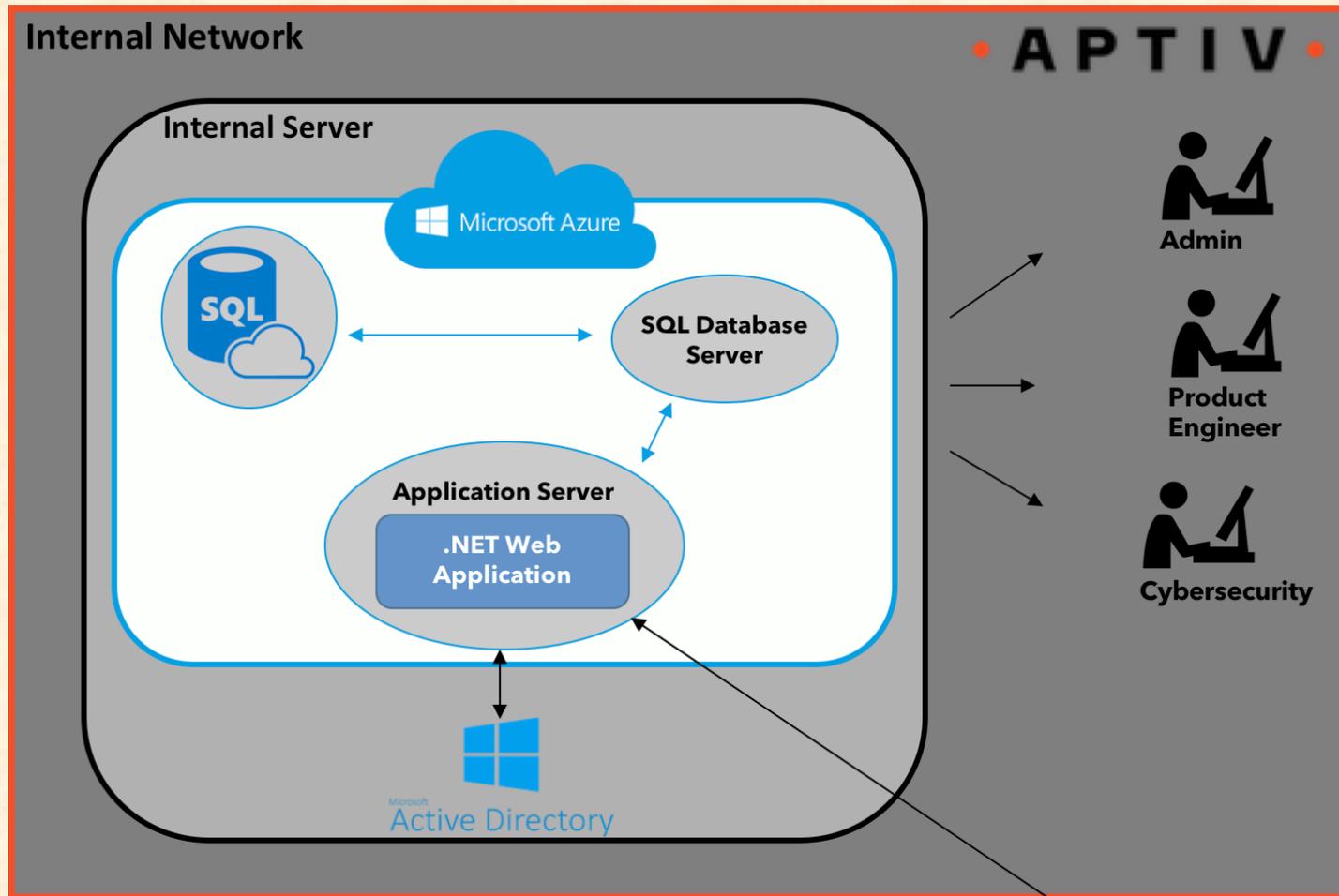


Technical Specifications

- 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?

?

?

?

?

?

?

?

?

?

