

**MICHIGAN STATE**  

---

**U N I V E R S I T Y**

# Beta Presentation

## CMS: Cybersecurity Management System

### The Capstone Experience

Team Aptiv

Dillon Brown

Wei Jiang

Clayton Peters

Ashtaan Rapanos

Winton Qian

Department of Computer Science and Engineering  
Michigan State University  
Spring 2018



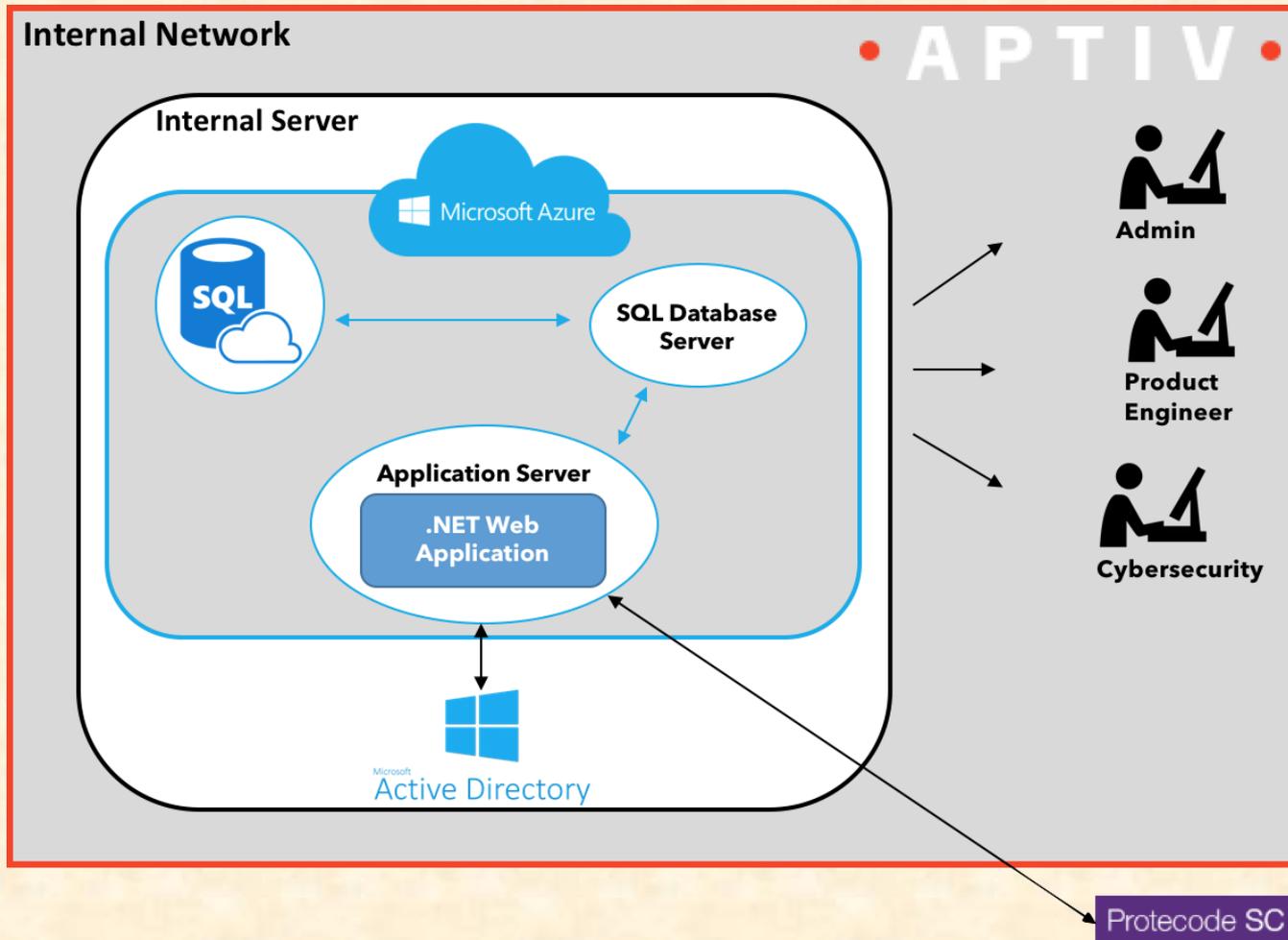
*From Students...  
...to Professionals*

# Project Overview

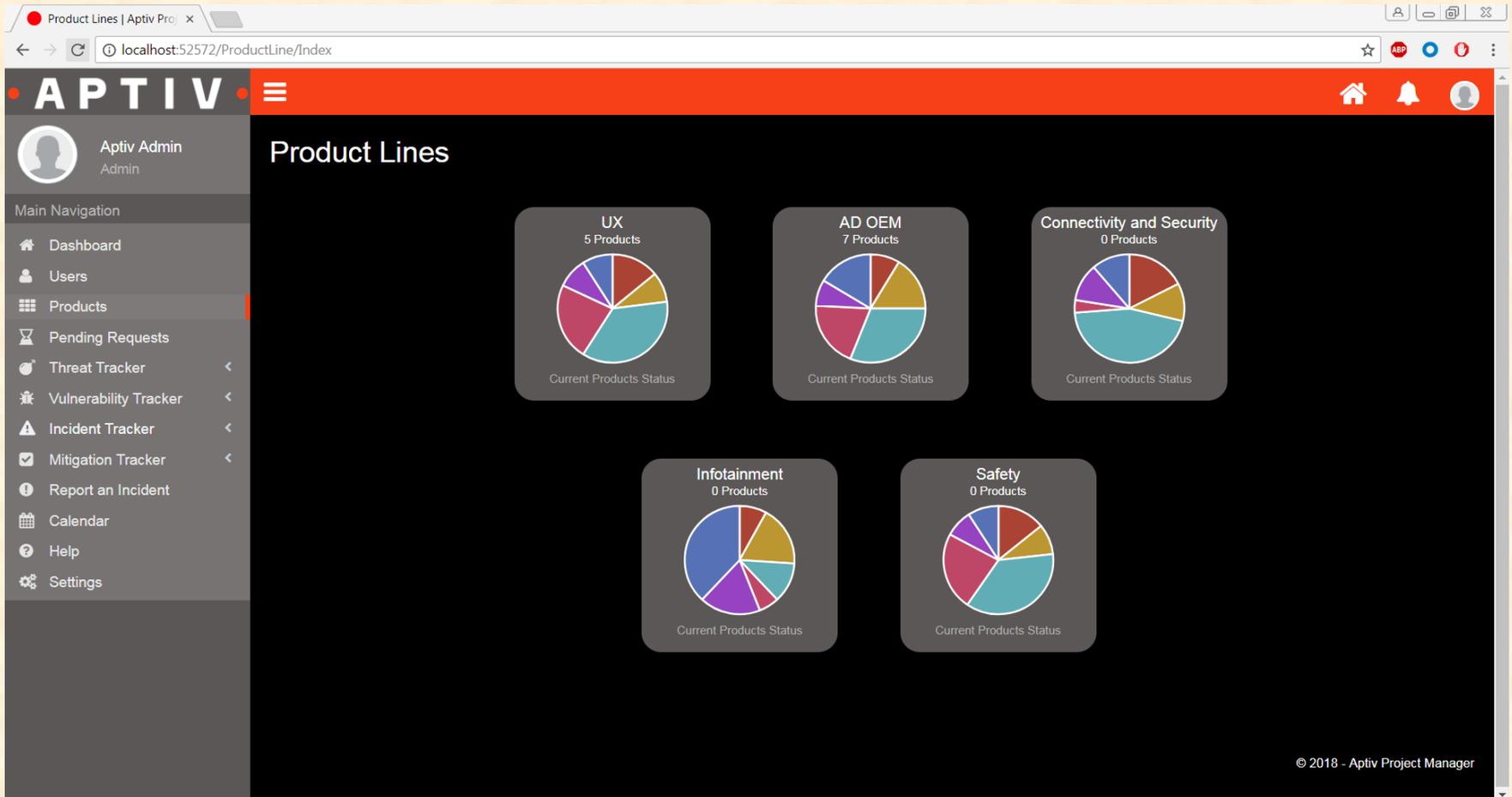
- Web application to help with automation and consolidation of Aptiv's product cybersecurity processes
- 4 Trackers for analysis and visualization of information collected by system
  - Threats/Risks
  - Vulnerabilities
  - Incidents
  - Mitigations
- Increase productivity and help communication by implementing request system, email alerts and notifications



# System Architecture



# Product Lines



© 2018 - Aptiv Project Manager

# Product Page

The screenshot displays the APTIV V2X 2017 Product Page. The browser address bar shows the URL: localhost:52572/Product/Index?productName=V2X%202017&lineName=UX. The user is logged in as 'Aptiv Admin'.

**Main Navigation:**

- Dashboard
- Users
- Products
- Pending Requests
- Threat Tracker
- Vulnerability Tracker
- Incident Tracker
- Mitigation Tracker
- Report an Incident
- Calendar
- Help
- Settings

**V2X 2017 Product Status: Final Approval**

Product Status Progress: Product Registration → TARA → Mitigation Remediation → Vulnerability Assessment → Penetration Assessment → Final Approval → Finalized

**Recent Updates:** There are no recent updates.

**Product Modules:**

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

**Task Status:** There are no tasks.

**Tasks:** There are no tasks.

**Pending Requests:**

Request	Date
Upload data schematics for penetration assessment	2/18/2018 12:00:00 AM
Upload firmware for penetration assessment	2/18/2018 12:00:00 AM
Complete mitigation #23	2/17/2018 12:00:00 AM



# TARA Module

The screenshot displays the TARA Module web interface. The browser address bar shows the URL: localhost:52572/TARA/Index?product=V2X%202017. The page header features the APTIV logo and navigation icons. The user is logged in as 'Aptiv Admin Admin'. The main content area is titled 'V2X 2017 > TARA' and 'V2X 2017 Risk Assessment'. The asset ID is 'V2XFAC\_01' and the case ID is 'Use\_Case\_01'. The interface shows three risk assessment cards, each with a table of threat factors and their corresponding Likelihood, Impact, and Risk scores.

Threat Type	Risk Severity	Likelihood	Impact	Risk
Spoofting	Critical	4	5.66	22.64
Information Disclosure	Critical	4	3.22	12.88
Spoofting	Low	1	1	1

Asset ID: V2XFAC\_01 Case ID: Use\_Case\_01

Threat Type: Spoofting Risk Severity: Critical

Expertise: Very High Safety: Very High Likelihood: 4 Impact: 5.66 Risk: 22.64

Knowledge: Very High Operational: Very High

Window of Opportunity: Very High Privacy: Very High

Required Equipment: Very High

Likelihood Impact Scores

Threat Type: Information Disclosure Risk Severity: Critical

Expertise: Very High Safety: High Likelihood: 4 Impact: 3.22 Risk: 12.88

Knowledge: Very High Operational: Medium

Window of Opportunity: Very High Privacy: Medium

Required Equipment: Very High

Likelihood Impact Scores

Threat Type: Spoofting Risk Severity: Low

Expertise: Low Safety: Low Likelihood: 1 Impact: 1 Risk: 1

Knowledge: Low Operational: Low

Window of Opportunity: Low Privacy: Low

# Penetration Assessment Module

The screenshot displays the APTIV web application interface for the Penetration Assessment Module. The browser address bar shows the URL: localhost:52572/PenetrationAssessment/Index?product=V2X%202017. The interface features a dark theme with a prominent orange header bar containing the APTIV logo and navigation icons. A left sidebar lists various navigation options: Dashboard, Users, Products, Pending Requests, Threat Tracker, Vulnerability Tracker, Incident Tracker, Mitigation Tracker, Report an Incident, Calendar, Help, and Settings. The main content area is titled "V2X 2017 > Penetration Assessment" and includes an "Add Asset" button. Below this, there are two asset cards: "Asset: Bluetooth" and "Asset: CAN". The Bluetooth asset card contains three attack plans: Plan 1, Plan 2, and Plan 3, each with an "Edit" link and a description. The CAN asset card contains one attack plan: Plan 1, also with an "Edit" link and description. A right sidebar lists "Assessment Request", "Attack Plan", and "Tests". The footer of the interface shows the copyright notice: © 2018 - Aptiv Project Manager.



# What's left to do?

---

- Project video
- Bug fixes
- Input validation
- Small UX changes



# Questions?

---

?

?

?

?

?

?

?

?

?

