Cyber Risk Insights (CRI)

PwC's Cyber Risk Insights Will Address These Challenges in a Strategic, Calibrated and Efficient Manner

PwC's Next Generation threat management solution ('Cyber Risk Insights') delivers automated monitoring, protection and remediation measures. The focus is to provide a complete view of the risk landscape and proactively respond to emerging risks.

1 Contextualized Risk-Based Prioritization

Context based risk scoring is the core of 'Cyber Risk Insights' platform which is enabled by threat models, exploitability parameters, external threat feed and patterns generated from organization specific landscape.

2 One Click Risk View across the landscape

Unified dashboards provide holistic view of real time vulnerabilities and support senior management to visualize the risk movement across the organization

3 Agility to integrate new processes

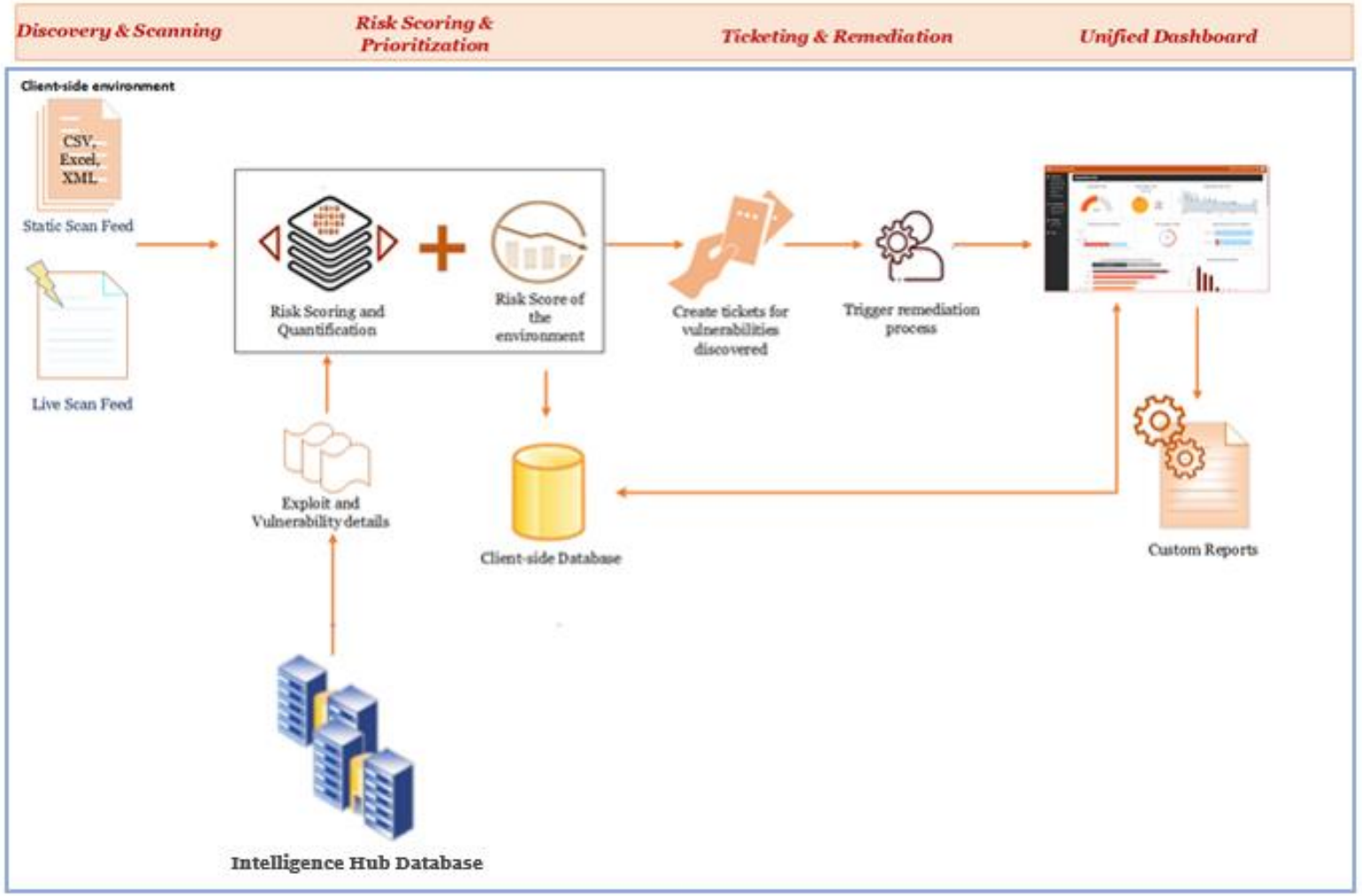
Integrate the associated processes to accelerate the entire discovery , communication and remediation processes

4 Support in Remediation Orchestration

The platform offers an in-built way to track the status of the issue in its remediation workflow, along with capability to integrate with external ticketing systems.

Cyber Risk Insights Architecture and Base Technologies

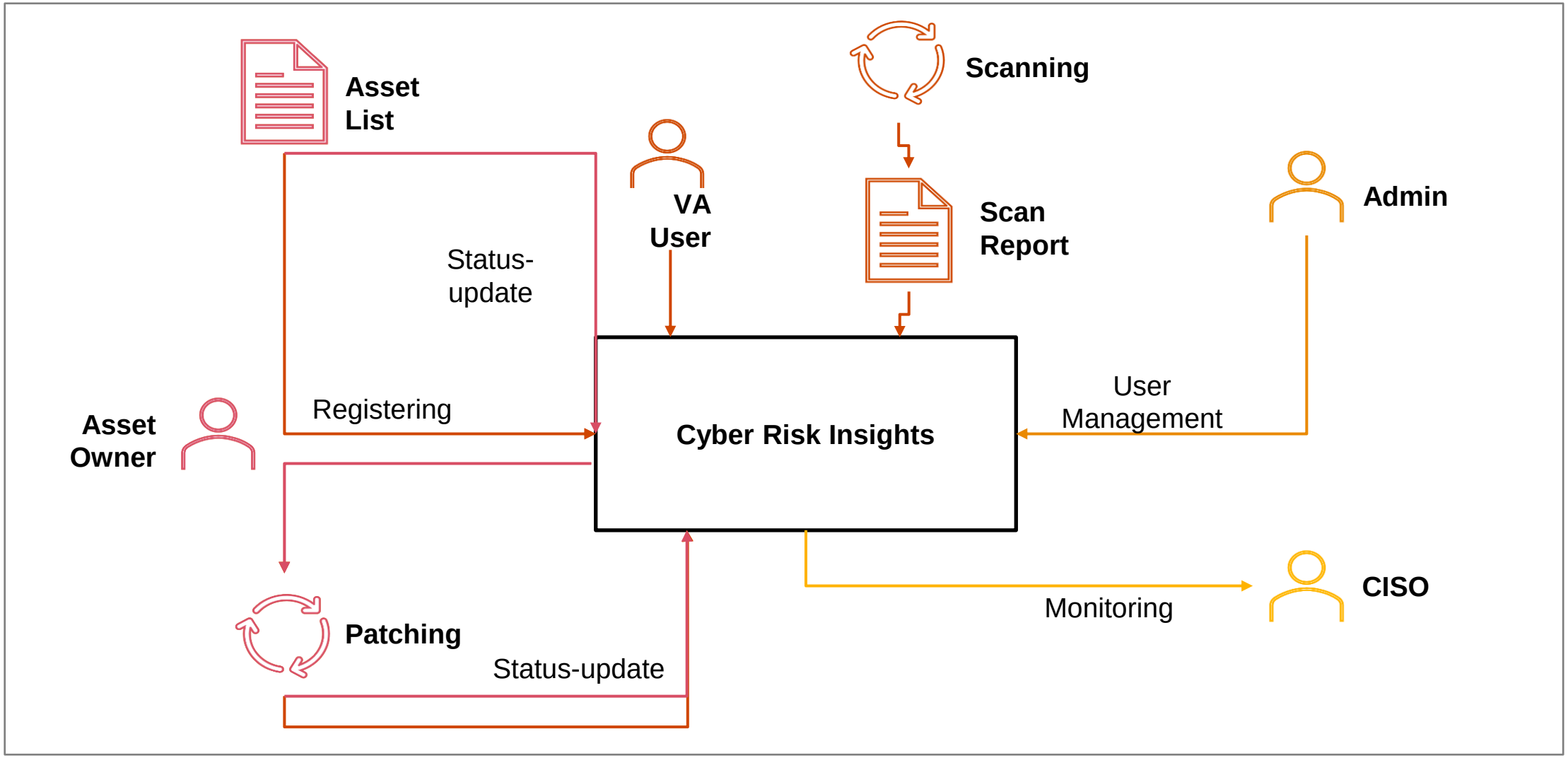
S. No.	Solution Components
1	User Interface built using modern SPA (Single Page Application) UI framework.
2	Dedicated business logic implemented via REST APIs.
3	Multiple data-analytics and automation scripts at the backend
4	Relational Database is integrated in the solution.
5	Dedicated LDAP is integrated in the solution for Identity management.



User Roles in Cyber Risk Insights Tool

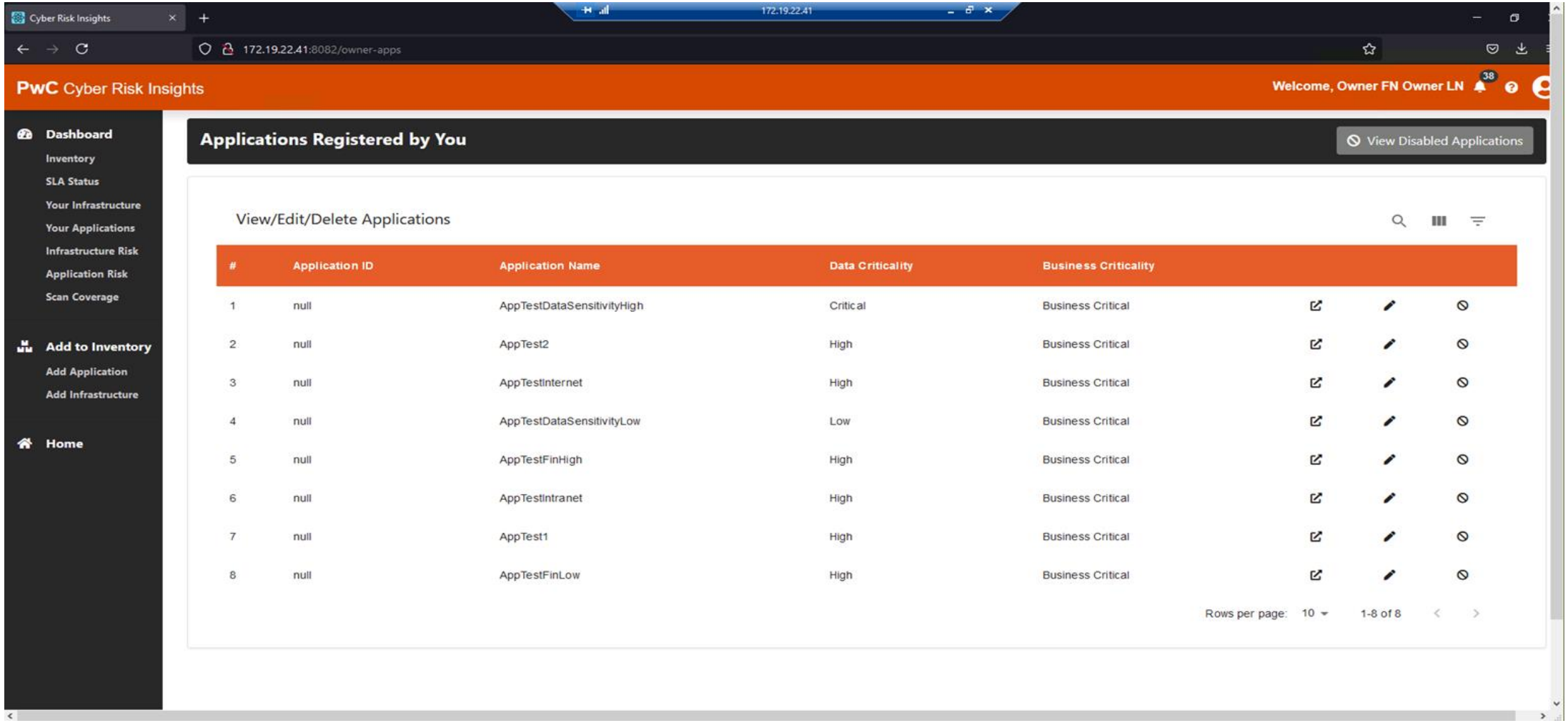
Role Name	Role Description	What does the role have access to?
Asset Owner	The asset owner can register assets (applications/ infrastructure) on the CRI application and monitor the assets registered by them.	This role has access to the data pertaining to the specific assets registered by them. Eg: vulnerabilities, trends , etc.
VA Team	This is the vulnerability analyst team member who is responsible for managing scans and related actions on IT assets from the CRI application.	This role has access to all data (except user profile related data) present in CRI application which includes data about the assets registered and the vulnerabilities pertaining to them.
CISO (Chief Information Security Officer)	The CISO is a senior management executive who has a holistic view of the organization's security posture.	This role has access to high level visualizations and charts, reporting metrics for organizational/asset level risks.
Admin	This is the role for managing various configurations in CRI.	The admin manages user access, configures SLAs and business units.

Responsibilities and Workflow in Cyber Risk Insights Tool



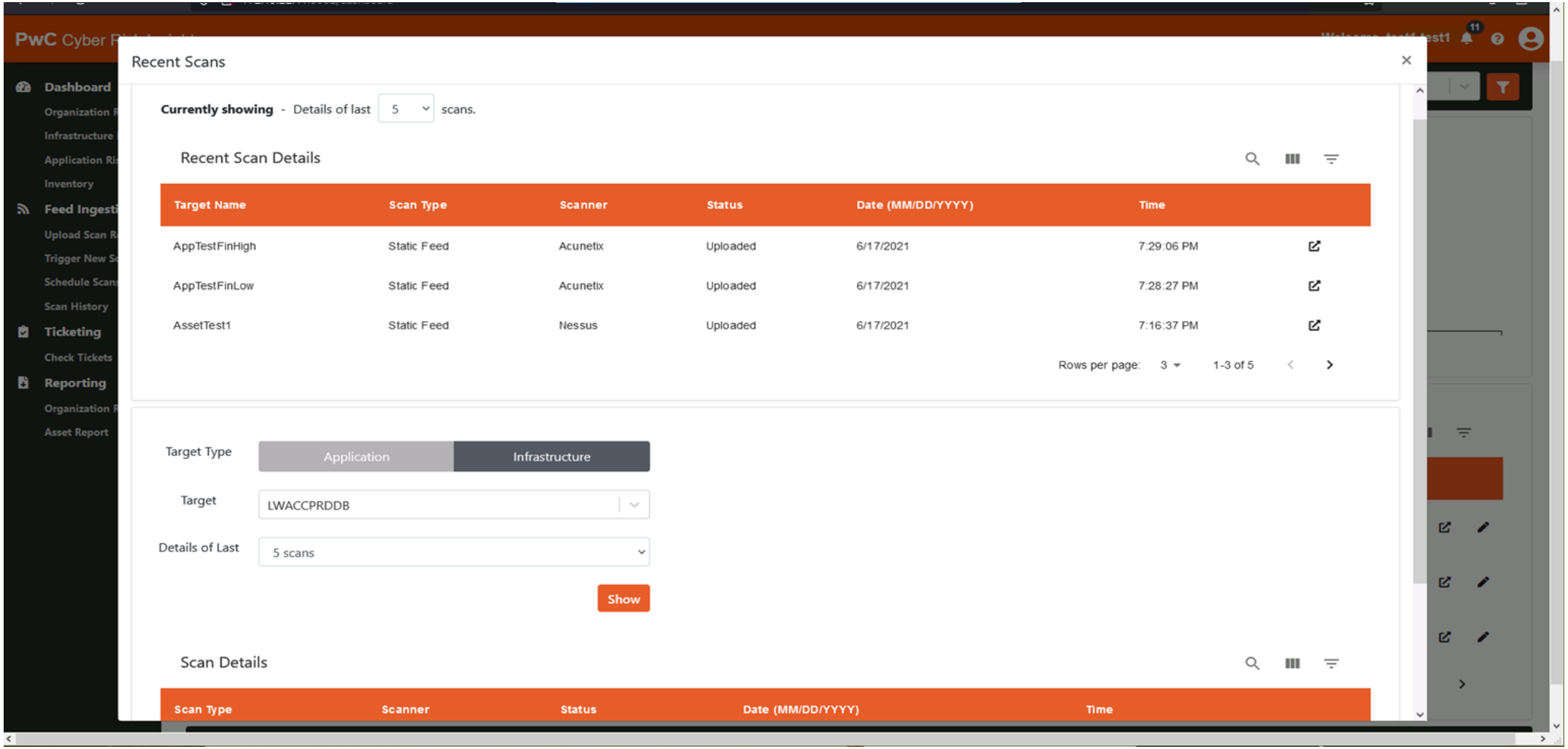
Asset Owner Dashboard

The figures below show the asset owner dashboard used to register assets and view security risk posture pertaining to the owner specific applications and infrastructures.



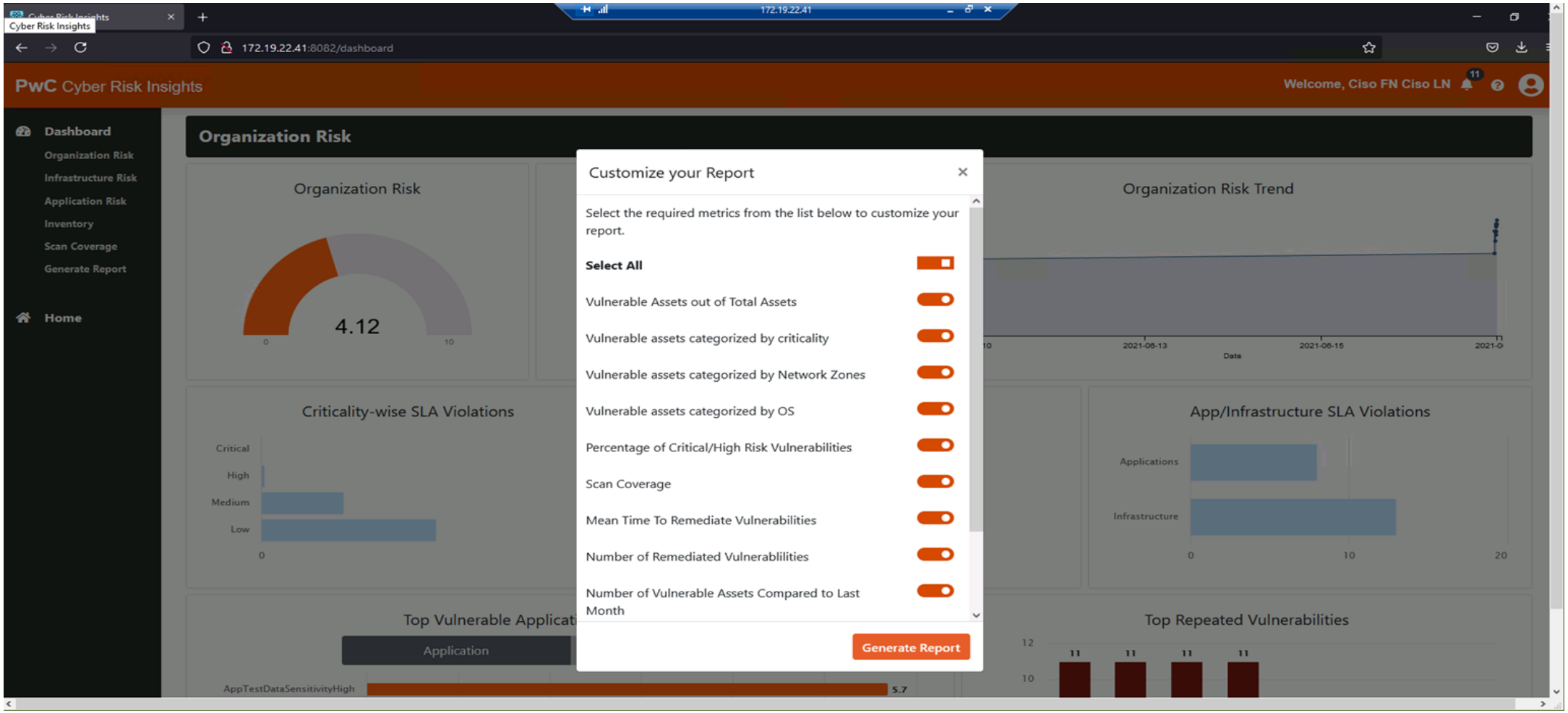
VA Team Member Dashboard

The below figures show the dashboard of a VA Team which is used to ingest scan reports, trigger or schedule new scans from the tool to generate risk scores.



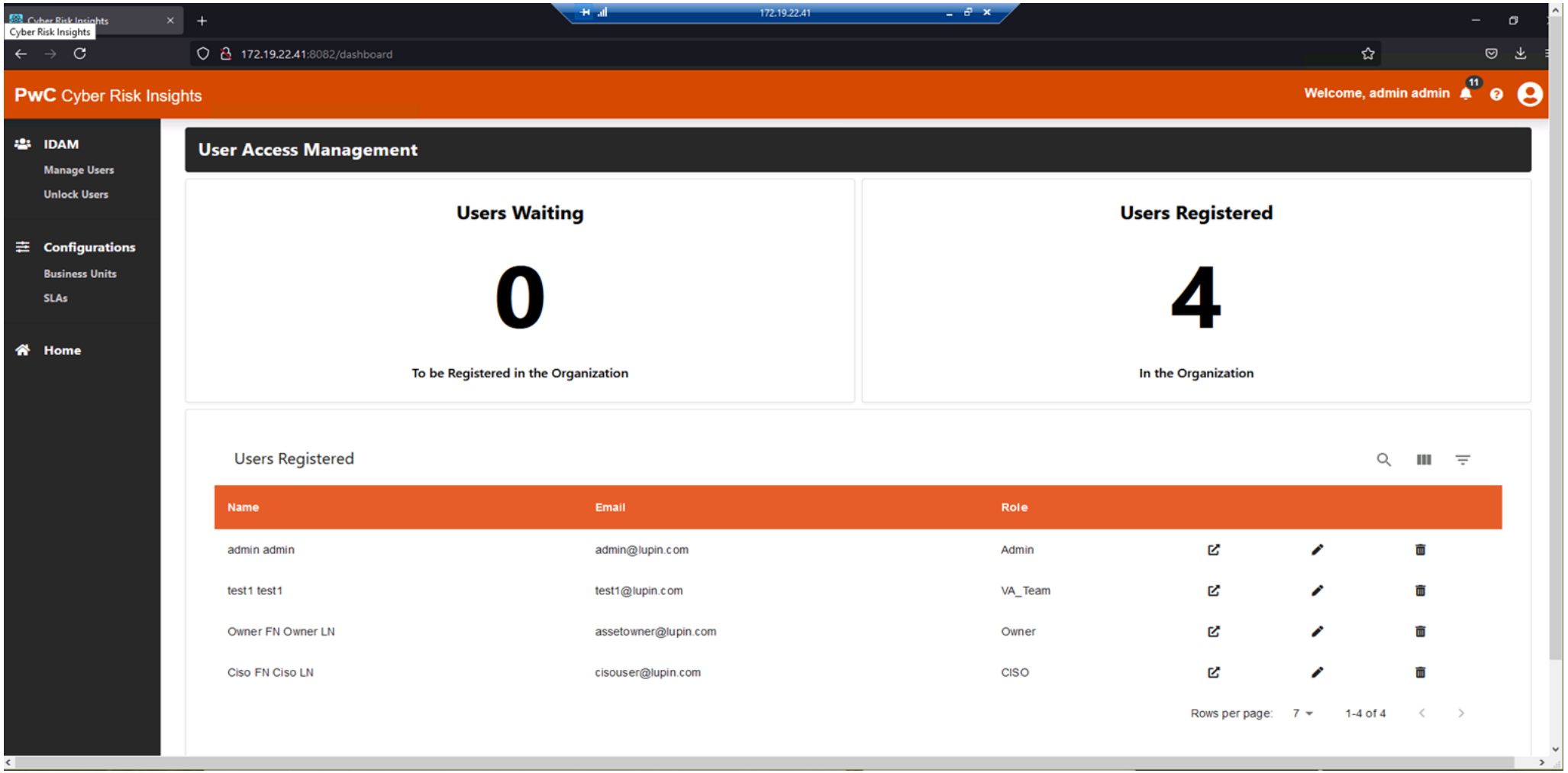
CISO Dashboard

The figures below show the CISO dashboard giving an overall view of the security risk posture of the organization.



Admin Dashboard

The below figure shows the dashboard of Admin who can perform user registration.



Deployment Requirements for CRI Tool

Sr. No.	Software requirements (we can install ourselves if Internet access if present)
1	Java - 8.0 and above
2	Python - https://www.python.org/ftp/python/3.8.6/python-3.8.6-amd64.exe
3	MySQL v8.0.21 - https://downloads.mysql.com/archives/get/p/25/file/mysql-installer-community-8.0.21.0.msi
4	Wkhtmltopdf - https://github.com/wkhtmltopdf/packaging/releases/download/0.12.6-1/wkhtmltox-0.12.6-1.msvc2015-win64.exe
5	OpenLDAP - https://www.maxcrc.de/wp-content/uploads/2020/04/OpenLDAPforWindows_x64.zip
6	Tomcat 9.0 - https://mirrors.estointernet.in/apache/tomcat/tomcat-9/v9.0.44/bin/apache-tomcat-9.0.44-windows-x64.zip
7	Apache Directory Studio - https://archive.apache.org/dist/directory/studio/2.0.0.v20200411-M15/ApacheDirectoryStudio-2.0.0.v20200411-M15-win32.win32.x86_64.exe
8	Node.js - https://nodejs.org/download/release/v14.15.4/node-v14.15.4-win-x86.zip
9	Windows IIS
10	SSL Certificate (nature as suitable)

Sr. No.	Minimum Hardware Requirements
1	16GB RAM
2	256 GB Storage
3	Windows Server OS 2019 or 2016
4	4-core processor
6	Internet Connectivity (or a way to get set-up files of required supporting software)