1. ****

**COMSATS University Islamabad (CUI)**

Software Requirement Specification  
(SRS DOCUMENT)

for

**Cyberfy**

Version 1.0

***By***

**Sidra Saleem SP21-BSE-082**

*Bachelor of Science in Software Engineering*

[1. Introduction 1](#_Toc136809943)

[1.1 Purpose 1](#_Toc136809944)

[1.2 Scope 1](#_Toc136809945)

[1.3 Modules 1](#_Toc136809946)

[1.3.1 Module 1: Threat Detection and Response 1](#_Toc136809947)

[1.3.2 Module 2: Vulnerability Assessment and Management 1](#_Toc136809948)

[1.3.3 Module 3: Network Monitoring and Analysis 2](#_Toc136809949)

[1.3.4 Module 4: Access Control and Authentication 2](#_Toc136809950)

[1.3.5 Module 5: Data Encryption and Protection 2](#_Toc136809951)

[1.3.6 Module 6: Incident Management and Response 2](#_Toc136809952)

[1.4 Overview 3](#_Toc136809953)

[2. Overall Description 3](#_Toc136809954)

[2.1 Product Perspective 3](#_Toc136809955)

[2.2 User classes and characteristics 4](#_Toc136809956)

[2.3 Operating Environment 5](#_Toc136809957)

[2.4 Design and Implementation Constraints 5](#_Toc136809958)

[3. Requirement Identifying Technique 6](#_Toc136809959)

[3.1 Use Case Diagram 6](#_Toc136809960)

[3.2 Event Response Tables 7](#_Toc136809961)

[3.2.1 Network Scanning Initiation 7](#_Toc136809962)

[3.2.2 Threat Intelligence Gathering 7](#_Toc136809963)

[3.2.3 Machine Learning-based Vulnerability Detection 8](#_Toc136809964)

[3.2.4 Remediation Plan Generation 8](#_Toc136809965)

[3.2.5 Compliance Check Initiation 8](#_Toc136809966)

[3.2.6 Notification and Alert Generation 8](#_Toc136809967)

[3.2.7 Report Generation 9](#_Toc136809968)

[3.3 Detail Use Cases 10](#_Toc136809969)

[3.3.1 UC-1 : User Account Creation 10](#_Toc136809970)

[3.3.2 User Authentication 11](#_Toc136809971)

[3.3.3 User Account Management 12](#_Toc136809972)

[3.3.4 System Update 12](#_Toc136809973)

[3.3.5 Dashboard Updating 13](#_Toc136809974)

[4. Functional Requirements 14](#_Toc136809975)

[4.1 User Account Creation 14](#_Toc136809976)

[4.1.1 < Register.User.Internet > 14](#_Toc136809977)

[4.1.2 < Register.Administrator.Validation > 15](#_Toc136809978)

[4.1.3 <Register.Administrator.UsernameUniqueness> 16](#_Toc136809979)

[4.1.4 <Register.Administrator.PasswordComplexity> 17](#_Toc136809980)

[4.1.5 <Register.Administrator.PasswordStorage> 18](#_Toc136809981)

[4.1.6 <Register.Administrator.ConfirmationEmail> 18](#_Toc136809982)

[4.1.7 <Register.Administrator.ActivationLink> 19](#_Toc136809983)

[4.1.8 <Register.Administrator.AccountActivation> 20](#_Toc136809984)

[4.2 User Authentication 21](#_Toc136809985)

[4.2.1 < Login.User.LoginForm> 21](#_Toc136809986)

[4.2.2 <Login.User.CredentialsValidation> 21](#_Toc136809987)

[4.2.3 <Login.User.AccountAccess> 22](#_Toc136809988)

[4.2.4 <Login.User.InvalidCredentialsError> 22](#_Toc136809989)

[4.2.5 <Login.User.PasswordValidation> 23](#_Toc136809990)

[4.2.6 <Login.User.PasswordEncryption> 23](#_Toc136809991)

[4.2.7 <Login.User.AccountLockout> 24](#_Toc136809992)

[4.2.8 <Login.User.SecureCommunication> 24](#_Toc136809993)

[4.2.9 <Login.User.LoginAttemptsLogging> 25](#_Toc136809994)

[4.2.10 <Login.User.UnauthorizedAccessProtection> 25](#_Toc136809995)

[4.2.11 <Login.User.SecureSessionManagement> 26](#_Toc136809996)

[4.2.12 <Login.User.VulnerabilityProtection> 27](#_Toc136809997)

[4.2.13 <Login.User.SessionExpiration> 27](#_Toc136809998)

[4.3 Forget Password 28](#_Toc136809999)

[4.3.1 <Login.User.ForgotPasswordOption> 28](#_Toc136810000)

[4.3.2 <Login.User.ForgotPasswordPrompt> 29](#_Toc136810001)

[4.3.3 <Login.User.EmailValidation> 29](#_Toc136810002)

[4.3.4 <Login.User.PasswordResetLink> 29](#_Toc136810003)

[4.3.5 <Login.User.PasswordResetLinkSecurity> 30](#_Toc136810004)

[4.3.6 <Login.User.PasswordResetSuccessMessage> 30](#_Toc136810005)

[4.3.7 <Login.User.InvalidEmailAddressErrorMessage> 31](#_Toc136810006)

[4.3.8 <Login.User.PasswordResetForm> 31](#_Toc136810007)

[4.3.9 <Login.User.PasswordValidation> 31](#_Toc136810008)

[4.3.10 <Login.User.PasswordEncryption> 32](#_Toc136810009)

[4.3.11 <Login.User.PasswordResetSuccessMessage> 32](#_Toc136810010)

[4.3.12 <Login.User.PasswordRecoverySecurity> 32](#_Toc136810011)

[4.3.13 <Login.User.PasswordRecoveryLogging > 33](#_Toc136810012)

[4.3.14 <Login.User.PasswordRecoverySecurity> 33](#_Toc136810013)

[4.4 Network Scanning 34](#_Toc136810014)

[4.4.1 < NetworkScanning.UserInterface > 34](#_Toc136810015)

[4.4.2 < NetworkScanning.UserInterface.NetworkSegments> 37](#_Toc136810016)

[4.4.3 < NetworkScanning.DisplayProgress > 38](#_Toc136810017)

[4.4.4 < NetworkScanning.CustomizeParameters > 38](#_Toc136810018)

[4.4.5 < NetworkScanning.PresentScanResults > 39](#_Toc136810019)

[4.4.6 < NetworkScanning.UserInterface.FilterSortScanResults > 39](#_Toc136810020)

[4.4.7 < NetworkScanning.UserInterface.VisualizeSecurityPosture > 40](#_Toc136810021)

[4.4.8 < NetworkScanning.UserInterface.VisualizeSecurityPosture > 40](#_Toc136810022)

[4.4.9 < NetworkScanning.UserInterface.ScanReports > 41](#_Toc136810023)

[4.4.10 < NetworkScanning.UserInterface.ScheduleScans > 42](#_Toc136810024)

[4.4.11 < NetworkScanning.System.NotificationsAndAlerts > 44](#_Toc136810025)

[4.4.12 < NetworkScanning.UserInterface.AuthenticationAccessControl > 45](#_Toc136810026)

[4.4.13 < NetworkScanning.UserInterface.ContextSensitiveHelp > 46](#_Toc136810027)

[4.4.14 < NetworkScanning.UserInterface. RealTimeUpdates > 48](#_Toc136810028)

[4.4.15 < NetworkScanning.History.MaintainHistoryAndReviewScans > 49](#_Toc136810029)

[4.4.16 < NetworkScanning.UserInterface.MultiLanguageAndAccessibility > 50](#_Toc136810030)

[4.4.17 < NetworkScanning.UserInterface.Dashboard> 52](#_Toc136810031)

[4.5 Network Scanning Techniques 53](#_Toc136810032)

[4.5.1 < NetworkScanning.Techniques.Support > 53](#_Toc136810033)

[4.5.2 < NetworkScanning.UserInterface.SelectScanningTechniques > 54](#_Toc136810034)

[4.5.3 < NetworkScanning.AutomatedScanningProfiles > 59](#_Toc136810035)

[4.5.4 < NetworkScanning.UserInterface.DisplayScanProgress > 60](#_Toc136810036)

[4.5.5 < NetworkScanning. <NetworkScanning.Presentation.PresentFindings > 60](#_Toc136810037)

[4.5.6 < NetworkScanning.UserInterface.GenerateTechniqueReports> 61](#_Toc136810038)

[4.5.7 < NetworkScanning.UserInterface. CompareScanningResults > 61](#_Toc136810039)

[4.5.8 < NetworkScanning.UserInterface.VisualRepresentations > 62](#_Toc136810040)

[4.5.9 < NetworkScanning.UserInterface. KnowledgeBase > 62](#_Toc136810041)

[4.5.10 < NetworkScanning.UserInterface.AdvancedScanningTechniques> 62](#_Toc136810042)

[4.5.11 < NetworkScanning.DatabasMaintainScanningTechniques > 64](#_Toc136810043)

[4.6 Report Generation 68](#_Toc136810044)

[4.6.1 < NetworkScanning.Report.GenerateComprehensiveReport > 68](#_Toc136810045)

[4.6.2 < NetworkScanning.Report.Generation.ScopeAndParameters > 71](#_Toc136810046)

[4.6.3 < NetworkScanning.Report.Compilation > 72](#_Toc136810047)

[4.6.4 < NetworkScanning.Report. GraphicalElements > 73](#_Toc136810048)

[4.6.5 < NetworkScanning.Report.CustomAnnotations > 73](#_Toc136810049)

[4.6.6 < NetworkScanning.Report.CustomAnnotations > 74](#_Toc136810050)

[4.7 Pause Scanning 74](#_Toc136810051)

[4.7.1 < NetworkScanning.PauseScanning > 74](#_Toc136810052)

[4.8 Restart Scanning 75](#_Toc136810053)

[4.9 Dashboard Updating 75](#_Toc136810054)

[4.9.1 < DashboardUpdating.RealTimeData > 75](#_Toc136810055)

[4.9.2 < DashboardUpdating.Customization > 76](#_Toc136810056)

[4.9.3 < DashboardUpdating.Widgets > 76](#_Toc136810057)

[4.9.4 <DashboardUpdating.AlertNotifications> 77](#_Toc136810058)

[4.9.5 <DashboardUpdating.DataVisualization > 77](#_Toc136810059)

[4.9.6 <DashboardUpdating.DataRefreshRate > 78](#_Toc136810060)

[4.9.7 <DashboardUpdating.DataVisualization > 78](#_Toc136810061)

[4.9.8 <DashboardUpdating.DataFilters > 78](#_Toc136810062)

[4.9.9 <DashboardUpdating.DataFilters > 79](#_Toc136810063)

[4.10 Data Aggregation 79](#_Toc136810064)

[4.10.1 <DataAggregation.Integration> 79](#_Toc136810065)

[4.10.2 <DataAggregation. Synchronization> 80](#_Toc136810066)

[4.10.3 <DataAggregation.Validation > 80](#_Toc136810067)

[4.10.4 <DataAggregation.Logging > 81](#_Toc136810068)

[4.11 Machine Learning-Based Vulnerability Detection 81](#_Toc136810069)

[4.11.1 < MachineLearning.Training > 81](#_Toc136810070)

[4.11.2 < MachineLearning.ModelRefinement > 82](#_Toc136810071)

[4.11.3 < MachineLearning.Classification > 82](#_Toc136810072)

[4.11.4 < MachineLearning.Accuracy > 83](#_Toc136810073)

[4.11.5 < MachineLearning.NetworkTrafficAnalysis > 83](#_Toc136810074)

[4.11.6 < MachineLearning.Integration> 84](#_Toc136810075)

[4.11.7 < MachineLearning.Alerts> 84](#_Toc136810076)

[4.11.8 < MachineLearning.VulnerabilityInformation > 85](#_Toc136810077)

[4.11.9 < MachineLearning.VulnerabilityPrioritization > 85](#_Toc136810078)

[4.11.10 < MachineLearning.VisualizationAndReporting > 85](#_Toc136810079)

[4.11.11 < MachineLearning.AlgoCustomization > 86](#_Toc136810080)

[4.12 Threat Intelligence Gathering 86](#_Toc136810081)

[4.12.1 < ThreatIntelligence.DataGatheringAndAnalysis > 86](#_Toc136810082)

[4.12.2 < ThreatIntelligence.Integration > 87](#_Toc136810083)

[4.12.3 < ThreatIntelligence.DataUpdate > 87](#_Toc136810084)

[4.12.4 < ThreatIntelligence.DataValidation > 88](#_Toc136810085)

[4.12.5 < ThreatIntelligence.DataStorage > 88](#_Toc136810086)

[4.12.6 < ThreatIntelligence.DataParsing > 89](#_Toc136810087)

[4.12.7 < ThreatIntelligence. DataNormalization > 89](#_Toc136810088)

[4.12.8 < ThreatIntelligence.DataAnalytics > 90](#_Toc136810089)

[4.12.9 < ThreatIntelligence.MachineLearningClassification > 90](#_Toc136810090)

[4.12.10 < ThreatIntelligence.NaturalLanguageProcessing> 91](#_Toc136810091)

[4.13 Notification and Alert Generation 91](#_Toc136810092)

[4.13.1 < NotificationAlertGeneration.RealTimeGeneration > 91](#_Toc136810093)

[4.13.2 < NotificationAlertGeneration.NetworkScanMonitoring > 92](#_Toc136810094)

[4.13.3 < NotificationAlertGeneration.NewVulnerabilityDetection > 92](#_Toc136810095)

[4.13.4 < NotificationAlertGeneration.SecurityBreachDetection > 93](#_Toc136810096)

[4.13.5 < NotificationAlertGeneration.SuspiciousActivityIdentification > 93](#_Toc136810097)

[4.13.6 < NotificationAlertGeneration. NotificationPreferences > 94](#_Toc136810098)

[4.13.7 < NotificationAlertGeneration.AdministratorActions > 94](#_Toc136810099)

[4.13.8 < NotificationAlertGeneration.HistoryArchive > 95](#_Toc136810100)

[4.13.9 < NotificationAlertGeneration.IncidentResponseIntegration > 95](#_Toc136810101)

[4.13.10 < NotificationAlertGeneration.AutomaticRemediation > 95](#_Toc136810102)

[4.13.11 < NotificationAlertGeneration.RecipientDelivery > 96](#_Toc136810103)

[4.14 Remediation Plan Checking 96](#_Toc136810104)

[4.14.1 < RemediationReview.CentralizedInterface > 97](#_Toc136810105)

[4.14.2 < RemediationReview.VulnerabilitySummary > 97](#_Toc136810106)

[4.14.3 < RemediationReview. StatusProgressTracking> 98](#_Toc136810107)

[4.14.4 < RemediationReview. StatusProgressTracking> 98](#_Toc136810108)

[4.15 SystemUpdate 99](#_Toc136810109)

[4.15.1 < SystemUpdates.DownloadInstall > 99](#_Toc136810110)

[4.15.2 < SystemUpdates.AutomaticUpdates > 99](#_Toc136810111)

[4.15.3 < SystemUpdates.UpdateNotifications> 100](#_Toc136810112)

[4.15.4 < SystemUpdates.VersionControl> 100](#_Toc136810113)

[4.15.5 < SystemUpdates.CompatibilityChecks > 101](#_Toc136810114)

[4.15.6 < SystemUpdates.ScheduledInstallations > 101](#_Toc136810115)

[4.15.7 < SystemUpdates.UpdateLog > 102](#_Toc136810116)

[4.15.8 < SystemUpdates.RollbackCapabilities > 102](#_Toc136810117)

[4.15.9 < SystemUpdates.SecureUpdateMechanisms > 103](#_Toc136810118)

[4.16 ComplianceChecking 103](#_Toc136810119)

[4.16.1 < ComplianceChecking.Analysis > 103](#_Toc136810120)

[4.16.2 < ComplianceChecking.DetailedReports > 104](#_Toc136810121)

[5. Non-Functional Requirements 104](#_Toc136810122)

[5.1 Reliability 104](#_Toc136810123)

[5.2 Usability 104](#_Toc136810124)

[5.3 Performance 105](#_Toc136810125)

[5.4 Security 105](#_Toc136810126)

[5.5 Availability 105](#_Toc136810127)

[5.6 Integrity 105](#_Toc136810128)

[5.7 Scalability 105](#_Toc136810129)

[6. External Interface Requirements 106](#_Toc136810130)

[6.1 User Interfaces Requirements 106](#_Toc136810131)

[6.2 Software interfaces 106](#_Toc136810132)

[6.2.1 SI-1: Integration with Threat Intelligence API 106](#_Toc136810133)

[6.2.2 SI-2: Integration with Reporting Module 106](#_Toc136810134)

[6.3 Hardware interfaces 107](#_Toc136810135)

[6.3.1 HI-1: Network Scanning Hardware 107](#_Toc136810136)

[6.4 Communications interfaces 107](#_Toc136810137)

[6.4.1 CI-1: Email Notifications 107](#_Toc136810138)

[6.4.2 CI-2: SMS Notifications 107](#_Toc136810139)

[6.4.3 CI-3: API Communication 107](#_Toc136810140)

[7. References 107](#_Toc136810141)

[7.1 Book 107](#_Toc136810142)

[7.2 Journal Article 108](#_Toc136810143)

[1.1 Conference Proceeding 108](#_Toc136810144)

[1.2 Website 108](#_Toc136810145)

# 

# Introduction

**Software Requirements Specification (SRS)** for **Cyberfy** providing an overview of the entire **SRS**. It includes the purpose, scope, modules and overview of the **SRS**.

## Purpose

This SRS document contains functional and non-functional requirements of Cyberfy, a desktop application designed especially for Cyber Specialists, Organizations and Government IT Sectors. The purpose of this document is to specify the Functional and Non-Functional requirements for Cyberfy, a comprehensive cybersecurity solution. Cyberfy is designed to cater to various types of readers, including but not limited to system administrators, security analysts, compliance officers, and IT managers. This document aims to provide a clear understanding of the functionalities and features of Cyberfy, enabling readers to effectively assess its suitability for their organization's cybersecurity needs. Additionally, it serves as a reference for development teams, allowing them to implement the specified requirements accurately and efficiently.

## Scope

The software being specified is Cyberfy, a comprehensive cybersecurity solution aimed at meeting the user and project goals of organizations seeking robust protection against cyber threats. Cyberfy is designed to enhance the security posture of an organization by providing a range of advanced features and functions. These include real-time threat detection and response, vulnerability assessment and management, network monitoring, data encryption, access control, and incident management. The software's purpose is to safeguard critical assets, prevent unauthorized access and data breaches, ensure regulatory compliance, and enable organizations to proactively manage and mitigate cybersecurity risks. By incorporating these major features, Cyberfy aims to provide a holistic and effective cybersecurity solution to help organizations achieve their project objectives of establishing a secure and resilient IT infrastructure.

## Modules

### 1.3.1 Module 1: Threat Detection and Response

FE-1: Real-time monitoring and detection of cyber threats across the network.

FE-2: Immediate alert notifications for identified threats and potential security breaches.

FE-3: Automated incident response actions to mitigate and contain cyber attacks.

FE-4: Forensic analysis and reporting for investigating security incidents.

FE-5: Integration with threat intelligence feeds for proactive threat hunting.

### 1.3.2 Module 2: Vulnerability Assessment and Management

FE-1: Regular scanning and identification of vulnerabilities in the IT infrastructure.

FE-2: Prioritization and risk assessment of identified vulnerabilities.

FE-3: Remediation recommendations and guidance for vulnerability patching.

FE-4: Tracking and monitoring of vulnerability management progress.

FE-5: Compliance checks against industry standards and regulatory requirements.

### 1.3.3 Module 3: Network Monitoring and Analysis

FE-1: Real-time monitoring of network traffic and activity.

FE-2: Detection and analysis of network anomalies and suspicious behavior.

FE-3: Identification of unauthorized devices and connections.

FE-4: Traffic flow analysis for performance optimization and anomaly detection.

FE-5: Visualization and reporting of network performance metrics.

### 1.3.4 Module 4: Access Control and Authentication

FE-1: User authentication and authorization mechanisms.

FE-2: Role-based access control for user privileges and permissions.

FE-3: Multi-factor authentication options for enhanced security.

FE-4: Audit logs and monitoring of user access and activity.

FE-5: Integration with identity and access management systems.

### 1.3.5 Module 5: Data Encryption and Protection

FE-1: Encryption of sensitive data at rest and in transit.

FE-2: Key management and secure storage of encryption keys.

FE-3: Data loss prevention mechanisms and policies.

FE-4: Secure file transfer and sharing capabilities.

FE-5: Compliance with data protection regulations.

### 1.3.6 Module 6: Incident Management and Response

FE-1: Incident ticketing and tracking system.

FE-2: Incident prioritization and escalation workflows.

FE-3: Collaboration and communication tools for incident response teams.

FE-4: Post-incident analysis and lessons learned documentation.

FE-5: Continuous improvement of incident response processes.

## Overview

The SRS document for Cyberfy provides a comprehensive description of the product and its functionalities. It outlines the types of users involved in interacting with the system and their corresponding interactions and system responses. Additionally, the document discusses the implementation technologies employed in the development of Cyberfy.

The SRS document is organized into several sections to facilitate understanding and navigation. It includes use case diagrams, which depict the various interactions between users and the system, along with detailed descriptions of each use case. The document also outlines the functional requirements related to different modules of Cyberfy, specifying the desired behaviors and capabilities of the system. Furthermore, non-functional requirements, such as performance, security, and usability considerations, are addressed in the document.

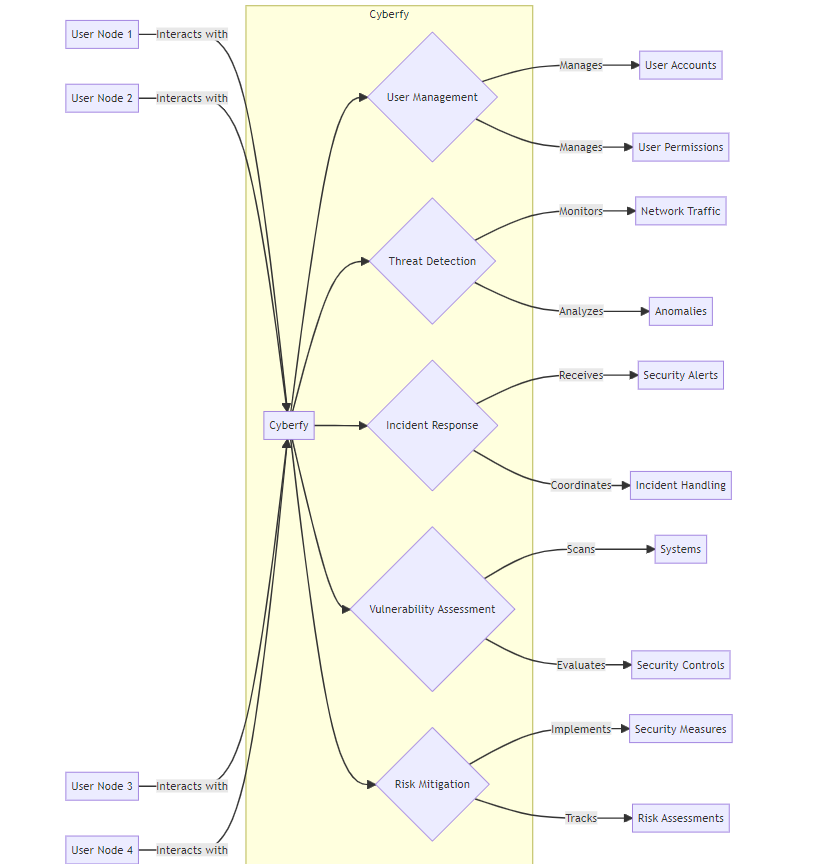
By providing a clear and structured layout, the SRS document ensures that stakeholders and development teams can easily grasp the purpose, functionalities, and technical aspects of Cyberfy, enabling effective communication and collaboration throughout the development process.

# Overall Description

This section presents a high-level overview of the product and the environment in which it will be used, the anticipated users, and known constraints, assumptions, and dependencies.

## Product Perspective

The Cyberfy system is a standalone product that operates as a comprehensive cybersecurity management platform. It is not dependent on any specific external systems or applications, but it can integrate with external vulnerability scanners, project management tools, compliance assessment services, and other security-related systems to enhance its capabilities. Cyberfy is designed to be scalable and adaptable, catering to the needs of various organizations regardless of their size or industry. It aims to revolutionize cybersecurity practices by providing a centralized and user-friendly solution that addresses vulnerability assessment, remediation planning, compliance checking, and security governance in an efficient and effective manner.



## User classes and characteristics

|  |  |
| --- | --- |
| User Class | Description |
| System Admin | Responsible for managing and configuring the Cyberfy system. |
| Security Analyst | Utilizes the Cyberfy system to perform threat detection, incident response, vulnerability assessment, etc. |
| Network Engineer | Interacts with Cyberfy to monitor and manage network traffic, security controls, and implement security measures. |
| IT Administrator | Uses Cyberfy to manage user accounts, permissions, and ensure overall system security. |
| Data Analyst | Utilizes Cyberfy's modules to analyze data, assess risks, and identify vulnerabilities. |
| Compliance Officer | Ensures that Cyberfy adheres to relevant regulations and industry standards. |
| System User | End-users of systems protected by Cyberfy, such as employees using computers, laptops, or lab equipment. |

## Operating Environment

**OE-1:** The software shall be compatible with popular web browsers, including but not limited to Google Chrome, Mozilla Firefox, Microsoft Edge, and Apple Safari, with their latest stable versions.

**OE-2:** Cyberfy shall support major operating systems such as Windows (versions 7 and above), macOS (latest version), and Linux (Ubuntu, Fedora, etc.) for both client-side and server-side deployment.

**OE-3:** The software should be able to run on various hardware platforms, including desktop computers, laptops, servers, and virtual machines.

**OE-4:** The geographical locations of the users, servers, and databases can be distributed globally, but Cyberfy is designed to function seamlessly over the internet.

**OE-5:** The software requires a stable internet connection to access its features and communicate with external systems and databases.

**OE-6:** Cyberfy can integrate with different database management systems, such as MySQL, PostgreSQL, Oracle, and MongoDB, depending on the specific requirements and configurations of the deployment.

**OE-7:** Organizations hosting the Cyberfy system are responsible for providing suitable infrastructure, including server hardware, storage systems, and backup solutions, to ensure optimal performance and data security.

**OE-8:** The software may require periodic updates and patches to stay compatible with the evolving operating systems, web browsers, and related technologies.

## Design and Implementation Constraints

**CON-1:** The system shall utilize MongoDB as the primary database for storing and managing data. MongoDB is chosen due to its flexibility, scalability, and ability to handle large volumes of data efficiently.

**CON-2:** Cyberfy shall be developed using the Python programming language as the backend framework. Python offers a rich set of libraries and frameworks that facilitate rapid development, scalability, and integration with other technologies.

**CON-3:** The frontend of Cyberfy shall be implemented using modern web development technologies, such as React.js or Angular.js. These frameworks provide a modular and maintainable approach to building user interfaces and enable seamless integration with the backend services.

**CON-4:** Cyberfy shall adhere to industry-standard security practices and protocols, such as SSL/TLS encryption for secure data transmission and authentication mechanisms to ensure authorized access to the system.

**CON-5:** The system shall be deployed using cloud infrastructure, such as Amazon Web Services (AWS) or Microsoft Azure, to leverage their scalability, reliability, and availability features. This constraint ensures that Cyberfy can handle increased user loads and maintain high uptime.

**CON-6:** Cyberfy shall follow responsive design principles to ensure optimal usability across various devices and screen sizes, including desktop computers, laptops, tablets, and smartphones.

**CON-7:** The system shall comply with relevant privacy and data protection regulations, such as GDPR (General Data Protection Regulation) and CCPA (California Consumer Privacy Act), to safeguard user data and maintain compliance with legal requirements.

# Requirement Identifying Technique

## Use Case Diagram

A picture containing line, diagram, plot, text

Description automatically generated

## Event Response Tables

* User initiates a request for network scanning.
* User initiates a request for threat intelligence gathering.
* User initiates a request for machine learning-based vulnerability detection.
* User initiates a request for remediation plan generation.
* User initiates a request for compliance check initiation.
* User initiates a request for notification and alert generation.
* User requests security threat notifications and alerts.
* User requests remediation progress notifications and alerts.
* User requests system status notifications and alerts.
* User initiates a request for report generation.
* User requests the generation of a specific report type.
* User requests customization of a specific report.
* User requests sharing of a specific report with designated recipients.
* User requests archiving or deletion of a specific report based on retention period and  
  deletion method

### Network Scanning Initiation

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ID | Event | Data Element | System State | Exception Condition | System Response (In case of Yes) | System Response (In case of No) | System State |
| 3 | Network Scanning Initiation | Scan Parameters | Network scan inactive | Insufficient permissions | Start network scanning process | Show error message: "Insufficient permissions" | Network scan active |

### Threat Intelligence Gathering

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ID | Event | Data Element | System State | Exception Condition | System Response (In case of Yes) | System Response (In case of No) | System State |
| 4 | Threat Intelligence Gathering | Threat Sources, Update Frequency | Threat intel not gathered | Data source unavailable or error | Gather and update threat intelligence | Show error message: "Data source unavailable or error" | Threat intel gathered |

### Machine Learning-based Vulnerability Detection

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ID | Event | Data Element | System State | Exception Condition | System Response (In case of Yes) | System Response (In case of No) | System State |
| 5 | Machine Learning-based Vulnerability Detection | Collected Vulnerability Data | ML-based detection inactive | Insufficient training data | Perform ML-based vulnerability detection | Show error message: "Insufficient training data" | ML-based detection active |

### Remediation Plan Generation

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ID | Event | Data Element | System State | Exception Condition | System Response (In case of Yes) | System Response (In case of No) | System State |
| 6 | Remediation Plan Generation | Vulnerability Data | Remediation not generated | No vulnerabilities found | Generate remediation plan | Show message: "No vulnerabilities found" | Remediation plan generated |

### Compliance Check Initiation

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ID | Event | Data Element | System State | Exception Condition | System Response (In case of Yes) | System Response (In case of No) | System State |
| 7 | Compliance Check Initiation | Compliance Standards | Compliance check inactive | Compliance standards unavailable | Initiate compliance check | Show error message: "Compliance standards unavailable" | Compliance check active |

### Notification and Alert Generation

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ID | Event | Data Element | System State | Exception Condition | System Response (In case of Yes) | System Response (In case of No) | System State |
| 9.1 | Notification and Alert Generation | Security Threat Data | Normal system operation state | No security threat data present | Generate notification and alert for detected security threat | Show message: "No security threat detected" | Normal system operation state |
| 9.2 | Notification and Alert Generation | Remediation Progress Data | Normal system operation state | No progress data available | Generate notification and alert for remediation progress update | Show message: "No progress data available" | Normal system operation state |
| 9.3 | Notification and Alert Generation | System Status Data | Normal system operation state | System status is not optimal | Generate notification and alert for sub-optimal system status | Show message: "System status is optimal" | Normal system operation state |

### Report Generation

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | Event | Data Element | System State | Exception Condition | System Response (Yes) | System Response (No) |
| 10.1 | Report generation | Report type (e.g. vulnerability report, compliance report) | Report generator module initialized | Report data not available | Generate and display report | Display error message indicating that report data is not available |
| 10.2 | Report customization | Report type, selected fields/columns, report filters | Report customization module initialized | Invalid or missing report type, fields, or filters | Generate and display customized report | Display error message indicating that report customization failed |
| 10.3 | Report sharing | Report type, recipient(s), delivery method | Report sharing module initialized | Invalid or missing report type, recipient(s), or method | Share report with designated recipient(s) via designated method | Display error message indicating that report sharing failed |
| 4 | Report archiving/deletion | Report type, retention period, deletion method | Report archive/deletion module initialized | Invalid or missing report type, retention period, or method | Archive/delete reports based on designated retention period and deletion method | Display error message indicating that report archive/deletion failed |

# 

## Detail Use Cases

### UC-1 : User Account Creation

|  |  |
| --- | --- |
| Category | Details |
| Use Case ID | UC-1 |
| Use Case Name | User Account Creation |
| Created By | Sidra Saleem |
| Actors | New user, system administrator |
| Description | Allows new users to create accounts and assign appropriate access levels. |
| Trigger | New user decides to create an account on the system. |
| Preconditions | New user has access to the system's registration page. |
| Postconditions | A new user account is created, and the user is assigned the appropriate access level. |
| Normal Flow | 1. New user navigates to the registration page.  2. New user enters required information (e.g., username, password, emai, rolel).  3. System validates the provided information.  4. System displays an error message in case of invalid information (see 1.1)  5. System creates a new user account and assigns the appropriate access level.  6. System sends a confirmation email to the user. (see 1.0. E1)  7. User confirms the account by clicking on the link in the email. |
| Alternative Flows | Alternative Flow 1.1 – Invalid Information:  1. System detects that the user entered invalid information during registration.  2. System displays an error message, prompting the user to correct the information.  3. User corrects the information and resubmits the registration form.  4. Return to step 3 of the Normal Flow. |
| Exceptions | E1 - Technical issue  System is unable to send a confirmation email due to technical issues. |
| Includes | UC-2 |
| Business Rules | BR-1. Usernames must be unique.  BR-2. Passwords must meet complexity requirements and length.  BR-3. Email addresses must be valid and unique. |
| Special Requirements/ | 1. The system must enforce password complexity requirements.  2. The system must send confirmation emails to users during the registration process.  3. The system must provide a way for users to reset their passwords if they forget them.  4. The system must securely store user credentials.  5. The system must provide options for multi-factor authentication, such as SMS or email verification. |

### User Authentication

|  |  |
| --- | --- |
| Category | Details |
| Use Case ID | UC-2 |
| Use Case Name | User Authentication |
| Created By | Urooj Fatima |
| Actors | Authenticated user, system administrator |
| Description | Verify user credentials and grant access to the system based on the provided authentication. |
| Trigger | User attempts to log in to the system. |
| Preconditions | User has a valid account in the system. |
| Postconditions | User is either granted or denied access to the system based on the provided authentication. |
| Normal Flow | 1. User enters their credentials (username and password). |
|  | 2. System verifies the provided credentials against the user database. |
|  | 3. System sends a verification code to the user’s registered email or phone number. |
|  | 4. User enters the verification code. |
|  | 3. If the code is valid, the system grants access to the user. |
|  | 4. If the credentials are invalid, the system denies access and displays an error message. |
| Alternative Flows | Alternative Flow 2.1 - Forget Password |
|  | 1. User enters their registered email. |
|  | 2. System sends the password reset link on the registered email. |
|  | 3. User clicks the link and redirects to the password reset page. |
|  | 4. User enters the new password according to the rules/constraints given . |
|  | 5. System updates the password. |
| Exceptions | 2.0.E1 - Invalid email  1. User forgets their password and requests a password reset. |
| Includes | N/A |
| Business Rules | BR-1. Passwords must meet minimum complexity requirements. |
|  | BR-2. Users must have a valid account in the system to access the system. |
| Special Requirements/Notes | 1. Implement multi-factor authentication for enhanced security. |
|  | 2. Log all authentication attempts, including failed attempts, for auditing purposes. |

### User Account Management

|  |  |
| --- | --- |
| Category | Details |
| Use Case ID | UC-3 |
| Use Case Name | User Account Management |
| Created By | Sidra Saleem |
| Actors | System administrator, user |
| Description | Manage user accounts, including account creation, modification, suspension, and deletion, as well as password management. |
| Trigger | A request to create, modify, suspend, or delete a user account or to reset a password. |
| Preconditions | 1. The organization has a user account management system in place. |
|  | 2. System administrator has access to the user account management system. |
| Postconditions | The requested user account action is completed, and the user account is in the desired state. |
| Normal Flow | 1. A request to create, modify, suspend, or delete a user account or to reset a password is received. |
|  | 2. System administrator verifies the request and determines the appropriate action. |
|  | 3. System administrator performs the action in the user account management system. |
|  | 4. System confirms the completion of the action, and the user account is in the desired state. |
| Alternative Flows | None. |
| Exceptions | 3.0.E1 – Limited access  1. System administrator does not have the necessary permissions to perform the action. |
|  | 3.1.E1 – System Failure  2. User account management system failure. |
| Includes | N/A |
| Business Rules | BR-1. User account actions should adhere to the organization's policies and procedures. |
|  | BR-2. Ensure proper authentication and authorization before performing any user account actions. |
| Special Requirements/Notes | 1. Implement a secure password policy, including periodic password changes and complexity requirements. |
|  | 2. Continuously monitor and evaluate the effectiveness of the user account management system, making improvements as needed. |
|  | 3. Provide training and support to the IT department on how to properly manage user accounts. |

### System Update

|  |  |
| --- | --- |
| Category | Details |
| Use Case ID | UC-4 |
| Use Case Name | System Update |
| Created By | Sidra Saleem |
| Actors | Security analyst, system administrator |
| Description | Update the organization's systems, including applications, operating systems, and firmware, to address security vulnerabilities and improve performance. |
| Trigger | A new update or patch is released, or a scheduled maintenance window is reached. |
| Preconditions | 1. The organization has a system update policy and procedure in place. |
|  | 2. System administrator has access to the system update tools and resources. |
| Postconditions | The requested system update is completed, and the system is up-to-date and secure. |
| Normal Flow | 1. Security analyst identifies the need for a system update. |
|  | 2. System administrator reviews the update details and plans the update. |
|  | 3. System administrator performs the update during the maintenance window. |
|  | 4. System confirms the completion of the update, and the system is up-to-date and secure. |
| Alternative Flows | None. |
| Exceptions | 4.0.E1 – Failure  1. System update fails or causes system instability. |
|  | 4.1.E1 – Limited Access  2. System administrator does not have the necessary permissions to perform the update. |
| Includes | N/A |
| Business Rules | BR-1. System updates should adhere to the organization's policies and procedures. |
|  | BR-2. Ensure proper testing and evaluation of updates before deployment. |
| Special Requirements/Notes | 1. Implement a regular system update schedule to maintain security and performance. |
|  | 2. Continuously monitor and evaluate the effectiveness of the system update process, making improvements as needed. |
|  | 3. Provide training and support to the IT department on how to properly update systems. |

### Dashboard Updating

|  |  |
| --- | --- |
| Category | Details |
| Use Case ID | UC-5 |
| Use Case Name | Dashboard Updating |
| Created By | Urooj Fatima |
| Actors | Security analyst, system administrator |
| Description | Update the organization's security dashboard with current security metrics, threat intelligence, and incident data. |
| Trigger | Periodic update or a significant change in the security landscape, incident, or vulnerability. |
| Preconditions | 1. A security dashboard is in place and accessible to authorized personnel. |
|  | 2. Security analyst and system administrator have access to relevant data and metrics. |
| Postconditions | The security dashboard is updated with the latest information and reflects the current security status. |
| Normal Flow | 1. Security analyst collects current security metrics, threat intelligence, and incident data. |
|  | 2. Security analyst analyzes the data and identifies trends, patterns, and areas of concern. |
|  | 3. Security analyst updates the security dashboard with the new information. |
|  | 4. System administrator reviews the updated dashboard and takes appropriate actions if needed. |
| Alternative Flows | None. |
| Exceptions | 5.0.E1 – Technical issues  1a. Unavailability of data or metrics.  2b. Dashboard access issues or technical problems. |
| Includes | N/A |
| Business Rules | BR-1. Dashboard updates must adhere to the organization's policies and procedures. |
|  | BR-2. Access to the security dashboard should be restricted to authorized personnel. |
| Special Requirements/Notes | 1. Ensure the dashboard provides accurate, relevant, and up-to-date information. |
|  | 2. Continuously monitor and evaluate the dashboard's effectiveness and make improvements as needed. |
|  | 3. Provide training and support to the IT department on how to use and interpret the dashboard. |

# Functional Requirements

## User Account Creation

### < Register.User.Internet >

|  |  |
| --- | --- |
| Identifier | 1.1 |
| Title | Register.User.Internet |
| Requirement | The user shall have an internet connection to register. |
| Source | Sidra, Urooj |
| Rationale | In order to register, the user must have internet on their desktop. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

#### < Register.User.NoInternet >

|  |  |
| --- | --- |
| Identifier | 1.2 |
| Title | <Register.User.NoInternet> |
| Requirement | If the user does not have an internet connection to register. The system displays an error message informing the user about the requirement for an internet connection to proceed with the registration.  The error message suggests the user to check their internet connection and try again.  If the user attempts to register without an internet connection again, the system continues to display the same error message.  Once the user establishes an internet connection, they can retry the registration process successfully. |
| Source | Sidra, Urooj |
| Rationale | To address the scenario where the user lacks internet connectivity during the registration process. |
| Business Rule | N/A |
| Dependencies | 4.1.1 |
| Priority | High |
| Remedy | The system shall prompt the user to connect to the internet in order to proceed with the registration process. |

### < Register.Administrator.Validation >

|  |  |
| --- | --- |
| Identifier | 1.3 |
| Title | <Register.Administrator.Validation> |
| Requirement | The system shall validate the format and integrity of the entered username, password, and email address to ensure they meet the required criteria. |
| Source | Sidra, Urooj |
| Rationale | To ensure the entered credentials and contact information are in the correct format and meet the system's criteria. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

#### < Register.Administrator.NotValid >

|  |  |
| --- | --- |
| Identifier | 1.3.1 |
| Title | <Register.Administrator.NotValid> |
| Requirement | If the system detects that the entered username, password, or email address does not meet the required criteria.  The system displays an error message indicating that the entered credentials are not valid and do not meet the required format.  The error message provides specific details about the required format for each field (username, password, and email address).  The error message guides the user on how to correct the entered credentials to meet the required criteria.  The system allows the user to edit the credentials and attempt registration again.  If the user continues to enter invalid credentials, the system continues to display the same error message with the required format guidelines.  Once the user enters valid credentials that meet the required criteria, the system proceeds with the registration process successfully. |
| Source | Sidra, Urooj |
| Rationale | To ensure the entered credentials and contact information are in the correct format and meet the system's criteria. |
| Business Rule | N/A |
| Dependencies | 4.1.3 |
| Priority | High |

### <Register.Administrator.UsernameUniqueness>

|  |  |
| --- | --- |
| Identifier | 1.4 |
| Title | <Register.Administrator.UsernameUniqueness> |
| Requirement | The system shall check the uniqueness of the entered username to avoid duplicate user accounts. |
| Source | Sidra, Urooj |
| Rationale | To ensure that each user has a unique username within the system to avoid conflicts and duplication. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

#### <Register.Administrator.UsernameNotUnique>

|  |  |
| --- | --- |
| Identifier | 4.1.4.1 |
| Title | <Register.Administrator.UsernameNotUnique> |
| Requirement | The system shall handle the scenario where the entered username is not unique and already exists in the system. |
| Source | Sidra, Urooj |
| Rationale | To prevent users from creating duplicate user accounts with the same username, which could lead to confusion and data integrity issues. |
| Business Rule | N/A |
| Dependencies | 4.1.4 |
| Priority | High |

### <Register.Administrator.PasswordComplexity>

|  |  |
| --- | --- |
| Identifier | 1.5 |
| Title | <Register.Administrator.PasswordComplexity> |
| Requirement | The system shall enforce password complexity rules, such as a minimum length, a combination of alphanumeric characters, and the inclusion of special symbols. |
| Source | Sidra, Urooj |
| Rationale | To enhance the security of user accounts by enforcing strong password requirements. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

#### <Register.Administrator.PasswordNotComplex>

|  |  |
| --- | --- |
| Identifier | 4.1.5.1 |
| Title | <Register.Administrator.PasswordNotComplex> |
| Requirement | The system evaluates the entered password to determine if it meets the required complexity rules.  If the entered password is found to be not complex enough, the system displays an error message indicating that the password does not meet the required complexity criteria.  The error message provides information on the specific complexity rules that were not met, such as minimum length, character types, or inclusion of special symbols.  The user is prompted to enter a new password that adheres to the complexity requirements.  The system may provide guidelines or suggestions on creating a strong password.  The user is encouraged to choose a password that combines alphanumeric characters, includes special symbols, and is of sufficient length.  Once a password that meets the complexity rules is entered, the system proceeds with the registration process successfully. |
| Source | Sidra, Urooj |
| Rationale | To ensure that user accounts are protected with strong passwords that meet the system's security standards. |
| Business Rule | N/A |
| Dependencies | FR4.1.5 |
| Priority | High |

### <Register.Administrator.PasswordStorage>

|  |  |
| --- | --- |
| Identifier | 4.1.6 |
| Title | <Register.Administrator.PasswordStorage> |
| Requirement | The system shall securely store the user's password by encrypting or hashing it. |
| Source | Sidra, Urooj |
| Rationale | To ensure the confidentiality and protection of user passwords. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

### <Register.Administrator.ConfirmationEmail>

|  |  |
| --- | --- |
| Identifier | 1.7 |
| Title | <Register.Administrator.ConfirmationEmail> |
| Requirement | The system shall send a confirmation email to the user's provided email address to verify its authenticity. |
| Source | Sidra, Urooj |
| Rationale | To ensure the authenticity of the user's email address. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

#### <Register.Administrator.ConfirmationEmailNotSent>

|  |  |
| --- | --- |
| Identifier | 4.1.7.1 |
| Title | <Register.Administrator.ConfirmationEmailNotSent> |
| Requirement | If the confirmation email fails to send, the system detects this failure and handles it accordingly.  The system logs the error or failure for monitoring and troubleshooting purposes.  The user is notified about the failure to send the confirmation email through an error message or notification.  The error message provides instructions to the user on possible solutions or actions to resolve the issue, such as checking the provided email address, checking spam folders, or retrying the registration process.  The user is prompted to verify their email address manually by following alternative procedures, such as contacting customer support or providing additional information for verification.  The system provides support channels or contacts information for the user to seek assistance in case of issues with the confirmation email.  The user can request a re-sending of the confirmation email if the initial attempt fails. |
| Source | Sidra, Urooj |
| Rationale | To ensure that the user receives the confirmation email for verifying the authenticity of their email address. |
| Business Rule | N/A |
| Dependencies | 4.1.7 |
| Priority | High |

### <Register.Administrator.ActivationLink>

|  |  |
| --- | --- |
| Identifier | 1.8 |
| Title | <Register.Administrator.ActivationLink> |
| Requirement | The system shall generate a unique activation link or code in the confirmation email for users to activate their accounts. |
| Source | Sidra, Urooj |
| Rationale | To provide users with a secure and unique method to activate their accounts. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

#### <Register.Administrator.ActivationLinkError>

|  |  |
| --- | --- |
| Identifier | 1.8.1 |
| Title | <Register.Administrator.ActivationLinkError> |
| Requirement | In case of errors or issues related to the activation link or code, the system shall handle them appropriately.  The system shall log any errors or failures related to the activation process for monitoring and troubleshooting purposes.  The user is notified about the error or issue with the activation link or code through an error message or notification.  The error message provides instructions to the user on possible solutions or actions to resolve the issue, such as contacting customer support, requesting a new activation link or code, or retrying the activation process.  The system provides support channels or contact information for the user to seek assistance in case of issues with the activation link or code.  The user can request a re-sending of the activation link or code if the initial one encounters an error. |
| Source | Sidra, Urooj |
| Rationale | To ensure a smooth and error-free activation process for user accounts. |
| Business Rule | N/A |
| Dependencies | 4.1.8 |
| Priority | High |

### <Register.Administrator.AccountActivation>

|  |  |
| --- | --- |
| Identifier | 1.9 |
| Title | <Register.Administrator.AccountActivation> |
| Requirement | The system shall activate the user's account upon successful verification of the activation link or code. |
| Source | Sidra, Urooj |
| Rationale | To allow users to access their accounts after successfully verifying their email address. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

## User Authentication

### < Login.User.LoginForm>

|  |  |
| --- | --- |
| Identifier | 2.1 |
| Title | <Login.User.LoginForm> |
| Requirement | The system shall provide a login form that allows users to enter their username and password. |
| Source | Sidra, Urooj |
| Rationale | To allow users to authenticate themselves and access their accounts. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

### <Login.User.CredentialsValidation>

|  |  |
| --- | --- |
| Identifier | 2.2 |
| Title | <Login.User.CredentialsValidation> |
| Requirement | The system shall validate the entered username and password against the stored user credentials. |
| Source | Sidra, Urooj |
| Rationale | To ensure the authenticity of the user's login credentials. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

#### <Login.User.CredentialsInvalid>

|  |  |
| --- | --- |
| Identifier | 2.2.1 |
| Title | <Login.User.CredentialsInvalid> |
| Requirement | If the entered username and password do not match the stored user credentials. The system shall display an error message indicating that the entered username and password combination is invalid. The user will be prompted to re-enter their credentials or initiate the password recovery process if needed. |
| Source | Sidra, Urooj |
| Rationale | To provide appropriate feedback to the user when invalid login credentials are entered. |
| Business Rule | N/A |
| Dependencies | 2.2 |
| Priority | High |

### <Login.User.AccountAccess>

|  |  |
| --- | --- |
| Identifier | 2.3 |
| Title | <Login.User.AccountAccess> |
| Requirement | The system shall grant access to the user's account if the entered username and password are valid. |
| Source | Sidra, Urooj |
| Rationale | To allow authenticated users to access their accounts and perform authorized actions. |
| Business Rule | N/A |
| Dependencies | 2.2 |
| Priority | High |

### <Login.User.InvalidCredentialsError>

|  |  |
| --- | --- |
| Identifier | 2.4 |
| Title | <Login.User.InvalidCredentialsError> |
| Requirement | If the entered username and password are invalid, the system shall display an appropriate error message indicating that the login credentials are incorrect. |
| Source | Sidra, Urooj |
| Rationale | To provide users with clear feedback when they enter incorrect login credentials, allowing them to troubleshoot and retry if necessary. |
| Business Rule | N/A |
| Dependencies | 2.3 |
| Priority | High |

### <Login.User.PasswordValidation>

|  |  |
| --- | --- |
| Identifier | 2.5 |
| Title | <Login.User.PasswordValidation> |
| Requirement | The system shall handle password validation securely, ensuring that passwords are not stored in plain text. Implement secure password hashing and storage techniques, such as using salted hashes or strong encryption algorithms, to ensure that passwords are not stored in plain text. Follow industry best practices and security guidelines for password handling and storage. Regularly review and update password security measures to address emerging threats and vulnerabilities. |
| Source | Sidra, Urooj |
| Rationale | To protect user passwords from unauthorized access and potential security breaches by securely handling and storing password information. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

### <Login.User.PasswordEncryption>

|  |  |
| --- | --- |
| Identifier | 2.6 |
| Title | <Login.User.PasswordEncryption> |
| Requirement | The system shall support password encryption or hashing techniques to protect user credentials. Implement industry-standard encryption or hashing algorithms, such as bcrypt or SHA-256, to securely encrypt or hash user passwords. Use appropriate salt values to further enhance the security of the password storage. Regularly update and review encryption or hashing techniques to ensure they align with current security best practices. Conduct regular security audits and penetration tests to identify any potential vulnerabilities in the password encryption or hashing implementation. |
| Source | Sidra, Urooj |
| Rationale | To enhance the security of user credentials by encrypting or hashing passwords, making them more resistant to unauthorized access. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

### <Login.User.AccountLockout>

|  |  |
| --- | --- |
| Identifier | 2.7 |
| Title | <Login.User.AccountLockout> |
| Requirement | The system shall enforce security measures, such as account lockouts after multiple failed login attempts, to prevent brute-force attacks. Implement a mechanism that tracks the number of failed login attempts for each user. Set a threshold for failed attempts, after which the user's account is locked. Upon reaching the threshold, lock the user's account for a specific duration, such as 15 minutes, to deter brute-force attacks. Display an appropriate error message indicating the account lockout. Provide a password reset mechanism for locked-out users to regain access to their accounts. Regularly monitor and review the account lockout mechanism to ensure its effectiveness and adjust the lockout threshold and duration if necessary. |
| Source | Sidra, Urooj |
| Rationale | To enhance the security of user accounts by preventing unauthorized access through brute-force attacks. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

### <Login.User.SecureCommunication>

|  |  |
| --- | --- |
| Identifier | 2.8 |
| Title | <Login.User.SecureCommunication> |
| Requirement | The system shall implement secure communication protocols, such as HTTPS, for transmitting login credentials over the network. Implement secure communication protocols, such as HTTPS, for transmitting login credentials over the network. HTTPS provides encryption and authentication mechanisms to protect the confidentiality and integrity of data exchanged between the user's device and the system. Use SSL/TLS certificates to establish a secure connection between the client and the server. Ensure that the system enforces the use of HTTPS for all login-related communications, including the submission of login credentials. Regularly update and maintain the SSL/TLS configuration to stay compliant with industry standards and address any security vulnerabilities. Perform security testing and monitoring to detect and mitigate any potential weaknesses in the secure communication implementation. |
| Source | Sidra, Urooj |
| Rationale | To ensure the confidentiality and integrity of login credentials during transmission over the network. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

### <Login.User.LoginAttemptsLogging>

|  |  |
| --- | --- |
| Identifier | 2.9 |
| Title | <Login.User.LoginAttemptsLogging> |
| Requirement | The system shall log successful and failed login attempts for auditing and security purposes. Implement a logging mechanism that records successful and failed login attempts. Each login attempt should be logged with relevant information such as the user's username, timestamp, IP address, and the result (success or failure). Ensure that the logs are securely stored and protected from unauthorized access. Regularly review the login logs for any suspicious activity or patterns that may indicate unauthorized access attempts. Implement security measures, such as account lockouts or additional verification steps, based on the number of failed login attempts within a specified timeframe. Maintain the logs for an appropriate duration according to regulatory requirements and organizational policies. |
| Source | Sidra, Urooj |
| Rationale | To provide an audit trail and enhance security by logging login activities. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

### <Login.User.UnauthorizedAccessProtection>

|  |  |
| --- | --- |
| Identifier | 2.10 |
| Title | <Login.User.UnauthorizedAccessProtection> |
| Requirement | The system shall have mechanisms in place to prevent unauthorized access to user accounts and protect against account hijacking. Implement robust security measures to prevent unauthorized access to user accounts and protect against account hijacking. This may include measures such as strong authentication mechanisms (e.g., multi-factor authentication), secure session management, and secure password policies. Regularly update and patch the system to address any security vulnerabilities. Implement intrusion detection and prevention systems to detect and respond to unauthorized access attempts. Conduct regular security audits and vulnerability assessments to identify and address potential weaknesses in the system. Educate users about best practices for account security, such as using strong passwords, avoiding sharing login credentials, and being cautious of phishing attempts. Monitor user account activities for any suspicious behavior and implement automated mechanisms to detect and respond to account hijacking attempts. Ensure that user account data is securely stored and protected from unauthorized access. Regularly review and enhance security measures based on evolving security threats and industry best practices. |
| Source | Sidra, Urooj |
| Rationale | To ensure the security and integrity of user accounts by preventing unauthorized access and protecting against account hijacking. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

### <Login.User.SecureSessionManagement>

|  |  |
| --- | --- |
| Identifier | 2.11 |
| Title | <Login.User.SecureSessionManagement> |
| Requirement | The system shall provide a secure session management mechanism to maintain user authentication throughout their interaction with the system. Implement a secure session management mechanism that generates and manages session tokens or identifiers for authenticated users. Ensure that session tokens are securely generated, transmitted, and stored. Use secure protocols (e.g., HTTPS) to encrypt the communication between the user's browser and the system. Implement session timeout mechanisms to automatically terminate inactive sessions and require reauthentication. Protect against session fixation attacks by generating new session tokens upon successful login or authentication. Implement measures to prevent session hijacking, such as using secure cookies, employing secure session storage techniques, and regularly rotating session keys. Regularly monitor and audit session activities to detect any unauthorized access or suspicious behavior. Implement appropriate mechanisms to revoke or invalidate sessions in case of user logout, account deactivation, or security incidents. Conduct regular security assessments and penetration tests to identify and address any vulnerabilities in the session management mechanism. Stay informed about emerging security threats and best practices in session management to ensure the system's security posture is up to date. |
| Source | Sidra, Urooj |
| Rationale | To ensure the security and integrity of user sessions and prevent unauthorized access to user accounts. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

### <Login.User.VulnerabilityProtection>

|  |  |
| --- | --- |
| Identifier | FR2.12 |
| Title | <Login.User.VulnerabilityProtection> |
| Requirement | The system shall implement measures to protect against common login vulnerabilities, such as cross-site scripting (XSS) and SQL injection attacks. Implement input validation and sanitization techniques to prevent cross-site scripting (XSS) attacks. Validate and sanitize user input to remove or neutralize any malicious code. Implement server-side validation to ensure that user input conforms to expected patterns and does not contain any harmful elements. Use parameterized queries or prepared statements to prevent SQL injection attacks. Avoid concatenating user input directly into SQL queries and instead use parameter binding techniques. Regularly update and patch the system's software components to address any known vulnerabilities. Conduct regular security audits and vulnerability assessments to identify and mitigate potential vulnerabilities. Stay informed about the latest security threats and best practices for login process security. Provide security training and awareness programs for developers to educate them about secure coding practices and common vulnerabilities. Implement a web application firewall (WAF) to detect and block potential attack attempts. Monitor system logs and user activities for any suspicious behavior or signs of attempted attacks. |
| Source | Sidra, Urooj |
| Rationale | To ensure the security and integrity of user login processes by mitigating common vulnerabilities. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

### <Login.User.SessionExpiration>

|  |  |
| --- | --- |
| Identifier | FR2.13 |
| Title | <Login.User.SessionExpiration> |
| Requirement | The system shall ensure that user sessions expire after a specified period of inactivity to prevent unauthorized access to the account. Implement session timeout mechanisms to automatically expire user sessions after a specified period of inactivity. Configure the session timeout duration based on the system's security requirements and user experience considerations. Provide appropriate notification or warning messages to users before their sessions are about to expire. Allow users to extend their session or reauthenticate to continue using the system. Implement a secure session management mechanism that handles session expiration events properly and clears session data to prevent any residual information leakage. Conduct regular testing and quality assurance to ensure that session expiration functionality is working as intended. Monitor and analyze session expiration events to identify any anomalies or unexpected behavior. |
| Source | Sidra, Urooj |
| Rationale | To enhance the security of user accounts by automatically terminating inactive sessions. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

## Forget Password

### <Login.User.ForgotPasswordOption>

|  |  |
| --- | --- |
| Identifier | FR3.1 |
| Title | <Login.User.ForgotPasswordOption> |
| Requirement | The system shall provide a "Forgot Password" link or option on the login interface. Implement a "Forgot Password" link or option on the login interface. |
| Source | Sidra, Urooj |
| Rationale | To allow users to recover or reset their passwords in case they forget them. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

### <Login.User.ForgotPasswordPrompt>

|  |  |
| --- | --- |
| Identifier | FR3.2 |
| Title | <Login.User.ForgotPasswordPrompt> |
| Requirement | When the user clicks on the "Forgot Password" link, the system shall prompt the user to enter their registered email address. |
| Source | Sidra, Urooj |
| Rationale | To collect the necessary information (registered email address) from the user to initiate the password recovery/reset process. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

### <Login.User.EmailValidation>

|  |  |
| --- | --- |
| Identifier | FR3.3 |
| Title | <Login.User.EmailValidation> |
| Requirement | The system shall validate the entered email address to ensure it matches a registered user in the system. |
| Source | Sidra, Urooj |
| Rationale | To verify the entered email address and ensure it corresponds to a registered user in the system before proceeding with the password recovery/reset process. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

### <Login.User.PasswordResetLink>

|  |  |
| --- | --- |
| Identifier | FR3.4 |
| Title | <Login.User.PasswordResetLink> |
| Requirement | If the entered email address is valid, the system shall generate and send a password reset link or code to the user's email address. |
| Source | Sidra, Urooj |
| Rationale | To provide a secure and convenient method for users to reset their passwords by generating a unique reset link or code and sending it to their registered email address. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

### <Login.User.PasswordResetLinkSecurity>

|  |  |
| --- | --- |
| Identifier | FR3.5 |
| Title | <Login.User.PasswordResetLinkSecurity> |
| Requirement | The password reset link or code sent to the user's email address shall be unique and time-limited to ensure security. |
| Source | Sidra, Urooj |
| Rationale | To enhance the security of the password reset process, the system should generate a unique and time-limited reset link or code. This ensures that only the intended user can reset their password and reduces the risk of unauthorized access to the account. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

### <Login.User.PasswordResetSuccessMessage>

|  |  |
| --- | --- |
| Identifier | FR3.6 |
| Title | <Login.User.PasswordResetSuccessMessage> |
| Requirement | The system shall display a success message indicating that the password reset link or code has been sent to the user's email address. |
| Source | Sidra, Urooj |
| Rationale | To provide feedback to the user that the password reset link or code has been successfully sent to their email address. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

### <Login.User.InvalidEmailAddressErrorMessage>

|  |  |
| --- | --- |
| Identifier | FR3.7 |
| Title | <Login.User.InvalidEmailAddressErrorMessage> |
| Requirement | If the entered email address is invalid or not registered in the system, the system shall display an appropriate error message indicating that the email address is not associated with any user account. |
| Source | Sidra, Urooj |
| Rationale | To inform the user that the entered email address is either invalid or not associated with any user account in the system. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

### <Login.User.PasswordResetForm>

|  |  |
| --- | --- |
| Identifier | FR3.8 |
| Title | <Login.User.PasswordResetForm> |
| Requirement | The system shall provide a password reset form where users can enter a new password after clicking the password reset link or entering the code. |
| Source | Sidra, Urooj |
| Rationale | To allow users to securely reset their passwords after receiving the password reset link or code. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

### <Login.User.PasswordValidation>

|  |  |
| --- | --- |
| Identifier | 3.9 |
| Title | <Login.User.PasswordValidation> |
| Requirement | The system shall validate the new password to ensure it meets the required complexity rules, such as minimum length and inclusion of alphanumeric characters and special symbols. |
| Source | Sidra, Urooj |
| Rationale | To enforce strong password requirements and enhance the security of user accounts. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

### <Login.User.PasswordEncryption>

|  |  |
| --- | --- |
| Identifier | FR3.10 |
| Title | <Login.User.PasswordEncryption> |
| Requirement | The system shall securely store the user's new password by encrypting or hashing it. |
| Source | Sidra, Urooj |
| Rationale | To protect the user's password from unauthorized access and enhance the security of user accounts. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

### <Login.User.PasswordResetSuccessMessage>

|  |  |
| --- | --- |
| Identifier | FR3.11 |
| Title | <Login.User.PasswordResetSuccessMessage> |
| Requirement | After successfully resetting the password, the system shall display a success message indicating that the password has been changed. |
| Source | Sidra, Urooj |
| Rationale | To provide feedback to the user and confirm that their password has been successfully reset. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

### <Login.User.PasswordRecoverySecurity>

|  |  |
| --- | --- |
| Identifier | FR3.12 |
| Title | <Login.User.PasswordRecoverySecurity> |
| Requirement | The system shall enforce measures to prevent brute-force attacks or abuse of the password recovery mechanism, such as rate limiting or captcha verification. |
| Source | Sidra, Urooj |
| Rationale | To protect the password recovery mechanism from malicious activities, such as brute-force attacks or abuse. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

### <Login.User.PasswordRecoveryLogging >

|  |  |
| --- | --- |
| Identifier | FR3.13 |
| Title | <Login.User.PasswordRecoveryLogging> |
| Requirement | The system shall log password recovery attempts for auditing and security purposes. |
| Source | Sidra, Urooj |
| Rationale | To track and monitor password recovery activities for auditing and security purposes. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

### <Login.User.PasswordRecoverySecurity>

|  |  |
| --- | --- |
| Identifier | FR3.14 |
| Title | <Login.User.PasswordRecoverySecurity> |
| Requirement | The system shall implement measures to protect against common password recovery vulnerabilities, such as email spoofing or interception. |
| Source | Sidra, Urooj |
| Rationale | To enhance the security of the password recovery process and prevent unauthorized access to user accounts. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

## Network Scanning

### < NetworkScanning.UserInterface >

|  |  |
| --- | --- |
| Identifier | FR4.1 |
| Title | <NetworkScanning.UserInterface> |
| Requirement | The system shall provide a user-friendly interface for initiating and managing automated network scanning. |
| Source | Sidra, Urooj |
| Rationale | To enable users to easily initiate and manage automated network scanning processes without the need for technical expertise. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

#### < NetworkScanning.UserInterface.StartScan >

|  |  |
| --- | --- |
| Identifier | FR4.1.1 |
| Title | <NetworkScanning.UserInterface.StartScan> |
| Requirement | Users shall be able to easily initiate the network scanning process with a single click or command. This can be done through a "Start Scan" button or a similar intuitive interface element. |
| Source | Sidra, Urooj |
| Rationale | To enable users to effortlessly initiate network scanning without complex procedures. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

#### < NetworkScanning.UserInterface.ScanConfiguration >

|  |  |
| --- | --- |
| Identifier | FR4.1.2 |
| Title | <NetworkScanning.UserInterface.ScanConfiguration> |
| Requirement | The interface shall allow users to specify the scanning parameters and configure the scan according to their requirements. This can include defining the target IP addresses or network ranges to be scanned, selecting the scanning techniques or protocols to be used, and setting any additional options or preferences. |
| Source | Sidra, Urooj |
| Rationale | To provide flexibility and customization options for the network scanning process. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

#### < NetworkScanning.UserInterface.ScanningProcessManagement >

|  |  |
| --- | --- |
| Identifier | FR4.1.3 |
| Title | <NetworkScanning.UserInterface.ScanningProcessManagement> |
| Requirement | The system shall provide users with the ability to manage the scanning processes, such as pausing, resuming, or cancelling scans. The interface shall provide intuitive controls for these actions and ensure that the user has sufficient control over the scanning activities. |
| Source | Sidra, Urooj |
| Rationale | To allow users to have control over the scanning processes and manage them according to their needs. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

#### < NetworkScanning.UserInterface.ProgressMonitoring >

|  |  |
| --- | --- |
| Identifier | FR4.1.4 |
| Title | <NetworkScanning.UserInterface.ProgressMonitoring> |
| Requirement | The interface shall provide real-time progress updates on the scanning process, displaying information such as the current status, scanned hosts or services, and any detected vulnerabilities or issues. |
| Source | Sidra, Urooj |
| Rationale | To keep users informed about the ongoing scanning process and provide visibility into the progress and findings. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

#### < NetworkScanning.UserInterface.ScanResults >

|  |  |
| --- | --- |
| Identifier | FR4.1.5 |
| Title | <NetworkScanning.UserInterface.ScanResults> |
| Requirement | Once the scanning is complete, the interface shall present the scan results in a clear and organized manner. This can include summaries, detailed reports, visual representations, or any other format that effectively communicates the findings to the user. |
| Source | Sidra, Urooj |
| Rationale | To provide users with comprehensive and easy-to-understand information about the network scanning results. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

#### < NetworkScanning.UserInterface.NotificationsAlerts >

|  |  |
| --- | --- |
| Identifier | FR4.1.6 |
| Title | <NetworkScanning.UserInterface.NotificationsAlerts> |
| Requirement | The system shall notify users of any important events or findings during the scanning process through the interface. This includes alerts for critical vulnerabilities, system anomalies, or completion of long-running scans. |
| Source | Sidra, Urooj |
| Rationale | To ensure users are informed about significant scanning events and can take appropriate actions based on the findings. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

### < NetworkScanning.UserInterface.NetworkSegments>

|  |  |
| --- | --- |
| Identifier | 4.4.2 |
| Title | <NetworkScanning.UserInterface.NetworkSegments> |
| Description | The system shall provide a user interface for managing network segments. |
| Source | User/Stakeholder Requirements |
| Rationale | Managing network segments is essential for effective network scanning and vulnerability assessment. By providing a user interface specifically designed for managing network segments, the system enables users to define, configure, and organize network segments based on their requirements. This feature enhances the usability and flexibility of the system, allowing users to easily manage and target specific network segments for scanning and assessment purposes. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

#### < NetworkScanning.UserInterface.SelectNetworkSegments >

|  |  |
| --- | --- |
| Identifier | 4.2.1 |
| Title | <NetworkScanning.UserInterface.SelectNetworkSegments> |
| Requirement | The scanning interface shall allow users to select specific network segments to be included in the scan. |
| Source | Sidra, Urooj |
| Rationale | To provide users with the flexibility to choose the network segments they want to include in the scanning process. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | N/A |

#### < NetworkScanning.UserInterface.SelectDevices >

|  |  |
| --- | --- |
| Identifier | 4.2.2 |
| Title | <NetworkScanning.UserInterface.SelectDevices> |
| Requirement | The scanning interface shall allow users to select specific devices or hosts to be included in the scan. |
| Source | Sidra, Urooj |
| Rationale | To provide users with the flexibility to choose the devices or hosts they want to include in the scanning process. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | N/A |

#### < NetworkScanning.UserInterface.ValidateSelection >

|  |  |
| --- | --- |
| Identifier | 4.2.3 |
| Title | <NetworkScanning.UserInterface.ValidateSelection> |
| Requirement | The scanning interface shall validate the user's selection of network segments and devices to ensure their accuracy and prevent inclusion of invalid or unauthorized targets. |
| Source | Sidra, Urooj |
| Rationale | To ensure that only valid and authorized network segments and devices are included in the scanning process. |
| Priority | High |
| Business Rule | N/A |
| Dependencies | N/A |

### < NetworkScanning.DisplayProgress >

|  |  |
| --- | --- |
| Identifier | 4.3 |
| Title | <NetworkScanning.DisplayProgress> |
| Requirement | The system shall display the progress of the network scan, indicating the current status and any detected vulnerabilities or security risks. |
| Source | Sidra, Urooj |
| Rationale | To provide users with real-time visibility into the scanning progress and the identification of vulnerabilities or security risks. |
| Priority | High |
| Business Rule | N/A |
| Dependencies | N/A |

### < NetworkScanning.CustomizeParameters >

|  |  |
| --- | --- |
| Identifier | 4.4 |
| Title | <NetworkScanning.CustomizeParameters> |
| Requirement | The scanning interface shall provide options to customize the scanning parameters, such as scan depth, scan intensity, and scan speed. |
| Source | Sidra, Urooj |
| Rationale | To allow users to tailor the scanning process based on their specific requirements and preferences, adjusting parameters such as scan depth, intensity, and speed. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | N/A |

### < NetworkScanning.PresentScanResults >

|  |  |
| --- | --- |
| Identifier | 4.5 |
| Title | <NetworkScanning.PresentScanResults> |
| Requirement | The system shall present the scan results in an intuitive and easily understandable format, highlighting critical vulnerabilities and providing detailed information for further analysis. |
| Source | Sidra, Urooj |
| Rationale | To enable users to comprehend the scan results effectively, the system should present them in a clear and user-friendly manner. This includes emphasizing critical vulnerabilities and providing comprehensive details for further analysis and remediation. |
| Priority | High |
| Business Rule | N/A |
| Dependencies | N/A |

### < NetworkScanning.UserInterface.FilterSortScanResults >

|  |  |
| --- | --- |
| Identifier | 4.6 |
| Title | <NetworkScanning.UserInterface.FilterSortScanResults> |
| Requirement | The scanning interface shall allow users to filter and sort the scan results based on severity, device type, or other relevant criteria. |
| Source | Sidra, Urooj |
| Rationale | To enhance the usability of the scanning interface, users should be able to filter and sort the scan results according to their specific needs. This functionality enables users to focus on specific criteria, such as severity or device type, for easier analysis and prioritization of vulnerabilities. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | N/A |

### < NetworkScanning.UserInterface.VisualizeSecurityPosture >

|  |  |
| --- | --- |
| Identifier | 4.7 |
| Title | <NetworkScanning.UserInterface.VisualizeSecurityPosture> |
| Requirement | The system shall provide interactive visualizations, such as charts or graphs, to summarize and present the overall security posture based on the scan results. |
| Source | Sidra, Urooj |
| Rationale | To enhance the understanding of the network security posture, interactive visualizations provide a clear and concise representation of the scan results. These visualizations, such as charts or graphs, offer a comprehensive overview of the security status, including vulnerabilities, risks, and strengths. Users can easily grasp the overall security posture at a glance and make informed decisions for further actions and improvements. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | N/A |

### < NetworkScanning.UserInterface.VisualizeSecurityPosture >

|  |  |
| --- | --- |
| Identifier | 4.8 |
| Title | <NetworkScanning.UserInterface.GenerateComprehensiveReports> |
| Requirement | The scanning interface shall support the generation of comprehensive reports summarizing the scan findings, including recommended actions for remediation. |
| Source | Sidra, Urooj |
| Rationale | Generating comprehensive reports is essential for documenting and communicating the scan findings effectively. These reports provide a summarized overview of the scan results, including vulnerabilities, risks, and recommended actions for remediation. By generating comprehensive reports, users can easily share the scan findings with relevant stakeholders, such as management, IT teams, or auditors, and facilitate the prioritization and implementation of necessary remediation measures. |
| Priority | High |
| Business Rule | N/A |
| Dependencies | N/A |

### < NetworkScanning.UserInterface.ScanReports >

#### <NetworkScanning.UserInterface.SelectExportFormat>

|  |  |
| --- | --- |
| Identifier | 4.9.1 |
| Title | <NetworkScanning.UserInterface.SelectExportFormat> |
| Requirement | The scanning interface shall provide options for users to select the desired export format for scan reports, such as PDF or HTML. |
| Source | Sidra, Urooj |
| Rationale | Offering options to select the export format for scan reports allows users to choose the format that best suits their needs. Users may have different requirements or preferences when it comes to sharing or further analyzing scan reports. Providing formats such as PDF or HTML ensures compatibility with different systems and tools, facilitating data dissemination and integration. This flexibility in export formats enhances the usability and versatility of the scanning interface. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | 4.9 |

#### < NetworkScanning.UserInterface.ExportScanReports >

|  |  |
| --- | --- |
| Identifier | 4.9.2 |
| Title | <NetworkScanning.UserInterface.ExportScanReports> |
| Requirement | The scanning interface shall provide the functionality to export the scan reports in the selected format, allowing users to save the reports locally or in a specified location. |
| Source | Sidra, Urooj |
| Rationale | To enable users to save and store the scan reports in their preferred format and location for future reference or sharing. |
| Priority | High |
| Business Rule | N/A |
| Dependencies | 4.9 |

#### < NetworkScanning.UserInterface.ShareScanReports >

|  |  |
| --- | --- |
| Identifier | 4.9.3 |
| Title | <NetworkScanning.UserInterface.ShareScanReports> |
| Requirement | The scanning interface shall provide options for users to share the scan reports directly from the interface, allowing them to send the reports via email or other communication channels. |
| Source | Sidra, Urooj |
| Rationale | To facilitate the sharing of scan reports with relevant stakeholders, such as security teams or network administrators, for further analysis or action. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | 4.9 |

#### < NetworkScanning.UserInterface.SaveScanReports >

|  |  |
| --- | --- |
| Identifier | 4.9.4 |
| Title | <NetworkScanning.UserInterface.SaveScanReports> |
| Requirement | The scanning interface shall provide the capability to save the scan reports locally on the user's system or designated storage location. |
| Source | Sidra, Urooj |
| Rationale | To allow users to archive or store the scan reports for future reference or compliance purposes. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | 4.9 |

### < NetworkScanning.UserInterface.ScheduleScans >

|  |  |
| --- | --- |
| Identifier | 4.10 |
| Title | <NetworkScanning.UserInterface.ScheduleScans> |
| Requirement | The scanning interface shall provide options for users to schedule regular automated scans. Users should be able to specify the frequency (e.g., daily, weekly, monthly) and time of the scans. |
| Source | Sidra, Urooj |
| Rationale | To automate the scanning process and ensure regular and timely assessment of the network's security. |
| Priority | High |
| Business Rule | N/A |
| Dependencies | N/A |

#### < NetworkScanning.UserInterface.SelectScanFrequency >

|  |  |
| --- | --- |
| Identifier | 4.10.1 |
| Title | <NetworkScanning.UserInterface.SelectScanFrequency> |
| Requirement | The scanning interface shall allow users to select the frequency of the automated scans, such as daily, weekly, or monthly. |
| Source | Sidra, Urooj |
| Rationale | To provide flexibility in scheduling the automated scans based on the user's preferences and requirements. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | 4.10 |

#### < NetworkScanning.UserInterface.SelectScanTime >

|  |  |
| --- | --- |
| Identifier | 4.10.2 |
| Title | <NetworkScanning.UserInterface.SelectScanTime> |
| Requirement | The scanning interface shall allow users to specify the time at which the automated scans should be initiated. |
| Source | Sidra, Urooj |
| Rationale | To enable users to schedule the scans at a convenient time, minimizing potential disruption to network operations. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | 4.10 |

#### < NetworkScanning.UserInterface.EditScheduledScans >

|  |  |
| --- | --- |
| Identifier | 4.10.3 |
| Title | <NetworkScanning.UserInterface.EditScheduledScans> |
| Requirement | The scanning interface shall provide options for users to modify or update the schedule of the automated scans, including changing the frequency or time. |
| Source | Sidra, Urooj |
| Rationale | To allow users to adjust the automated scanning schedule as needed, accommodating changes in network configurations or operational requirements. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | 4.10 |

### < NetworkScanning.System.NotificationsAndAlerts >

|  |  |
| --- | --- |
| Identifier | FR4.11 |
| Title | <NetworkScanning.System.NotificationsAndAlerts> |
| Requirement | The system shall send notifications or alerts to designated users or administrators when critical vulnerabilities or security risks are identified during the network scans. |
| Source | Sidra, Urooj |
| Rationale | To ensure that responsible individuals are promptly notified of critical vulnerabilities or security risks, allowing them to take immediate action for mitigation or remediation. |
| Priority | High |
| Business Rule | N/A |
| Dependencies | N/A |

#### < NetworkScanning.UserInterface.EditScheduledScans >

|  |  |
| --- | --- |
| Identifier | FR4.11.1 |
| Title | <NetworkScanning.System.ConfigureNotificationRecipients> |
| Requirement | The system shall allow users or administrators to configure the recipients of the notifications or alerts for critical vulnerabilities or security risks identified during network scans. |
| Source | Sidra, Urooj |
| Rationale | To provide flexibility in determining who should receive the notifications or alerts based on the organizational structure and responsibilities. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | 4.11 |

#### < NetworkScanning.UserInterface.EditScheduledScans >

|  |  |
| --- | --- |
| Identifier | FR4.11.2 |
| Title | <NetworkScanning.System.ConfigureNotificationMethods> |
| Requirement | The system shall support multiple notification methods, such as email, SMS, or push notifications, for sending notifications or alerts to the designated recipients when critical vulnerabilities or security risks are identified during network scans. |
| Source | Sidra, Urooj |
| Rationale | To accommodate different communication preferences and ensure that notifications or alerts are delivered effectively to the recipients. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | 4.11 |

#### < NetworkScanning.UserInterface.EditScheduledScans >

|  |  |
| --- | --- |
| Identifier | 4.11.3 |
| Title | <NetworkScanning.System.ConfigureNotificationSeverity> |
| Requirement | The system shall allow users or administrators to configure the severity threshold for sending notifications or alerts. Only critical vulnerabilities or security risks that exceed the configured severity threshold shall trigger the notifications or alerts. |
| Source | Sidra, Urooj |
| Rationale | To provide control over the notifications or alerts by allowing users or administrators to define the level of severity that warrants immediate attention. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | 4.11 |

### < NetworkScanning.UserInterface.AuthenticationAccessControl >

|  |  |
| --- | --- |
| Identifier | 4.12 |
| Title | <NetworkScanning.UserInterface.AuthenticationAccessControl> |
| Requirement | The scanning interface shall support user authentication and access control mechanisms to ensure that only authorized individuals can initiate or view scan results. |
| Source | Sidra, Urooj |
| Rationale | To enforce security and restrict access to the scanning interface and scan results, ensuring that sensitive information is only accessible to authorized users. |
| Priority | High |
| Business Rule | N/A |
| Dependencies | N/A |

#### < NetworkScanning.UserInterface.UserAuthentication >

|  |  |
| --- | --- |
| Identifier | FR4.12.1 |
| Title | <NetworkScanning.UserInterface.UserAuthentication> |
| Requirement | The scanning interface shall implement user authentication mechanisms, such as username and password, to verify the identity of the user before granting access to the scanning functionality. |
| Source | Sidra, Urooj |
| Rationale | To ensure that only authenticated users can access the scanning interface and perform scanning operations, preventing unauthorized access to sensitive information. |
| Priority | High |
| Business Rule | N/A |
| Dependencies | 4.12 |

#### < NetworkScanning.UserInterface.AccessControl>

|  |  |
| --- | --- |
| Identifier | 4.12.2 |
| Title | <NetworkScanning.UserInterface.AccessControl> |
| Requirement | The scanning interface shall enforce access control measures to restrict user access based on their roles or permissions, ensuring that only authorized individuals can initiate or view scan results. |
| Source | Sidra, Urooj |
| Rationale | To provide granular control over the scanning interface, allowing different levels of access for different users based on their assigned roles or permissions. |
| Priority | High |
| Business Rule | N/A |
| Dependencies | 4.12 |

### < NetworkScanning.UserInterface.ContextSensitiveHelp >

|  |  |
| --- | --- |
| Identifier | 4.13 |
| Title | <NetworkScanning.UserInterface.ContextSensitiveHelp> |
| Requirement | The scanning interface shall provide context-sensitive help and documentation, accessible within the interface, to assist users in understanding and utilizing the network scanning functionality effectively. |
| Source | Sidra, Urooj |
| Rationale | To provide users with on-demand assistance and guidance within the scanning interface, helping them navigate and utilize the features effectively, reducing the need for external support. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | N/A |

#### < NetworkScanning.UserInterface. HelpButton >

|  |  |
| --- | --- |
| Identifier | 4.13.1 |
| Title | <NetworkScanning.UserInterface.HelpButton> |
| Requirement | The scanning interface shall include a prominent "Help" button or link that users can click to access context-sensitive help and documentation. |
| Source | Sidra, Urooj |
| Rationale | To provide users with a convenient and easily accessible way to access help and documentation while using the scanning interface. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | 4.13 |

#### < NetworkScanning.UserInterface.ContextualHelp >

|  |  |
| --- | --- |
| Identifier | 4.13.2 |
| Title | <NetworkScanning.UserInterface.ContextualHelp> |
| Requirement | The scanning interface shall provide contextual help and documentation that is specific to the current page, section, or feature being used by the user. |
| Source | Sidra, Urooj |
| Rationale | To offer users relevant and targeted assistance based on their current context within the scanning interface, enhancing their understanding and utilization of the functionality. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | 4.13 |

### < NetworkScanning.UserInterface. RealTimeUpdates >

|  |  |
| --- | --- |
| Identifier | 4.14 |
| Title | <NetworkScanning.UserInterface.RealTimeUpdates> |
| Requirement | The scanning interface shall provide real-time updates to users during the scanning process, displaying information such as current status, progress, and any detected vulnerabilities or security risks. |
| Source | Sidra, Urooj |
| Rationale | To keep users informed and engaged by providing them with up-to-date information about the scanning progress and any potential security findings in real-time. |
| Priority | High |
| Business Rule | N/A |
| Dependencies | N/A |

#### < NetworkScanning.UserInterface.DisplayStatus >

|  |  |
| --- | --- |
| Identifier | FR4.14.1 |
| Title | <NetworkScanning.UserInterface.DisplayStatus> |
| Requirement | The scanning interface shall display the current status of the scanning process, indicating whether the scan is in progress, completed, or paused. |
| Source | Sidra, Urooj |
| Rationale | To provide users with immediate information about the status of the scanning process and its progress. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | 4.14 |

#### < NetworkScanning.UserInterface.DisplayProgress >

|  |  |
| --- | --- |
| Identifier | 4.14.2 |
| Title | <NetworkScanning.UserInterface.DisplayProgress> |
| Requirement | The scanning interface shall show the progress of the scanning process, indicating the percentage of completion or the number of hosts or services scanned. |
| Source | Sidra, Urooj |
| Rationale | To provide users with visibility into the progress of the scanning process, allowing them to track its advancement. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | 4.14 |

#### < NetworkScanning.UserInterface.DisplayVulnerabilities >

|  |  |
| --- | --- |
| Identifier | 4.14.3 |
| Title | <NetworkScanning.UserInterface.DisplayVulnerabilities> |
| Requirement | The scanning interface shall present any detected vulnerabilities or security risks in real-time, providing detailed information about the identified issues. |
| Source | Sidra, Urooj |
| Rationale | To enable users to promptly identify and respond to critical security findings during the scanning process. |
| Priority | High |
| Business Rule | N/A |
| Dependencies | 4.14 |

### < NetworkScanning.History.MaintainHistoryAndReviewScans >

|  |  |
| --- | --- |
| Identifier | 4.15 |
| Title | <NetworkScanning.History.MaintainHistoryAndReviewScans> |
| Requirement | The system shall maintain a history of past scans, storing the scan results and associated information for future reference. Users shall be able to review and analyze previous scan results for trend analysis and comparison purposes. |
| Source | Sidra, Urooj |
| Rationale | To enable users to track the security status of the network over time, identify trends, and make informed decisions based on historical scan results. |
| Priority | High |
| Business Rule | N/A |
| Dependencies | N/A |

#### < NetworkScanning.History.MaintainHistory >

|  |  |
| --- | --- |
| Identifier | 4.15.1 |
| Title | <NetworkScanning.History.MaintainHistory> |
| Requirement | The system shall maintain a history of past scans, storing the scan results and associated information for future reference. |
| Source | Sidra, Urooj |
| Rationale | To enable users to review and analyze previous scan results, track changes over time, and identify trends or patterns. |
| Priority | High |
| Business Rule | N/A |
| Dependencies | 4.15 |

#### < NetworkScanning.History.ViewPreviousScans >

|  |  |
| --- | --- |
| Identifier | 4.15.2 |
| Title | <NetworkScanning.History.ViewPreviousScans> |
| Requirement | The system shall provide functionality for users to access and review previous scan results, allowing them to view detailed reports or summaries of past scans. |
| Source | Sidra, Urooj |
| Rationale | To facilitate trend analysis and comparison of scan results, providing users with insights into the security posture of the network over time. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | 4.15.1 |

### < NetworkScanning.UserInterface.MultiLanguageAndAccessibility >

|  |  |
| --- | --- |
| Identifier | 4.16 |
| Title | <NetworkScanning.UserInterface.MultiLanguageAndAccessibility> |
| Requirement | The scanning interface shall support multi-language capabilities, allowing users to choose their preferred language for the interface. Additionally, the interface shall adhere to accessibility guidelines and provide features to support users with different accessibility needs, such as screen readers, keyboard navigation, and high contrast modes. |
| Source | Sidra, Urooj |
| Rationale | To enhance usability and inclusivity, accommodating users with different language preferences and accessibility requirements. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | N/A |

#### < NetworkScanning.UserInterface.SelectLanguage >

|  |  |
| --- | --- |
| Identifier | 4.16.1 |
| Title | <NetworkScanning.UserInterface.SelectLanguage> |
| Requirement | The scanning interface shall provide users with the ability to select their preferred language from a list of supported languages. |
| Source | Sidra, Urooj |
| Rationale | To accommodate users with different language preferences and enhance their experience with the scanning interface. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | 4.16 |

#### <NetworkScanning.UserInterface.AccessibilityFeatures >

|  |  |
| --- | --- |
| Identifier | 4.16.2 |
| Title | <NetworkScanning.UserInterface.AccessibilityFeatures> |
| Requirement | The scanning interface shall adhere to accessibility guidelines and incorporate features such as screen reader compatibility, keyboard navigation support, and high contrast modes. |
| Source | Sidra, Urooj |
| Rationale | To ensure that users with different accessibility needs can effectively use the scanning interface. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | 4.16 |

### < NetworkScanning.UserInterface.Dashboard>

|  |  |
| --- | --- |
| Identifier | 4.17 |
| Title | <NetworkScanning.UserInterface.Dashboard> |
| Requirement | The scanning interface shall include a dashboard or overview page that provides users with a summary of ongoing and completed scans, key metrics, and actionable insights. |
| Source | Sidra, Urooj |
| Rationale | To offer users a centralized view of the scanning activities, allowing them to quickly assess the overall security posture and identify areas that require attention or further investigation. |
| Priority | High |
| Business Rule | N/A |
| Dependencies | N/A |

#### < NetworkScanning.UserInterface.Dashboard.Summary >

|  |  |
| --- | --- |
| Identifier | 4.17.1 |
| Title | <NetworkScanning.UserInterface.Dashboard.Summary> |
| Requirement | The dashboard or overview page shall include a summary section that provides a high-level overview of ongoing and completed scans, highlighting key metrics and indicators of the network security status. |
| Source | Sidra, Urooj |
| Rationale | To give users a quick snapshot of the scanning activities and the overall security posture without the need to delve into detailed reports. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | 4.17 |

#### < NetworkScanning.UserInterface.Dashboard.ScanMetrics >

|  |  |
| --- | --- |
| Identifier | 4.17.2 |
| Title | <NetworkScanning.UserInterface.Dashboard.ScanMetrics> |
| Requirement | The dashboard or overview page shall display key metrics related to the scans, such as the number of scans performed, scan duration, scan coverage, and detected vulnerabilities. |
| Source | Sidra, Urooj |
| Rationale | To provide users with quantitative information about the scanning activities and the security posture of the network. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | 4.17 |

#### < NetworkScanning.UserInterface.Dashboard.ActionableInsights >

|  |  |
| --- | --- |
| Identifier | FR4.17.3 |
| Title | <NetworkScanning.UserInterface.Dashboard.ActionableInsights> |
| Requirement | The dashboard or overview page shall present actionable insights based on the scan results, such as highlighting critical vulnerabilities, identifying potential security risks, and recommending remediation actions. |
| Source | Sidra, Urooj |
| Rationale | To guide users in taking necessary actions based on the scan findings and improve the overall network security. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | 4.17 |

## Network Scanning Techniques

### < NetworkScanning.Techniques.Support >

|  |  |
| --- | --- |
| Identifier | 5.1.1 |
| Title | <NetworkScanning.Techniques.Support> |
| Requirement | The system shall support multiple scanning techniques, including port scanning, vulnerability scanning, and penetration testing, to identify potential vulnerabilities and security risks in the network. |
| Source | Sidra, Urooj |
| Rationale | To provide a comprehensive and diverse set of scanning techniques that cater to different aspects of network security assessment and testing. |
| Priority | High |
| Business Rule | N/A |
| Dependencies | 5.1 |

### < NetworkScanning.UserInterface.SelectScanningTechniques >

|  |  |
| --- | --- |
| Identifier | 5.2 |
| Title | <NetworkScanning.UserInterface.SelectScanningTechniques> |
| Requirement | The scanning interface shall provide options for users to select specific scanning techniques, such as port scanning, vulnerability scanning, and penetration testing, based on their requirements and objectives. |
| Source | Sidra, Urooj |
| Rationale | To offer users the flexibility to choose the scanning techniques that align with their specific goals and network assessment needs. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | N/A |

#### < NetworkScanning.UserInterface.SelectPortScanning >

|  |  |
| --- | --- |
| Identifier | 5.2.1 |
| Title | <NetworkScanning.UserInterface.SelectPortScanning> |
| Requirement | The scanning interface shall provide options for users to select port scanning as a specific scanning technique, allowing them to scan for open ports on target devices or network segments. |
| Source | Sidra, Urooj |
| Rationale | To enable users to choose port scanning as a specific technique to identify open ports on target systems, which helps in assessing network security and identifying potential vulnerabilities. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | 5.2 |

##### <NetworkScanning.UserInterface.SelectTargetPorts>

|  |  |
| --- | --- |
| Identifier | 5.2.1.1 |
| Title | <NetworkScanning.UserInterface.SelectTargetPorts> |
| Requirement | The scanning interface shall provide options for users to specify the target ports or port ranges to be scanned during the port scanning process. |
| Source | Sidra, Urooj |
| Rationale | To allow users to customize the port scanning process by selecting specific ports or port ranges to be scanned, providing flexibility and control over the scanning activity. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | 5.2.1 |

##### <NetworkScanning.UserInterface.SelectPortScanningTechniques >

|  |  |
| --- | --- |
| Identifier | 5.2.1.2 |
| Title | <NetworkScanning.UserInterface.SelectPortScanningTechniques> |
| Requirement | The scanning interface shall provide options for users to select different types of port scanning techniques, such as TCP, UDP, or SYN scanning, during the port scanning process. |
| Source | Sidra, Urooj |
| Rationale | To allow users to choose the appropriate port scanning techniques based on their specific requirements and the nature of the target network, providing flexibility and customization options for the scanning activity. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | 5.2.1 |

##### < NetworkScanning.UserInterface.ConfigurePortScanningParameters >

|  |  |
| --- | --- |
| Identifier | 5.2.1.3 |
| Title | <NetworkScanning.UserInterface.ConfigurePortScanningParameters> |
| Requirement | The scanning interface shall provide options for users to configure port scanning parameters, such as scan speed or timeout settings, to customize the port scanning process according to their specific needs. |
| Source | Sidra, Urooj |
| Rationale | To allow users to adjust and optimize the port scanning parameters based on the network environment, target systems, and scan requirements, providing flexibility and control over the scanning activity. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | 5.2.1 |

#### < NetworkScanning.UserInterface.SelectVulnerabilityScanning >

|  |  |
| --- | --- |
| Identifier | 5.2.2 |
| Title | <NetworkScanning.UserInterface.SelectVulnerabilityScanning> |
| Requirement | The scanning interface shall allow users to select the vulnerability scanning technique for identifying potential security vulnerabilities in the target systems. |
| Source | Sidra, Urooj |
| Rationale | To provide users with the flexibility to choose the vulnerability scanning technique based on their specific needs and requirements, enabling them to assess the security posture of their systems. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | N/A |

##### < NetworkScanning.UserInterface. SelectVulnerabilityScanningTool >

|  |  |
| --- | --- |
| Identifier | 5.2.2.1 |
| Title | <NetworkScanning.UserInterface.SelectVulnerabilityScanningTool> |
| Requirement | The scanning interface shall provide options for users to select specific vulnerability scanning tools or databases to be used during the vulnerability scanning process. |
| Source | Sidra, Urooj |
| Rationale | To allow users to choose the appropriate vulnerability scanning tools or databases that best suit their scanning requirements and preferences. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | 5.2.2 |

##### < NetworkScanning.UserInterface.DefineVulnerabilityScanningScope >

|  |  |
| --- | --- |
| Identifier | 5.2.2.2 |
| Title | <NetworkScanning.UserInterface.DefineVulnerabilityScanningScope> |
| Requirement | The scanning interface shall provide options for users to define the scope of vulnerability scanning, including specifying target hosts or IP ranges to be scanned. |
| Source | Sidra, Urooj |
| Rationale | To enable users to customize the vulnerability scanning process by selecting the specific hosts or IP ranges they want to target for scanning. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | 5.2.2 |

##### < NetworkScanning.UserInterface. ScheduleAutomatedScan >

|  |  |
| --- | --- |
| Identifier | FR5.2.2.3 |
| Title | <NetworkScanning.UserInterface.ScheduleAutomatedScans> |
| Requirement | The scanning interface shall offer options for users to schedule automated vulnerability scans at regular intervals, allowing them to define the frequency and timing of the scans. |
| Source | Sidra, Urooj |
| Rationale | To enable users to automate the vulnerability scanning process and perform regular scans at specified intervals, reducing manual effort and ensuring continuous monitoring of security vulnerabilities. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | N/A |

#### < NetworkScanning.UserInterface.SelectPentesting >

|  |  |
| --- | --- |
| Identifier | 4.5.2.3 |
| Title | <NetworkScanning.UserInterface.SelectPentesting> |
| Description | The system shall provide a user interface for selecting pentesting activities. |
| Source | User/Stakeholder Requirements |
| Rationale | Pentesting activities play a crucial role in assessing the security of a network. By providing a user interface for selecting pentesting activities, the system enables users to choose and configure specific tests or activities to be performed during the pentesting process. This feature enhances the flexibility and customization options for conducting comprehensive security assessments and helps users focus on specific areas of interest or concern. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

##### < NetworkScanning.UserInterface. ConfigurePentestingParameters >

|  |  |
| --- | --- |
| Identifier | 5.2.3.1 |
| Title | <NetworkScanning.UserInterface.ConfigurePenTestingParameters> |
| Requirement | The scanning interface shall provide options for users to configure the parameters and options for penetration testing, such as specifying the target hosts or IP ranges, selecting the penetration testing tools or frameworks, and defining any additional settings or preferences. |
| Source | Sidra, Urooj |
| Rationale | To allow users to customize the penetration testing process based on their requirements, including the selection of tools, defining the scope, and configuring specific parameters, ensuring a comprehensive and tailored approach to security testing. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | 5.2.3 |

##### < NetworkScanning.UserInterface. SelectPenTestingMethodologies>

|  |  |
| --- | --- |
| Identifier | 5.2.3.2 |
| Title | <NetworkScanning.UserInterface.SelectPenTestingMethodologies> |
| Requirement | The scanning interface shall provide options for users to select specific penetration testing methodologies, such as black-box, white-box, or gray-box testing. |
| Source | Sidra, Urooj |
| Rationale | To allow users to choose the appropriate penetration testing methodology based on the requirements and goals of the testing process, ensuring a comprehensive and targeted approach to identifying vulnerabilities and weaknesses. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | N/A |

##### < NetworkScanning.UserInterface.SpecifyPenTestingTargets >

|  |  |
| --- | --- |
| Identifier | 5.2.3.3 |
| Title | <NetworkScanning.UserInterface.SpecifyPenTestingTargets> |
| Requirement | The scanning interface shall provide options for users to specify the target systems, networks, or applications for penetration testing. |
| Source | Sidra, Urooj |
| Rationale | To allow users to define the scope of the penetration testing activities and focus the testing efforts on specific systems, networks, or applications of interest. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | N/A |

##### < NetworkScanning.UserInterface.ConfigurePenTestingParameters >

|  |  |
| --- | --- |
| Identifier | 5.2.3.4 |
| Title | <NetworkScanning.UserInterface.ConfigurePenTestingParameters> |
| Requirement | The scanning interface shall provide options for users to configure penetration testing parameters, such as attack vectors, payload customization, or exploitation techniques. |
| Source | Sidra, Urooj |
| Rationale | To allow users to customize the penetration testing activities according to their specific requirements and testing objectives. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | N/A |

### < NetworkScanning.AutomatedScanningProfiles >

|  |  |
| --- | --- |
| Identifier | 5.3 |
| Title | <NetworkScanning.AutomatedScanningProfiles> |
| Requirement | The system shall support automated scanning profiles or presets, providing predefined configurations for common scanning scenarios. |
| Source | Sidra, Urooj |
| Rationale | To facilitate the scanning process by offering preconfigured profiles that align with common scanning requirements, saving time and effort for users. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | N/A |

#### < NetworkScanning.AutomatedScanningProfiles.CreateProfile >

|  |  |
| --- | --- |
| Identifier | 5.3.1 |
| Title | <NetworkScanning.AutomatedScanningProfiles.CreateProfile> |
| Requirement | The scanning interface shall allow users to create custom automated scanning profiles by specifying their own configurations and parameters. |
| Source | Sidra, Urooj |
| Rationale | To offer flexibility for users to define and save their own scanning profiles that suit their unique scanning requirements. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | N/A |

#### < NetworkScanning.AutomatedScanningProfiles.SelectProfile>

|  |  |
| --- | --- |
| Identifier | 5.3.2 |
| Title | <NetworkScanning.AutomatedScanningProfiles.SelectProfile> |
| Requirement | The scanning interface shall allow users to select a predefined automated scanning profile from a list of available options. |
| Source | Sidra, Urooj |
| Rationale | To provide users with a convenient way to choose preconfigured scanning profiles that align with their specific needs and scenarios. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | N/A |

### < NetworkScanning.UserInterface.DisplayScanProgress >

|  |  |
| --- | --- |
| Identifier | 5.4 |
| Title | <NetworkScanning.UserInterface.DisplayScanProgress> |
| Requirement | The scanning interface shall display the progress and status of each scanning technique, indicating the completion and results of the respective scans. |
| Source | Sidra, Urooj |
| Rationale | To provide users with real-time visibility into the progress and status of each scanning technique, ensuring they are informed about the scanning process and its outcomes. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | N/A |

### < NetworkScanning. <NetworkScanning.Presentation.PresentFindings >

|  |  |
| --- | --- |
| Identifier | 5.5 |
| Title | <NetworkScanning.Presentation.PresentFindings> |
| Requirement | The system shall present the findings of each scanning technique in a comprehensive and easily interpretable manner, highlighting vulnerabilities, potential risks, and suggested remediation actions. |
| Source | Sidra, Urooj |
| Rationale | To provide users with a clear understanding of the scan results, emphasizing identified vulnerabilities, associated risks, and recommended actions for mitigation or remediation. |
| Priority | High |
| Business Rule | N/A |
| Dependencies | N/A |

### < NetworkScanning.UserInterface.GenerateTechniqueReports>

|  |  |
| --- | --- |
| Identifier | 5.6 |
| Title | <NetworkScanning.UserInterface.GenerateTechniqueReports> |
| Requirement | The scanning interface shall support the generation of separate reports for each scanning technique, capturing the specific findings and analysis. |
| Source | Sidra, Urooj |
| Rationale | To provide users with detailed and focused reports for each scanning technique, facilitating in-depth analysis and remediation planning. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | N/A |

### < NetworkScanning.UserInterface. CompareScanningResults >

|  |  |
| --- | --- |
| Identifier | Sub-FR5.7 |
| Title | <NetworkScanning.UserInterface.CompareScanningResults> |
| Requirement | The scanning interface shall provide options for users to compare the results from different scanning techniques. |
| Source | Sidra, Urooj |
| Rationale | To enable users to identify cross-references and potential dependencies between the results of different scanning techniques. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | N/A |

### < NetworkScanning.UserInterface.VisualRepresentations >

|  |  |
| --- | --- |
| Identifier | FR5.8 |
| Title | <NetworkScanning.UserInterface.VisualRepresentations> |
| Requirement | The scanning interface shall offer visual representations, such as diagrams or charts, to illustrate the outcomes and relationships between different scanning techniques. |
| Source | Sidra, Urooj |
| Rationale | To provide users with a visual and intuitive way to understand and interpret the outcomes and relationships between different scanning techniques. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | N/A |

### < NetworkScanning.UserInterface. KnowledgeBase >

|  |  |
| --- | --- |
| Identifier | 4.5.9 |
| Title | <NetworkScanning.UserInterface.KnowledgeBase> |
| Requirement | The scanning interface shall include a knowledge base or FAQ section that addresses common questions and concerns related to each scanning technique. |
| Source | Sidra, Urooj |
| Rationale | To provide users with a centralized resource to access information and find answers to common questions or concerns they may have about each scanning technique. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

### < NetworkScanning.UserInterface.AdvancedScanningTechniques>

|  |  |
| --- | --- |
| Identifier | 5.10 |
| Title | <NetworkScanning.UserInterface.AdvancedScanningTechniques> |
| Requirement | The scanning interface shall support advanced scanning techniques, such as stealth scanning or custom script-based scanning, for advanced users or specific use cases. |
| Source | Sidra, Urooj |
| Rationale | To cater to the needs of advanced users or specific use cases, the scanning interface should provide support for advanced scanning techniques that go beyond the standard scanning methods. This allows for more comprehensive and specialized scanning capabilities. |
| Priority | Medium |
| Dependencies | N/A |
| Business Rule | N/A |

#### < NetworkScanning.UserInterface.SupportStealthScanning >

|  |  |
| --- | --- |
| Identifier | 5.10.1 |
| Title | <NetworkScanning.UserInterface.SupportStealthScanning> |
| Requirement | The scanning interface shall provide support for stealth scanning techniques, such as idle scanning or fragmented packet scanning, to identify potential vulnerabilities without raising suspicion or triggering security measures. |
| Source | Sidra, Urooj |
| Rationale | To enable users to perform covert scanning techniques that can help identify vulnerabilities without alerting potential attackers or triggering security mechanisms. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | N/A |

#### <NetworkScanning.UserInterface.UploadCustomScripts>

|  |  |
| --- | --- |
| Identifier | 5.10.2 |
| Title | <NetworkScanning.UserInterface.UploadCustomScripts> |
| Requirement | The scanning interface shall allow users to upload and execute custom scanning scripts or plugins, enabling the execution of tailored scanning methods specific to their environment or requirements. |
| Source | Sidra, Urooj |
| Rationale | To provide flexibility and customization options for users to perform scanning techniques that are specific to their environment or unique requirements. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | N/A |

#### <NetworkScanning.UserInterface.AdvancedConfigurationOptions >

|  |  |
| --- | --- |
| Identifier | 5.10.3 |
| Title | <NetworkScanning.UserInterface.AdvancedConfigurationOptions> |
| Requirement | The scanning interface shall offer advanced configuration options for fine-tuning scanning parameters, including timeouts, packet fragmentation, or source IP spoofing, to facilitate more sophisticated scanning techniques. |
| Source | Sidra, Urooj |
| Rationale | To provide advanced users with the ability to customize scanning parameters and employ more sophisticated scanning techniques that require fine-tuning for optimal results. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | N/A |

### < NetworkScanning.DatabasMaintainScanningTechniques >

|  |  |
| --- | --- |
| Identifier | 5.11 |
| Title | <NetworkScanning.DatabasMaintainScanningTechniques> |
| Requirement | The system shall maintain an up-to-date database of scanning techniques, regularly updating and expanding the available options based on emerging vulnerabilities and evolving security practices. |
| Source | Sidra, Urooj |
| Rationale | To ensure the effectiveness and relevance of the scanning capabilities, it is crucial to maintain an up-to-date database of scanning techniques. This allows the system to adapt to emerging vulnerabilities and evolving security practices, providing users with the latest and most effective scanning options to detect potential risks and vulnerabilities in their networks. |
| Priority | Medium |
| Business Rule | N/A |
| Dependencies | N/A |

#### < NetworkScanning.Database.AddScanningTechnique >

|  |  |
| --- | --- |
| Identifier | 5.11.1 |
| Title | <NetworkScanning.Database.AddScanningTechnique> |
| Requirement | The system shall provide the capability to add new scanning techniques to the database. |
| Source | N/A |
| Rationale | To allow for the inclusion of new and emerging scanning techniques to enhance the system's capabilities. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

#### < NetworkScanning.Database.UpdateScanningTechnique>

|  |  |
| --- | --- |
| Identifier | 5.11.2 |
| Title | <NetworkScanning.Database.UpdateScanningTechnique> |
| Requirement | The system shall provide the capability to update existing scanning techniques in the database. |
| Source | N/A |
| Rationale | To ensure that the scanning techniques in the database are up to date and reflect the latest security practices and vulnerabilities. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

#### < NetworkScanning.Database.RemoveScanningTechnique >

|  |  |
| --- | --- |
| Identifier | 5.11.3 |
| Title | <NetworkScanning.Database.RemoveScanningTechnique> |
| Requirement | The system shall provide the capability to remove outdated or deprecated scanning techniques from the database. |
| Source | N/A |
| Rationale | To ensure that the database only includes relevant and up-to-date scanning techniques, removing any techniques that are no longer applicable or effective. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

#### < NetworkScanning.Database.ExpandScanningTechniques>

|  |  |
| --- | --- |
| Identifier | 5.11.4 |
| Title | <NetworkScanning.Database.ExpandScanningTechniques> |
| Requirement | The system shall regularly expand the available options of scanning techniques in the database based on emerging vulnerabilities and evolving security practices. |
| Source | N/A |
| Rationale | To ensure that the system stays up-to-date with the latest scanning techniques, providing users with a wide range of options to address emerging vulnerabilities and evolving security practices. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

#### < NetworkScanning.Database.VerifyScanningTechniques >

|  |  |
| --- | --- |
| Identifier | 5.11.5 |
| Title | <NetworkScanning.Database.VerifyScanningTechniques> |
| Requirement | The system shall verify and validate the accuracy and effectiveness of scanning techniques in the database to ensure their reliability and relevance. |
| Source | N/A |
| Rationale | By verifying and validating the scanning techniques, the system can ensure that they are accurate, effective, and provide reliable results to users. This helps maintain the integrity of the scanning process and enhances the overall effectiveness of the system. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

#### < NetworkScanning.Database. NotifyScanningTechniqueUpdates>

|  |  |
| --- | --- |
| Identifier | 5.11.6 |
| Title | <NetworkScanning.Database.NotifyScanningTechniqueUpdates> |
| Requirement | The system shall notify users or administrators when new scanning techniques are added or existing techniques are updated in the database. |
| Source | N/A |
| Rationale | By providing notifications for scanning technique updates, users or administrators can stay informed about the latest additions or changes in the scanning techniques database. This allows them to take advantage of new techniques or update their scanning practices accordingly. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Low |

#### < NetworkScanning.Database.AuditScanningTechniqueUpdates >

|  |  |
| --- | --- |
| Identifier | 5.11.7 |
| Title | <NetworkScanning.Database.AuditScanningTechniqueUpdates> |
| Requirement | The system shall maintain an audit trail of changes made to the scanning techniques in the database, including the date, time, and user responsible for the update. |
| Source | N/A |
| Rationale | By maintaining an audit trail of scanning technique updates, the system can ensure accountability and traceability of changes made to the database. This information can be valuable for compliance, troubleshooting, or identifying potential issues related to scanning techniques. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

#### < NetworkScanning.Database.AutomateScanningTechniqueUpdates >

|  |  |
| --- | --- |
| Identifier | FR5.11.8 |
| Title | <NetworkScanning.Database.AutomateScanningTechniqueUpdates> |
| Requirement | The system shall provide automated mechanisms to periodically update the scanning techniques database, ensuring that it stays up-to-date without manual intervention. |
| Source | N/A |
| Rationale | Automated scanning technique updates help ensure that the database is regularly refreshed with the latest information on emerging vulnerabilities and evolving security practices. This allows the system to provide accurate and relevant scanning options to users without requiring manual efforts for updating the database. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

## Report Generation

### < NetworkScanning.Report.GenerateComprehensiveReport >

|  |  |
| --- | --- |
| Identifier | 6.1 |
| Title | <NetworkScanning.Report.GenerateComprehensiveReport> |
| Requirement | The system shall generate a comprehensive report containing scan results, including identified vulnerabilities and their severity. |
| Source | N/A |
| Rationale | Generating a comprehensive report is essential to provide users and administrators with a clear overview of the scan results, including the vulnerabilities identified and their severity levels. This allows for effective communication of the security posture and aids in prioritizing remediation efforts. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

#### < NetworkScanning.Report.Selection >

|  |  |
| --- | --- |
| Identifier | 6.1.1 |
| Title | <NetworkScanning.Report.Selection> |
| Requirement | The interface shall allow users to select the desired scan results and configurations to be included in the report. |
| Source | N/A |
| Rationale | Allowing users to select specific scan results and configurations to be included in the report provides flexibility and customization options. Users can tailor the report to their specific needs, focusing on relevant findings and configurations. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

#### < NetworkScanning.FormatCustomization >

|  |  |
| --- | --- |
| Identifier | 6.1.2 |
| Title | <NetworkScanning.Report.FormatCustomization> |
| Requirement | The interface shall provide options for customizing the report format, such as choosing between PDF, HTML, or CSV. |
| Source | N/A |
| Rationale | Offering customizable report formats allows users to select the format that best suits their needs. Different formats may be preferred for various purposes, such as sharing the report electronically (PDF), importing data into a spreadsheet (CSV), or embedding the report in a web page (HTML). |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

#### < NetworkScanning. Report.Scan >

|  |  |
| --- | --- |
| Identifier | 6.1.3 |
| Title | <NetworkScanning.Report.Scan > |
| Requirement | The interface shall support the generation of reports for individual scans, as well as aggregated reports for multiple scans. |
| Source | N/A |
| Rationale | Providing the ability to generate reports for individual scans allows users to obtain detailed information about a specific scan. Additionally, supporting aggregated reports for multiple scans enables users to consolidate and compare results across multiple scanning instances, facilitating trend analysis and comprehensive reporting. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

#### < NetworkScanning.Report.Recipients >

|  |  |
| --- | --- |
| Identifier | 6.1.4 |
| Title | <NetworkScanning.Report.Recipients> |
| Requirement | The interface shall allow users to specify the target audience or recipients of the generated scan reports. |
| Source | N/A |
| Rationale | Specifying the target audience or recipients of the scan reports ensures that the reports reach the relevant stakeholders who need the information for decision-making, vulnerability remediation, or compliance purposes. By allowing users to define the recipients, the system enables efficient and effective communication of the scan results to the appropriate parties. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

#### < NetworkScanning. Report.Preview >

|  |  |
| --- | --- |
| Identifier | 6.1.5 |
| Title | <NetworkScanning.Report.Preview> |
| Requirement | The interface shall provide a preview or summary of the report contents before generating the final report. |
| Source | N/A |
| Rationale | Providing a preview or summary of the report contents allows users to review and ensure the accuracy and completeness of the information before generating the final report. It helps users make any necessary adjustments or modifications to the report configuration to meet their requirements. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

#### < NetworkScanning. Report. Scheduling >

|  |  |
| --- | --- |
| Identifier | Sub-FR6.1.6 |
| Title | <NetworkScanning.Report.Scheduling> |
| Requirement | The interface shall offer scheduling options for automatically generating and delivering reports at specified intervals. |
| Source | N/A |
| Rationale | Offering scheduling options for report generation and delivery reduces the manual effort and potential delays associated with initiating and distributing reports. Users can set up automated processes to generate and deliver reports at regular intervals, ensuring that relevant stakeholders receive timely and up-to-date information about the scan results. This feature improves productivity, enables proactive vulnerability management, and supports timely decision-making and remediation efforts. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

Top of Form

#### < NetworkScanning. Report.Exporting >

|  |  |
| --- | --- |
| Identifier | 6.1.7 |
| Title | <NetworkScanning.Report.Exporting> |
| Requirement | The interface shall support exporting and saving the generated reports for future reference or sharing with stakeholders. |
| Source | N/A |
| Rationale | Supporting the exporting and saving of generated reports enhances the usability and accessibility of the scan results. Users can save the reports in different formats that suit their needs and share them with relevant stakeholders, such as IT teams, management, or auditors. The ability to export and save reports enables easy integration with other systems, facilitates collaboration, and supports compliance and documentation requirements. It ensures that the valuable information obtained from the scans is preserved and can be effectively utilized in the future. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

### < NetworkScanning.Report.Generation.ScopeAndParameters >

|  |  |
| --- | --- |
| Identifier | 6.2 |
| Title | <NetworkScanning.Report.Generation.ScopeAndParameters> |
| Requirement | The report generation interface shall allow users to specify the scope and parameters for generating the report, such as the target systems, scanning techniques, and time frame. |
| Source | N/A |
| Rationale | Allowing users to specify the scope and parameters for generating the report gives them control over what information is included in the report. Users can customize the report based on their specific needs, focusing on specific target systems, selecting preferred scanning techniques, and defining the time frame for which the scan results are included. This flexibility ensures that the generated report is relevant and tailored to the user's requirements, providing valuable insights and actionable information. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

#### < NetworkScanning.Report.Generation.ScopeAndParameters.TargetSystems >

|  |  |
| --- | --- |
| Identifier | 6.2.1 |
| Title | <NetworkScanning.Report.Generation.ScopeAndParameters.TargetSystems> |
| Requirement | The report generation interface shall provide options for users to specify the target systems or networks for which the report should be generated. |
| Source | N/A |
| Rationale | Specifying the target systems or networks allows users to focus the report generation on specific assets or network segments. Users can select the systems or networks that are of interest or relevance to them, ensuring that the generated report provides insights and findings specific to those targets. This capability enables users to effectively analyze and address vulnerabilities or risks associated with the selected systems or networks, facilitating targeted remediation actions. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

### < NetworkScanning.Report.Compilation >

|  |  |
| --- | --- |
| Identifier | 6.3 |
| Title | <NetworkScanning.Report.Compilation> |
| Requirement | The system shall automatically compile and consolidate the scan results into a comprehensive report, including identified vulnerabilities, their severity levels, and associated details. |
| Source | N/A |
| Rationale | The automatic compilation of scan results into a comprehensive report eliminates the need for manual data aggregation and reduces the risk of human error. By consolidating the scan results, the system provides a centralized and consistent view of the identified vulnerabilities, their severity levels, and relevant details such as affected hosts, vulnerability descriptions, and recommended remediation actions. This automation streamlines the reporting process, saves time and effort, and ensures that the generated reports are accurate, complete, and readily available for analysis, decision-making, and remediation activities. |
| Business Rule | N/A |
| Dependencies | The system must have access to the scan results database. |
| Priority | High |

### < NetworkScanning.Report. GraphicalElements >

|  |  |
| --- | --- |
| Identifier | 6.4 |
| Title | <NetworkScanning.Report.GraphicalElements> |
| Requirement | The report interface shall support the inclusion of graphical elements, such as charts or graphs, to visualize the distribution of vulnerabilities by severity or other attributes. |
| Source | N/A |
| Rationale | Including graphical elements in the report enhances the visual representation of vulnerability distribution, making it easier for users to understand and interpret the data. Charts or graphs can provide an overview of vulnerabilities by severity levels, their trends over time, or their distribution across different systems or networks. These visualizations help stakeholders quickly identify areas of concern, prioritize remediation efforts, and communicate the impact of vulnerabilities to relevant parties. By presenting information in a visually appealing and intuitive manner, graphical elements improve the effectiveness and usability of the generated reports. |
| Business Rule | N/A |
| Dependencies | 6.2, 6.2 |
| Priority | Medium |

### < NetworkScanning.Report.CustomAnnotations >

|  |  |
| --- | --- |
| Identifier | 6.5 |
| Title | <NetworkScanning.Report.CustomAnnotations> |
| Requirement | The report interface shall allow users to add custom annotations, comments, or supplementary information to the generated report, facilitating collaboration and knowledge sharing. |
| Source | N/A |
| Rationale | Allowing users to add custom annotations, comments, or supplementary information to the generated report promotes collaboration and knowledge sharing among stakeholders. Users can provide additional context, insights, or recommendations related to identified vulnerabilities, enabling better understanding and decision-making. Custom annotations and comments facilitate communication between security teams, IT personnel, management, or auditors, fostering collaboration and improving the effectiveness of vulnerability remediation efforts. By providing a mechanism for users to contribute their expertise and insights, the report interface enhances the value and utility of the generated reports. |
| Business Rule | N/A |
| Dependencies | None |
| Priority | Medium |

### < NetworkScanning.Report.CustomAnnotations >

|  |  |
| --- | --- |
| Identifier | 6.6 |
| Title | <NetworkScanning.Report.AccuracyConsistency> |
| Requirement | The system shall ensure the accuracy and consistency of the generated reports, verifying that all relevant scan results are correctly included and categorized. |
| Source | N/A |
| Rationale | Ensuring the accuracy and consistency of generated reports is crucial for reliable vulnerability assessment and decision-making. By verifying that all relevant scan results are correctly included and categorized, the system guarantees that the reports provide an accurate representation of the network's security posture. This verification process helps identify and rectify any potential errors or omissions, ensuring that stakeholders have complete and reliable information to act upon. Accuracy and consistency are essential for effective vulnerability management and aligning with industry standards and best practices. |
| Business Rule | N/A |
| Dependencies | None |
| Priority | High |

## Pause Scanning

### < NetworkScanning.PauseScanning >

|  |  |
| --- | --- |
| Identifier | 7.1 |
| Title | <NetworkScanning.PauseScanning> |
| Requirement | The system shall allow users to pause an ongoing network scanning process. |
| Source | N/A |
| Rationale | Network scanning processes can sometimes take a significant amount of time to complete, depending on the size and complexity of the network. In certain situations, users may need to pause the scanning process temporarily to address other priorities or to avoid performance impacts on the network or target systems. Providing the ability to pause the scanning process allows users to have better control over the scanning activities and can help them manage resources more effectively. |
| Business Rule | N/A |
| Dependencies | None |
| Priority | Medium |

## Restart Scanning

|  |  |
| --- | --- |
| Identifier | 8.1 |
| Title | <NetworkScanning.ResumeScanning> |
| Requirement | The system shall provide the option to resume the paused scanning process from where it left off. |
| Source | N/A |
| Rationale | Pausing a scanning process allows users to temporarily suspend the scanning activities. To ensure the efficiency of the scanning process and avoid redoing the previously scanned targets, it is essential to provide the option to resume the scanning from the point where it was paused. This feature enables users to pick up where they left off and continue the scanning process seamlessly, saving time and resources. |
| Business Rule | N/A |
| Dependencies | FR7 |
| Priority | Medium |

## Dashboard Updating

### < DashboardUpdating.RealTimeData >

|  |  |
| --- | --- |
| Identifier | 9.1 |
| Title | <DashboardUpdating.RealTimeData> |
| Requirement | The system shall provide real-time data updates on the dashboard. |
| Source | N/A |
| Rationale | Real-time data updates on the dashboard allow users to have immediate access to the most current information. This feature ensures that the dashboard reflects the latest status of the network, system, or application being monitored. It enables users to make informed decisions based on real-time data and enhances situational awareness and responsiveness. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

### < DashboardUpdating.Customization >

|  |  |
| --- | --- |
| Identifier | 9.2 |
| Title | <DashboardUpdating.Customization> |
| Requirement | The system shall allow users to customize the dashboard layout and content. |
| Source | N/A |
| Rationale | Providing customization options for the dashboard allows users to tailor the layout and content based on their specific needs and preferences. This feature enhances user experience and flexibility, as users can prioritize and display the information that is most relevant to their monitoring and analysis tasks. Customization capabilities also support different user roles and their specific monitoring requirements. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

### < DashboardUpdating.Widgets >

|  |  |
| --- | --- |
| Identifier | 9.3 |
| Title | <DashboardUpdating.Widgets> |
| Requirement | The system shall offer a variety of widgets for displaying different types of data on the dashboard. |
| Source | N/A |
| Rationale | Having a range of widgets available for displaying various types of data allows users to visualize and interpret information in a meaningful way. Widgets can include charts, graphs, tables, or other visual elements that present data in a clear and concise manner. By offering a diverse set of widgets, the system caters to different data visualization needs and enhances the effectiveness of the dashboard as a monitoring and analysis tool. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

### <DashboardUpdating.AlertNotifications>

|  |  |
| --- | --- |
| Identifier | 9.4 |
| Title | <DashboardUpdating.AlertNotifications> |
| Requirement | The system shall provide alert notifications on the dashboard for critical events or anomalies. |
| Source | N/A |
| Rationale | Alert notifications on the dashboard allow users to quickly identify and respond to critical events or anomalies in the monitored systems or applications. These notifications can be in the form of visual alerts, pop-up messages, or audible alarms, drawing immediate attention to important incidents that require action. This feature enables proactive monitoring and response, helping to minimize downtime, mitigate risks, and ensure the overall security and performance of the network or system. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

### <DashboardUpdating.DataVisualization >

|  |  |
| --- | --- |
| Identifier | 9.5 |
| Title | <DashboardUpdating.DataVisualization> |
| Requirement | The system shall provide data visualization capabilities on the dashboard. |
| Source | N/A |
| Rationale | Data visualization plays a crucial role in understanding complex information and identifying patterns or trends. By offering data visualization capabilities on the dashboard, users can analyze and interpret data more effectively. This feature can include interactive charts, graphs, heatmaps, or other visual representations that help users grasp information intuitively and make informed decisions. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

### <DashboardUpdating.DataRefreshRate >

|  |  |
| --- | --- |
| Identifier | 9.6 |
| Title | <DashboardUpdating.DataRefreshRate> |
| Requirement | The system shall allow users to configure the refresh rate of the dashboard data. |
| Source | N/A |
| Rationale | The ability to configure the data refresh rate provides users with control over the frequency at which the dashboard updates its information. Users can set the refresh rate based on their monitoring requirements, system performance considerations, or data volatility. This feature ensures that the dashboard displays the most up-to-date information while optimizing resource utilization. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Low |

### <DashboardUpdating.DataVisualization >

|  |  |
| --- | --- |
| Identifier | 9.7 |
| Title | <DashboardUpdating.DataVisualization > |
| Requirement | The system shall support integration with various devices or systems to gather data for the dashboard. |
| Source | N/A |
| Rationale | Many monitoring systems rely on data collected from multiple devices or systems. By supporting device integration, the system can gather relevant data from diverse sources and present it on the dashboard. This feature enables holistic monitoring by consolidating data from various devices or systems into a single interface, providing users with a comprehensive view of the monitored environment. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

### <DashboardUpdating.DataFilters >

|  |  |
| --- | --- |
| Identifier | 9.8 |
| Title | <DashboardUpdating.DataFilters> |
| Requirement | The system shall allow users to apply data filters on the dashboard to focus on specific information. |
| Source | N/A |
| Rationale | Data filters enhance the usability and flexibility of the dashboard by enabling users to narrow down the displayed information based on specific criteria or attributes. Users can apply filters such as time range, device category, severity level, or other relevant parameters to customize the dashboard view according to their monitoring needs. This feature promotes efficient data analysis, reduces information overload, and improves user experience. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

### <DashboardUpdating.DataFilters >

|  |  |
| --- | --- |
| Identifier | 9.9 |
| Title | <DashboardUpdating.UserCustomization> |
| Requirement | The system shall allow users to customize the layout and appearance of the dashboard. |
| Source | N/A |
| Rationale | User customization empowers users to personalize the dashboard according to their preferences and monitoring requirements. This feature can include options for rearranging widgets, resizing components, selecting color themes, or adding custom branding elements. User customization enhances the user experience, improves productivity, and allows users to tailor the dashboard to their specific needs and preferences. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Low |

## Data Aggregation

### <DataAggregation.Integration>

|  |  |
| --- | --- |
| Identifier | 10.1 |
| Title | <DataAggregation.Integration> |
| Requirement | The system shall integrate with multiple data sources, including network scanning tools, threat intelligence feeds, and user activity logs, to gather relevant security data. |
| Source | N/A |
| Rationale | Integrating with diverse data sources allows the system to collect a wide range of security-related information. Network scanning tools provide insights into vulnerabilities and weaknesses in the network infrastructure. Threat intelligence feeds offer up-to-date information on emerging threats and known attack patterns. User activity logs provide visibility into user behavior and potential security incidents. By aggregating data from these sources, the system can provide a comprehensive and holistic view of the security posture. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

### <DataAggregation. Synchronization>

|  |  |
| --- | --- |
| Identifier | 10.2 |
| Title | <DataAggregation.Synchronization> |
| Requirement | The system shall regularly synchronize and update data from integrated sources to ensure the freshness and accuracy of the aggregated information. |
| Source | N/A |
| Rationale | Regular synchronization and updates of data from integrated sources are necessary to ensure that the aggregated information remains up-to-date and reflects the current state of the security environment. By continuously retrieving and incorporating new data, the system can provide users with real-time insights and enable timely decision-making. |
| Business Rule | N/A |
| Dependencies | FR10.1 |
| Priority | Medium |

### <DataAggregation.Validation >

|  |  |
| --- | --- |
| Identifier | 10.3 |
| Title | <DataAggregation.Validation> |
| Requirement | The system shall perform data validation and cleansing processes to ensure the integrity and reliability of the aggregated data. |
| Source | N/A |
| Rationale | Data integrity and reliability are crucial for accurate analysis and decision-making. The system should implement validation and cleansing processes to identify and rectify any inconsistencies, errors, or anomalies in the aggregated data. By ensuring data quality, the system enhances the reliability and trustworthiness of the insights derived from the aggregated information. |
| Business Rule | N/A |
| Dependencies | FR10.1 |
| Priority | High |

### <DataAggregation.Logging >

|  |  |
| --- | --- |
| Identifier | 10.4 |
| Title | <DataAggregation.Logging> |
| Requirement | The system shall log and track data integration activities, including the source, timestamp, and outcome of each data retrieval process. |
| Source | N/A |
| Rationale | Logging and tracking data integration activities provide an audit trail and enable traceability of data sources and retrieval processes. This information is valuable for troubleshooting, monitoring, and ensuring compliance with data governance and security policies. By maintaining comprehensive logs, the system enhances transparency and accountability in the data aggregation process. |
| Business Rule | N/A |
| Dependencies | FR10.1 |
| Priority | Medium |

## Machine Learning-Based Vulnerability Detection

### < MachineLearning.Training >

.

|  |  |
| --- | --- |
| Identifier | 11.1 |
| Title | <MachineLearning.Training> |
| Description | The system shall train the machine learning models using labeled data that includes known vulnerabilities. |
| Source | N/A |
| Rationale | Training machine learning models using labeled data allows the system to learn patterns and characteristics of known vulnerabilities. By providing the system with a dataset that includes labeled vulnerabilities, it can build models that can accurately classify and detect similar vulnerabilities in the future. Training the models is a crucial step in ensuring the effectiveness and accuracy of the vulnerability detection system. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

### < MachineLearning.ModelRefinement >

|  |  |
| --- | --- |
| Identifier | 11.2 |
| Title | <MachineLearning.ModelRefinement> |
| Description | The system shall continuously update and refine the machine learning models based on new data and emerging vulnerabilities. |
| Source | N/A |
| Rationale | As new vulnerabilities are discovered and security threats evolve, it is essential for the machine learning models to adapt and stay up-to-date. By continuously updating and refining the models, the system can improve its detection capabilities and ensure that it can effectively identify emerging vulnerabilities. Regular model refinement helps maintain the system's accuracy and relevance in the ever-changing security landscape. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

### < MachineLearning.Classification >

|  |  |
| --- | --- |
| Identifier | 11.3 |
| Title | <MachineLearning.Classification> |
| Description | The system shall classify detected vulnerabilities based on severity levels. |
| Source | N/A |
| Rationale | Classification of vulnerabilities based on severity levels helps prioritize remediation efforts and enables effective risk management. By leveraging machine learning algorithms, the system can automatically assign severity levels to detected vulnerabilities, allowing users to focus on addressing the most critical security issues first. This feature enhances the system's efficiency and helps organizations efficiently allocate resources for vulnerability management. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

### < MachineLearning.Accuracy >

|  |  |
| --- | --- |
| Identifier | 11.4 |
| Title | <MachineLearning.Accuracy> |
| Description | The system shall provide accurate and reliable vulnerability detection with a low false positive rate. |
| Source | N/A |
| Rationale | Accurate and reliable vulnerability detection is crucial for effective security management. By minimizing false positives, the system ensures that detected vulnerabilities are genuine and require attention. This feature reduces the manual effort required to investigate false positives, allowing security teams to focus on addressing legitimate security risks. Additionally, low false positives improve user trust in the system and increase overall confidence in the vulnerability detection process. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

### < MachineLearning.NetworkTrafficAnalysis >

|  |  |
| --- | --- |
| Identifier | 11.5 |
| Title | <MachineLearning.NetworkTrafficAnalysis> |
| Description | The system shall analyze network traffic patterns and system behavior to identify potential vulnerabilities. |
| Source | N/A |
| Rationale | Analyzing network traffic patterns and system behavior is an effective way to identify potential vulnerabilities. By leveraging machine learning techniques, the system can detect anomalies and patterns indicative of security risks. This feature enhances the system's ability to proactively identify vulnerabilities, even in complex and dynamic network environments. It allows security teams to stay ahead of emerging threats and take appropriate mitigation actions in a timely manner. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

### < MachineLearning.Integration>

|  |  |
| --- | --- |
| Identifier | 11.6 |
| Title | <MachineLearning.Integration> |
| Description | The system shall integrate with vulnerability databases and security feeds to enhance the accuracy of vulnerability detection. |
| Source | N/A |
| Rationale | Integrating with vulnerability databases and security feeds provides the system with up-to-date information about known vulnerabilities and emerging threats. By leveraging this external intelligence, the system can improve the accuracy and effectiveness of vulnerability detection. It ensures that the system is aware of the latest security risks and can identify vulnerabilities based on the most current information available. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

### < MachineLearning.Alerts>

|  |  |
| --- | --- |
| Identifier | 11.7 |
| Title | <MachineLearning.Alerts> |
| Description | The system shall generate alerts or notifications when high-severity vulnerabilities are detected. |
| Source | N/A |
| Rationale | Generating alerts or notifications for high-severity vulnerabilities allows for timely response and remediation. By alerting users or administrators, immediate action can be taken to mitigate the risk associated with critical vulnerabilities. This requirement ensures that high-severity vulnerabilities are given priority attention and appropriate measures are taken to address them promptly. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

### < MachineLearning.VulnerabilityInformation >

|  |  |
| --- | --- |
| Identifier | 11.8 |
| Title | <MachineLearning.VulnerabilityInformation> |
| Description | The system shall provide detailed information about detected vulnerabilities, including their description, impact, and recommended remediation actions. |
| Source | N/A |
| Rationale | Providing detailed information about detected vulnerabilities is crucial for effective vulnerability management. Users need to understand the nature, potential impact, and recommended actions to address the vulnerabilities. This requirement ensures that the system delivers comprehensive information about vulnerabilities, enabling users to make informed decisions and prioritize remediation efforts based on the severity and potential risks associated with each vulnerability. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

### < MachineLearning.VulnerabilityPrioritization >

|  |  |
| --- | --- |
| Identifier | 11.9 |
| Title | <MachineLearning.VulnerabilityPrioritization> |
| Description | The system shall prioritize vulnerabilities based on their severity and potential impact on the network or systems. |
| Source | N/A |
| Rationale | Prioritizing vulnerabilities is essential for effective vulnerability management. By considering factors such as severity and potential impact, the system can help users focus on addressing the most critical vulnerabilities first. This requirement ensures that the system provides a mechanism to assess and prioritize vulnerabilities, enabling efficient resource allocation and timely remediation efforts to mitigate the highest risks. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

### < MachineLearning.VisualizationAndReporting >

|  |  |
| --- | --- |
| Identifier | 11.10 |
| Title | <MachineLearning.VisualizationAndReporting> |
| Description | The system shall provide visualization and reporting features to present vulnerability detection results in a clear and understandable manner. |
| Source | N/A |
| Rationale | Visualization and reporting are crucial for communicating vulnerability detection results effectively. By providing visual representations, such as charts, graphs, or dashboards, and comprehensive reports, the system enhances the understanding of detected vulnerabilities and facilitates decision-making and remediation efforts. This requirement ensures that the system includes features to visualize and report vulnerability detection results in a clear and understandable manner, promoting efficient analysis and action by the users. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

### < MachineLearning.AlgoCustomization >

|  |  |
| --- | --- |
| Identifier | 11.11 |
| Title | <MachineLearning.AlgoCustomization> |
| Description | The system shall support customization of machine learning models and algorithms to adapt to different network and system environments. |
| Source | N/A |
| Rationale | Network and system environments can vary greatly, and different organizations may have unique requirements and characteristics. By allowing customization of machine learning models and algorithms, the system can be tailored to specific environments, improving the accuracy and effectiveness of vulnerability detection. This requirement ensures that the system provides the flexibility to customize and adapt machine learning components to meet the needs of different network and system environments. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

## Threat Intelligence Gathering

### < ThreatIntelligence.DataGatheringAndAnalysis >

|  |  |
| --- | --- |
| Identifier | 12.1 |
| Title | <ThreatIntelligence.DataGatheringAndAnalysis> |
| Description | The system shall gather and analyze threat intelligence data from reliable sources, such as security feeds, databases, and online forums. |
| Source | N/A |
| Rationale | Threat intelligence plays a crucial role in identifying and mitigating potential security threats. By gathering and analyzing data from reliable sources, the system can enhance its understanding of current and emerging threats, improve the accuracy of its detection capabilities, and provide timely and effective responses to security incidents. This requirement ensures that the system has the capability to collect and process threat intelligence data from diverse sources, enabling proactive threat detection and response. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

### < ThreatIntelligence.Integration >

|  |  |
| --- | --- |
| Identifier | 12.2 |
| Title | <ThreatIntelligence.Integration> |
| Description | The system shall establish connections and integrate with reliable threat intelligence feeds and databases. |
| Source | N/A |
| Rationale | Integrating with reliable threat intelligence feeds and databases allows the system to access up-to-date and relevant information about known threats and vulnerabilities. By establishing connections with these sources, the system can gather and leverage threat intelligence data to enhance its detection and response capabilities. This requirement ensures that the system has the necessary integration capabilities to connect with trusted threat intelligence sources and access the latest information for effective threat analysis and mitigation. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

### < ThreatIntelligence.DataUpdate >

|  |  |
| --- | --- |
| Identifier | 12.3 |
| Title | <ThreatIntelligence.DataUpdate> |
| Description | The system shall regularly retrieve and update threat intelligence data from the integrated sources. |
| Source | N/A |
| Rationale | Regularly retrieving and updating threat intelligence data from integrated sources ensures that the system has access to the most current and relevant information about emerging threats and vulnerabilities. By keeping the threat intelligence data up-to-date, the system can improve its ability to detect and respond to evolving threats in a timely manner. This requirement ensures that the system implements mechanisms to regularly fetch and update the threat intelligence data from the integrated sources, maintaining the accuracy and effectiveness of its threat analysis capabilities. |
| Business Rule | N/A |
| Dependencies | FR13.1 |
| Priority | Medium |

### < ThreatIntelligence.DataValidation >

|  |  |
| --- | --- |
| Identifier | 12.4 |
| Title | <ThreatIntelligence.DataValidation> |
| Description | The system shall validate the authenticity and reliability of the gathered threat intelligence data. |
| Source | N/A |
| Rationale | Validating the authenticity and reliability of the gathered threat intelligence data ensures that the system relies on trustworthy and accurate information for threat analysis. By implementing data validation mechanisms, the system can verify the source credibility, integrity, and trustworthiness of the gathered threat intelligence data. This requirement ensures that the system includes mechanisms to assess and validate the authenticity and reliability of the gathered data, enhancing the overall accuracy and effectiveness of its threat analysis capabilities. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

### < ThreatIntelligence.DataStorage >

|  |  |
| --- | --- |
| Identifier | 12.5 |
| Title | <ThreatIntelligence.DataStorage> |
| Description | The system shall store and organize the threat intelligence data in a structured manner for efficient analysis. |
| Source | N/A |
| Rationale | Storing and organizing the threat intelligence data in a structured manner enables efficient and effective analysis. By structuring the data, the system can easily retrieve, query, and analyze the information, allowing for faster and more accurate threat analysis. This requirement ensures that the system implements appropriate data storage and organization mechanisms to optimize the efficiency of its threat intelligence analysis processes. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

### < ThreatIntelligence.DataParsing >

|  |  |
| --- | --- |
| Identifier | 12.6 |
| Title | <ThreatIntelligence.DataParsing> |
| Description | The system shall perform automated parsing and extraction of relevant information from the gathered data. |
| Source | N/A |
| Rationale | Automated parsing and extraction of relevant information from the gathered data reduces manual effort and improves the efficiency of threat intelligence analysis. By implementing automated parsing techniques, the system can extract key information, such as indicators of compromise (IOCs), threat actor profiles, or attack techniques, from the gathered data. This requirement ensures that the system includes automated parsing and extraction mechanisms to process the gathered data and extract relevant information for analysis and threat detection purposes. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

### < ThreatIntelligence. DataNormalization >

|  |  |
| --- | --- |
| Identifier | 12.7 |
| Title | <ThreatIntelligence.DataNormalization> |
| Description | The system shall normalize and standardize the threat intelligence data for effective analysis and comparison. |
| Source | N/A |
| Rationale | Normalizing and standardizing the threat intelligence data enables effective analysis, comparison, and correlation of different information sources. By applying normalization and standardization techniques, the system can ensure consistency, accuracy, and compatibility of the gathered data, facilitating meaningful analysis and correlation of threat intelligence. This requirement ensures that the system includes mechanisms to normalize and standardize the threat intelligence data, enhancing the overall effectiveness and reliability of its threat analysis capabilities. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

### < ThreatIntelligence.DataAnalytics >

|  |  |
| --- | --- |
| Identifier | 12.8 |
| Title | <ThreatIntelligence.DataAnalytics> |
| Description | The system shall employ data analytics techniques to identify patterns, trends, and emerging threats. |
| Source | N/A |
| Rationale | Employing data analytics techniques allows the system to uncover patterns, trends, and emerging threats from the gathered threat intelligence data. By applying analytics algorithms, statistical analysis, and data mining techniques, the system can identify anomalies, detect trends, and gain insights into emerging threats. This requirement ensures that the system leverages data analytics techniques to enhance its ability to identify and respond to evolving security threats. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

### < ThreatIntelligence.MachineLearningClassification >

|  |  |
| --- | --- |
| Identifier | 12.9 |
| Title | <ThreatIntelligence.MachineLearningClassification> |
| Description | The system shall utilize machine learning algorithms to classify and prioritize the gathered threat intelligence. |
| Source | N/A |
| Rationale | Utilizing machine learning algorithms enables the system to automate the classification and prioritization of threat intelligence data. By training machine learning models on labeled data, the system can automatically classify and prioritize the gathered threat intelligence based on various factors such as severity, likelihood, or impact. This requirement ensures that the system incorporates machine learning capabilities to enhance its ability to effectively categorize and prioritize threat intelligence for efficient threat response. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

### < ThreatIntelligence.NaturalLanguageProcessing>

|  |  |
| --- | --- |
| Identifier | 12.10 |
| Title | <ThreatIntelligence.NaturalLanguageProcessing> |
| Description | The system shall apply natural language processing techniques to extract actionable information from unstructured threat intelligence data. |
| Source | N/A |
| Rationale | Applying natural language processing (NLP) techniques allows the system to extract actionable information from unstructured threat intelligence data, such as security reports, articles, or blogs. By leveraging NLP algorithms, the system can analyze text and extract relevant information, such as indicators, attack techniques, or vulnerability details. This requirement ensures that the system incorporates NLP capabilities to enhance its ability to extract actionable insights from unstructured threat intelligence data. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

## Notification and Alert Generation

### < NotificationAlertGeneration.RealTimeGeneration >

|  |  |
| --- | --- |
| Identifier | 13.1 |
| Title | <NotificationAlertGeneration.RealTimeGeneration> |
| Description | The system shall generate real-time notifications and alerts for identified vulnerabilities, security breaches, or suspicious activities. |
| Source | N/A |
| Rationale | Generating real-time notifications and alerts allows for immediate awareness and response to identified vulnerabilities, security breaches, or suspicious activities. By providing timely information to relevant stakeholders, the system enables prompt action to mitigate risks and address security incidents. This requirement ensures that the system has the capability to generate real-time notifications and alerts for the identified security events. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

### < NotificationAlertGeneration.NetworkScanMonitoring >

|  |  |
| --- | --- |
| Identifier | 13.2 |
| Title | <NotificationAlertGeneration.NetworkScanMonitoring> |
| Description | The system shall monitor network scans and vulnerability assessments in real-time. |
| Source | N/A |
| Rationale | Monitoring network scans and vulnerability assessments in real-time enables the system to identify potential vulnerabilities as soon as they are detected. By continuously monitoring and analyzing the scan results, the system can promptly generate notifications and alerts for the identified vulnerabilities, facilitating timely remediation. This requirement ensures that the system has the capability to monitor network scans and vulnerability assessments in real-time. |
| Business Rule | N/A |
| Dependencies | 13 |
| Priority | Medium |

### < NotificationAlertGeneration.NewVulnerabilityDetection >

|  |  |
| --- | --- |
| Identifier | 13.3 |
| Title | <NotificationAlertGeneration.NewVulnerabilityDetection> |
| Description | The system shall detect and identify newly discovered vulnerabilities in real-time. |
| Source | N/A |
| Rationale | Detecting and identifying newly discovered vulnerabilities in real-time allows for immediate action to address the associated risks. By continuously monitoring and analyzing vulnerability feeds, security advisories, and other relevant sources, the system can promptly generate notifications and alerts for the newly identified vulnerabilities. This requirement ensures that the system has the capability to detect and identify newly discovered vulnerabilities in real-time. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

### < NotificationAlertGeneration.SecurityBreachDetection >

|  |  |
| --- | --- |
| Identifier | 13.4 |
| Title | <NotificationAlertGeneration.SecurityBreachDetection> |
| Description | The system shall detect and identify security breaches or unauthorized access attempts in real-time. |
| Source | N/A |
| Rationale | Detecting and identifying security breaches or unauthorized access attempts in real-time is crucial for timely response and mitigation. By monitoring system logs, network traffic, and other relevant data sources, the system can identify anomalous activities and generate notifications and alerts for potential security incidents. This requirement ensures that the system has the capability to detect and identify security breaches or unauthorized access attempts in real-time. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

### < NotificationAlertGeneration.SuspiciousActivityIdentification >

|  |  |
| --- | --- |
| Identifier | 13.5 |
| Title | <NotificationAlertGeneration.SuspiciousActivityIdentification> |
| Description | The system shall analyze network traffic and system logs to identify suspicious activities in real-time. |
| Source | N/A |
| Rationale | Analyzing network traffic and system logs in real-time enables the system to identify potential security threats and suspicious activities as they occur. By applying intelligent algorithms and detection techniques, the system can generate notifications and alerts for anomalous behaviors and indicators of compromise. This requirement ensures that the system has the capability to analyze network traffic and system logs to identify suspicious activities in real-time. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

### < NotificationAlertGeneration. NotificationPreferences >

|  |  |
| --- | --- |
| Identifier | 13.6 |
| Title | <NotificationAlertGeneration.NotificationPreferences> |
| Description | The system shall provide configurable notification preferences for administrators and users. |
| Source | N/A |
| Rationale | Providing configurable notification preferences allows administrators and users to customize the types and frequency of notifications they receive. Different stakeholders may have varying needs and preferences regarding the level of detail and frequency of notifications. This requirement ensures that the system has the capability to provide configurable notification preferences for administrators and users. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

### < NotificationAlertGeneration.AdministratorActions >

|  |  |
| --- | --- |
| Identifier | 13.7 |
| Title | <NotificationAlertGeneration.AdministratorActions> |
| Description | The system shall provide mechanisms for administrators to acknowledge, escalate, or resolve notifications and alerts. |
| Source | N/A |
| Rationale | Providing mechanisms for administrators to acknowledge, escalate, or resolve notifications and alerts allows for effective incident management and response. Administrators need the ability to acknowledge the receipt of a notification, escalate it to the appropriate team or personnel for further action, or mark it as resolved once the issue has been addressed. This requirement ensures that the system provides the necessary mechanisms for administrators to perform these actions. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

### < NotificationAlertGeneration.HistoryArchive >

|  |  |
| --- | --- |
| Identifier | 13.8 |
| Title | <NotificationAlertGeneration.HistoryArchive> |
| Description | The system shall provide notification history and an archive of past alerts for reference and review. |
| Source | N/A |
| Rationale | Maintaining a notification history and archive allows users to review past alerts, track the resolution of issues, and perform trend analysis. This requirement ensures that the system retains a record of past notifications and alerts, providing users with a valuable reference for incident management, analysis, and reporting purposes. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

### < NotificationAlertGeneration.IncidentResponseIntegration >

|  |  |
| --- | --- |
| Identifier | 13.9 |
| Title | <NotificationAlertGeneration.IncidentResponseIntegration> |
| Description | The system shall integrate with external incident response systems or ticketing systems for seamless handling of identified vulnerabilities and security incidents. |
| Source | N/A |
| Rationale | Integration with external incident response systems or ticketing systems enhances the overall incident management process. This requirement ensures that the system can seamlessly exchange information with such systems, enabling efficient and coordinated handling of identified vulnerabilities and security incidents. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

### < NotificationAlertGeneration.AutomaticRemediation >

|  |  |
| --- | --- |
| Identifier | 13.10 |
| Title | <NotificationAlertGeneration.AutomaticRemediation> |
| Description | The system shall support automatic remediation actions or workflows triggered by specific notifications or alerts. |
| Source | N/A |
| Rationale | Automating remediation actions or workflows based on specific notifications or alerts can help streamline the response process and minimize the time to resolve issues. This requirement ensures that the system provides the capability to define and execute automated remediation actions or workflows in response to certain notifications or alerts, improving incident response efficiency. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

### < NotificationAlertGeneration.RecipientDelivery >

|  |  |
| --- | --- |
| Identifier | 13.11 |
| Title | <NotificationAlertGeneration.RecipientDelivery> |
| Description | The system shall ensure that notifications and alerts are delivered to the appropriate recipients based on their roles and responsibilities. |
| Source | N/A |
| Rationale | Delivering notifications and alerts to the right recipients based on their roles and responsibilities is crucial for effective incident response. This requirement ensures that the system has mechanisms in place to determine the appropriate recipients for each notification or alert, ensuring that the information reaches the relevant individuals or teams responsible for taking action. |
| Business Rule | N/A |
| Dependencies | FR15 |
| Priority | High |

## Remediation Plan Checking

|  |  |
| --- | --- |
| Identifier | 14 |
| Title | <RemediationReview.Validation> |
| Description | The system shall facilitate the review and validation of remediation plans proposed to address identified vulnerabilities. |
| Source | N/A |
| Rationale | Once vulnerabilities are identified, it is crucial to develop effective remediation plans to address them. This requirement emphasizes that the system should provide features and functionalities to facilitate the review and validation of proposed remediation plans. This includes allowing administrators or authorized personnel to assess and evaluate the proposed plans, ensuring that they are appropriate, feasible, and effective in mitigating the identified vulnerabilities. By facilitating the review and validation process, the system helps to ensure that appropriate actions are taken to address vulnerabilities and improve the overall security posture. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

### < RemediationReview.CentralizedInterface >

|  |  |
| --- | --- |
| Identifier | 14.1 |
| Title | <RemediationReview.CentralizedInterface> |
| Description | The system shall provide a centralized interface for reviewing and managing proposed remediation plans. |
| Source | N/A |
| Rationale | To facilitate the review and management of proposed remediation plans, it is essential to have a centralized interface within the system. This interface should serve as a single point of access for authorized personnel to view and assess the proposed plans. By providing a centralized interface, the system ensures that the review and management process is streamlined and easily accessible to stakeholders involved in the remediation process. It promotes efficiency and collaboration by consolidating all relevant information and functionalities in one location. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

### < RemediationReview.VulnerabilitySummary >

|  |  |
| --- | --- |
| Identifier | 14.2 |
| Title | <RemediationReview.VulnerabilitySummary> |
| Description | The system shall display a summary of identified vulnerabilities along with corresponding proposed remediation plans. |
| Source | N/A |
| Rationale | To provide an overview of the remediation efforts, it is necessary to display a summary of identified vulnerabilities and their associated remediation plans. This summary view allows reviewers to quickly grasp the scope and severity of the vulnerabilities and assess the overall remediation progress. By presenting the information in a concise and informative manner, the system enables efficient decision-making and prioritization of remediation efforts. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

### < RemediationReview. StatusProgressTracking>

|  |  |
| --- | --- |
| Identifier | 14.3 |
| Title | <RemediationReview.StatusProgressTracking> |
| Description | The system shall track the status and progress of approved remediation plans. |
| Source | N/A |
| Rationale | To ensure visibility and accountability, the system should track the status and progress of approved remediation plans. This tracking functionality allows stakeholders to monitor the implementation and completion of approved plans. By providing clear visibility into the status and progress, the system enables effective oversight, facilitates communication between relevant parties, and ensures that remediation efforts are progressing as planned. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

### < RemediationReview. StatusProgressTracking>

|  |  |
| --- | --- |
| Identifier | 14.4 |
| Title | <RemediationReview.StatusProgressTracking > |
| Description | The system shall provide notifications and alerts for pending remediation plan reviews and deadlines. |
| Source | N/A |
| Rationale | To ensure timely and efficient review and validation of remediation plans, the system should provide notifications and alerts to users involved in the process. These notifications can inform reviewers about pending reviews, approaching deadlines, or any updates or changes made to the plans. By providing proactive notifications and alerts, the system helps users stay informed and ensures that the review process progresses smoothly and on schedule. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

## SystemUpdate

### < SystemUpdates.DownloadInstall >

|  |  |
| --- | --- |
| Identifier | 15.1 |
| Title | <SystemUpdates.DownloadInstall> |
| Description | The system shall provide a mechanism for downloading and installing new vulnerability signatures, security patches, and software enhancements. |
| Source | N/A |
| Rationale | To maintain the security, stability, and functionality of the system, it is important to have a mechanism for downloading and installing new vulnerability signatures, security patches, and software enhancements. This allows the system to stay up-to-date with the latest security fixes, performance improvements, and new features. By providing a reliable mechanism for updates, the system can effectively address vulnerabilities, mitigate risks, and enhance overall system performance. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

### < SystemUpdates.AutomaticUpdates >

|  |  |
| --- | --- |
| Identifier | 15.2 |
| Title | <SystemUpdates.AutomaticUpdates> |
| Description | The system shall support automatic updates to ensure timely incorporation of new releases and updates. |
| Source | N/A |
| Rationale | To streamline the update process and ensure timely incorporation of new releases and updates, the system should support automatic updates. Automatic updates eliminate the need for manual intervention and reduce the risk of delayed or missed updates. By automatically applying new releases and updates, the system can maintain the latest security patches, bug fixes, and enhancements, improving the overall performance, reliability, and security of the system. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

### < SystemUpdates.UpdateNotifications>

|  |  |
| --- | --- |
| Identifier | 15.3 |
| Title | <SystemUpdates.UpdateNotifications> |
| Description | The system shall notify users about the availability of new updates and provide instructions for their installation. |
| Source | N/A |
| Rationale | To keep users informed and ensure that updates are applied in a timely manner, the system should provide notifications about the availability of new updates. Notifications can alert users to important updates, such as security patches or critical bug fixes, and provide instructions or guidance on how to install or apply the updates. By notifying users and providing clear instructions, the system promotes user awareness, encourages prompt action, and facilitates the successful installation of updates to maintain system integrity and security. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

### < SystemUpdates.VersionControl>

|  |  |
| --- | --- |
| Identifier | 15.4 |
| Title | <SystemUpdates.VersionControl> |
| Description | The system shall maintain a version control system to track the installed version and update history. |
| Source | N/A |
| Rationale | To keep track of the installed version and update history, the system should maintain a version control system. This allows users to easily identify the current system version, track the updates applied, and review the update history. The version control system provides transparency, facilitates troubleshooting, and supports rollback or restoration to previous versions if necessary. By maintaining a version control system, the system ensures accountability, facilitates system management, and enables efficient tracking of system updates and changes. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

### < SystemUpdates.CompatibilityChecks >

|  |  |
| --- | --- |
| Identifier | 15.5 |
| Title | <SystemUpdates.CompatibilityChecks> |
| Description | The system shall perform compatibility checks before applying updates to ensure the integrity and stability of the system. |
| Source | N/A |
| Rationale | Before applying updates, it is important to ensure compatibility to maintain the integrity and stability of the system. Compatibility checks verify that the updates are compatible with the system's existing components, configurations, and dependencies. By performing compatibility checks, the system can minimize the risk of introducing conflicts, errors, or instability due to incompatible updates. This helps maintain a reliable and functioning system while incorporating necessary updates and enhancements. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

### < SystemUpdates.ScheduledInstallations >

|  |  |
| --- | --- |
| Identifier | 15.6 |
| Title | <SystemUpdates.ScheduledInstallations> |
| Description | The system shall allow users to schedule update installations during maintenance windows or off-peak hours. |
| Source | N/A |
| Rationale | To minimize disruptions and ensure uninterrupted system availability, the system should allow users to schedule update installations during maintenance windows or off-peak hours. By providing flexible scheduling options, users can plan update installations at times when the system usage is low or when maintenance activities are traditionally conducted. This reduces the impact on system performance and user experience, while still maintaining the system's security and functionality through timely updates. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

### < SystemUpdates.UpdateLog >

|  |  |
| --- | --- |
| Identifier | 15.7 |
| Title | <SystemUpdates.UpdateLog> |
| Description | The system shall maintain an update log to record the details of installed updates, including their release dates and changes. |
| Source | N/A |
| Rationale | To maintain a historical record and facilitate traceability, the system should maintain an update log. The update log keeps track of installed updates, including their release dates and changes. This log provides valuable information for auditing, troubleshooting, and reference purposes. It allows users to review the update history, identify the applied updates, and understand the changes introduced by each update. By maintaining an update log, the system ensures transparency, accountability, and effective management of system updates. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | Medium |

### < SystemUpdates.RollbackCapabilities >

|  |  |
| --- | --- |
| Identifier | 15.8 |
| Title | <SystemUpdates.RollbackCapabilities> |
| Description | The system shall provide rollback capabilities to revert to a previous version in case of issues or compatibility conflicts. |
| Source | N/A |
| Rationale | To mitigate the impact of issues or compatibility conflicts introduced by updates, the system should provide rollback capabilities. Rollback allows users to revert to a previous version of the system in a controlled and efficient manner. This ensures that the system can quickly recover from any unforeseen problems caused by updates, minimizing disruptions and maintaining system stability. By providing rollback capabilities, the system enhances its resilience and enables effective risk management during the update process. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

### < SystemUpdates.SecureUpdateMechanisms >

|  |  |
| --- | --- |
| Identifier | 15.9 |
| Title | <SystemUpdates.SecureUpdateMechanisms> |
| Description | The system shall enforce secure update mechanisms to prevent unauthorized or tampered updates. |
| Source | N/A |
| Rationale | To maintain the integrity and security of the system, it is crucial to enforce secure update mechanisms. Secure update mechanisms prevent unauthorized or tampered updates from being applied to the system. This includes implementing measures such as cryptographic verification, digital signatures, secure communication channels, and access controls to ensure that only trusted and verified updates are installed. By enforcing secure update mechanisms, the system reduces the risk of malicious or compromised updates compromising the system's security and functionality. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

## ComplianceChecking

### < ComplianceChecking.Analysis >

|  |  |
| --- | --- |
| Identifier | 16.1 |
| Title | <ComplianceChecking.Analysis> |
| Description | The system shall analyze compliance data and identify areas of non-compliance. |
| Source | User/Stakeholder Requirements |
| Rationale | Analyzing compliance data allows the system to assess the adherence to security standards and identify areas where non-compliance exists. By performing an analysis of the compliance data, the system can provide valuable insights and guidance for remediation efforts. |
| Business Rule | N/A |
| Dependencies | N/A |
| Priority | High |

### < ComplianceChecking.DetailedReports >

|  |  |
| --- | --- |
| Identifier | FR26.2 |
| Title | <ComplianceChecking.DetailedReports> |
| Description | The system shall generate detailed compliance reports highlighting specific non-compliant areas. |
| Source | User/Stakeholder Requirements |
| Rationale | Generating detailed compliance reports helps in providing a comprehensive overview of the non-compliant areas and their specific details. This enables stakeholders to understand the extent of non-compliance and take appropriate actions to address the identified issues. |
| Business Rule | N/A |
| Dependencies | FR26.1 |
| Priority | Medium |

# Non-Functional Requirements

## Reliability

REL-1: The system shall have a mean time between failures (MTBF) of at least 30 days.

REL-2: The system shall ensure successful completion of network scanning for 95% of the initiated scans.

REL-3: The system downtime shall not exceed 1% of the total operational time.

REL-4: The system shall maintain data integrity with a maximum data loss rate of 0.5%.

## Usability

USE-1: The user interface shall be intuitive and easy to navigate.

USE-2: The system shall provide clear and concise instructions to guide users in performing tasks.

USE-3: The system shall support accessibility features, such as screen readers and keyboard navigation.

USE-4: The system shall allow users to customize their dashboard layout and preferences.

USE-5: The system shall provide context-sensitive help and tooltips to assist users in understanding functionality.

## Performance

PER-1: The system shall authenticate users within 3 seconds.

PER-2: The system shall display dashboard updates in real-time, with a maximum delay of 1 second.

PER-3: The system shall generate vulnerability reports within 10 seconds for scans involving up to 10,000 assets.

PER-4: The system shall support concurrent scanning of up to 100 assets without performance degradation.

## Security

SEC-1: User accounts shall be protected through secure password hashing and encryption techniques.

SEC-2: The system shall enforce role-based access control to ensure appropriate data access for each user.

SEC-3: The system shall employ secure communication protocols, such as HTTPS, for data transmission.

SEC-4: The system shall log and monitor user activities for detecting and preventing unauthorized access.

SEC-5: The system shall undergo regular security audits and vulnerability assessments to identify and mitigate potential threats.

## Availability

AV-1: The system shall be available for user access 99.9% of the time, excluding scheduled maintenance windows.

AV-2: The system shall provide failover and redundancy mechanisms to minimize downtime in case of hardware or software failures.

AV-3: The system shall have a disaster recovery plan in place to restore services within 4 hours in the event of a major system failure.

## Integrity

INT-1: The system shall ensure the integrity of stored data by employing data validation and checksum mechanisms.

INT-2: The system shall maintain an audit trail of data modifications, including the user responsible for each change.

INT-3: The system shall perform regular data backups to prevent data loss in case of system failure.

## Scalability

SCA-1: The system shall handle a concurrent user load of at least 500 users without significant performance degradation.

SCA-2: The system shall scale horizontally to accommodate an increase in network assets and users without sacrificing performance.

# External Interface Requirements

## User Interfaces Requirements

UI-1: The system shall follow a modern and intuitive graphical user interface (GUI) design.

UI-2: The user interface shall comply with established industry standards for fonts, icons, color schemes, and controls.

UI-3: The system shall support a responsive design that adapts to different screen resolutions and device types.

UI-4: Commonly used controls, such as buttons and dropdown menus, shall be consistently implemented throughout the application.

UI-5: The system shall provide standard navigation links or buttons for common actions, such as accessing help or returning to the homepage.

UI-6: The user interface shall support shortcut keys for frequently used functions.

UI-7: Error messages and status updates shall be displayed in a clear and user-friendly manner.

UI-8: The user interface shall be designed to facilitate software localization and translation.

UI-9: The system shall incorporate accessibility features to accommodate visually impaired users, such as support for screen readers and alternative text for images.

## Software interfaces

### SI-1: Integration with Threat Intelligence API

SI-1.1: The system shall communicate with the Threat Intelligence API to retrieve up-to-date threat intelligence information.

SI-1.2: The system shall pass relevant scan data to the Threat Intelligence API for analysis and enrichment.

SI-1.3: The system shall receive threat intelligence data from the API and incorporate it into vulnerability assessment processes.

### SI-2: Integration with Reporting Module

SI-2.1: The system shall provide an interface to export vulnerability assessment reports in PDF format.

SI-2.2: The system shall enable integration with third-party reporting tools, such as JIRA or ServiceNow, to automatically create tickets for identified vulnerabilities.

## Hardware interfaces

### HI-1: Network Scanning Hardware

HI-1.1: The system shall interact with network scanning hardware devices, such as routers or network switches, through standard network protocols (e.g., SNMP).

## Communications interfaces

### CI-1: Email Notifications

CI-1.1: The system shall send email notifications to users for account activation, password reset, and critical system updates.

CI-1.2: The system shall include relevant information, such as order confirmations or vulnerability reports, in email notifications.

### CI-2: SMS Notifications

CI-2.1: The system shall provide the option to send SMS notifications to users for important alerts or system notifications.

### CI-3: API Communication

CI-3.1: The system shall expose RESTful APIs to allow integration with external systems or custom-developed modules.

# References

## Book

* **Network Security Essentials: Applications and Standards by William Stallings. Pearson, 2017.**

## Journal Article

* "Machine Learning for Network Security: A Review" by Yuan Zhang, Lina Yao, and Xianzhi Wang. IEEE Access, vol. 6, pp. 36399-36411, 2018.
* Blessing Guembe, Ambrose Azeta, Sanjay Misra, Victor Chukwudi Osamor, Luis Fernandez-Sanz & Vera Pospelova (2022) The Emerging Threat of Ai-driven Cyber Attacks: A Review, Applied Artificial Intelligence, 36:1, DOI: [10.1080/08839514.2022.2037254](https://doi.org/10.1080/08839514.2022.2037254)

## Conference Proceeding

* "Vulnerability Assessment of Cyber-Physical Systems Using Machine Learning" by Harsh Kupwade Patil, Manoj Kumar Gupta, and Sanjeev Kumar Gupta. In Proceedings of the International Conference on Information and Communication Technology for Intelligent Systems, Springer, pp. 75-87, 2020.

## Website

* The National Institute of Standards and Technology (NIST) provides guidelines and standards for cybersecurity, including password policies and compliance standards. <https://www.nist.gov/cyberframework>. Accessed March 20, 2023.
* (Artificial Intelligence for Cybersecurity: Offensive Tactics, Mitigation Techniques and Future Directions, n.d.)
* Artificial Intelligence for Cybersecurity. (n.d.). Artificial Intelligence for Cybersecurity. Https://www.blackberry.com/. <https://www.blackberry.com/us/en/solutions/endpoint-security/cybersecurity-ai>