

# **DocuDino**

# **Current Risk Summary report**

Thu May 08 2025 20:07:02 GMT+0000 (Coordinated Universal Time)

#### Project description:

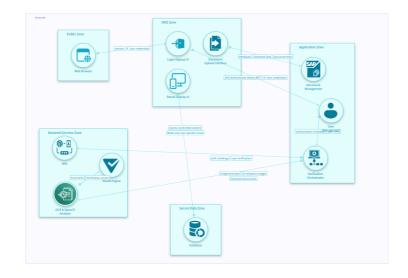
- Automates identity verification
- Leverages OCR and computer vision to analyze both textual and visual security features
- Reduces human dependency and error
- Enhances speed, accuracy, and fraud detection capabilities

Filtered by: No filters

Unique ID: docudino-1746734670094

Owner: Noor-ul-ain Islam
Workflow state: Draft

Tags: No tags





Report: DocuDino 2 of 19



# **Content menu**

Current risk summary

Components

Accepted Risks

#### Current Risks

- Application Zone
- Backend Services Zone
- Database
- DMZ Zone
- Document Management
- Document Upload Interface
- Login/Signup UI
- MFA
- OCR & OpenCV Analysis
- Public Zone
- Result Display UI
- Result Engine
- Secure Data Zone
- User Management
- Verification Orchestrator
- Web Browser



# **Current Risk summary**

Inherent risk description: The Inherent Risk before countermeasures were applied.

• Risk Rating: 69% ^ High

The Current Risk description (the risk we are at now): The Current Risk is based on the current implementation status of the countermeasures and test results.

• Risk Rating: 69% High

Projected Risk description: The Projected Risk is the level of risk that would be reached should the required countermeasures be implemented.

• Risk Rating: 69% ^ High

# **Components**

- Application Zone
- Backend Services Zone
- Database
- DMZ Zone
- Document Management
- Document Upload Interface
- Login/Signup UI
- MFA
- OCR & OpenCV Analysis
- Public Zone
- Result Display UI
- Result Engine
- Secure Data Zone
- User Management
- Verification Orchestrator
- Web Browser



# **Accepted Risks**

No data



## **Current Risks**

# Component: Application Zone

```
CRT1. Threat name: Attackers conduct a Denial of Service Attack
  • Inherent risk: ^ High
  • Current risk: A High
   • Projected risk: ^ High
  • State: Expose

    CR1. Countermeasure name: Implement Comprehensive Resource Management and Protection Mechanisms

    Status: RECOMMENDED

→ Use case: Information Disclosure

CRT2. Threat name: Attackers exploit misconfiguration
   • Inherent risk: ^ High
  • Current risk: A High
  • Projected risk: ^ High
  • State: Expose

    CR2. Countermeasure name: Regular Configuration and Security Reviews

    • Status: RECOMMENDED
CRT3. Threat name: Attackers take advantage of insecure communication channels
  • Inherent risk: ^ High
   • Current risk: A High
  • Projected risk: ^ High
  • State: Expose
  • CR3. Countermeasure name: Implement Comprehensive Data Protection Measures
    • Status: RECOMMENDED

√⊗ Use case: Elevation of Privilege

CRT4. Threat name: Attackers gain elevated privileges
   • Inherent risk: ^ High
  • Current risk: A High
  • Projected risk: ^ High
  • State: Expose

    CR4. Countermeasure name: Regular Patch Management and Vulnerability Assessment

    • Status: RECOMMENDED
 CRT5. Threat name: Attackers gain Unauthorized access by Identity Spoofing
  • Inherent risk: ^ High
  • Current risk: A High
  • Projected risk: ^ High
  • State: Expose
  • CR5. Countermeasure name: Enforce Multi-Factor Authentication

    Status: RECOMMENDED

 CRT6. Threat name: Attackers perform Unauthorized Data Modification
  • Inherent risk: = Medium
   • Current risk: 

Medium
  • Projected risk: = Medium
  • State: Expose
  • CR6. Countermeasure name: Implement Data Integrity Checks

    Status: RECOMMENDED

CRT7. Threat name: Lack of evidences of misuse due to insufficient Auditing and Logging
   • Inherent risk: = Medium
  • Current risk: 

Medium
  • Projected risk: = Medium

    State: Expose
```

CR7. Countermeasure name: Implement Comprehensive Logging and Auditing

• Status: RECOMMENDED

#### Component: Backend Services Zone

#### ∘**g Use case:** General

CRT8. Threat name: Back-end servers used as a means to attack a vehicle or extract data

- Current risk: 🔼 Critical
- State: Expose
- CR8. Countermeasure name: Prevent unauthorized access through system design
- Status: RECOMMENDED
- CR9. Countermeasure name: Minimize unauthorized access
- Status: RECOMMENDED
- CR10. Countermeasure name: Minimize the risk of insider attack
- Status: RECOMMENDED

CRT9. Threat name: Services from back-end server being disrupted affecting the operation of a vehicle

- Inherent risk: 
   Critical
- Current risk: 🔊 Critical
- Projected risk: ♠ Critical
- State: Expose
- CR11. Countermeasure name: Prepare recovery measures in case of system outage
- Status: RECOMMENDED

CRT10. Threat name: Vehicle related data held on back-end servers being lost or compromised

- Current risk: 🔼 Critical
- State: Expose
- CR12. Countermeasure name: Minimize risks associated with cloud computing
- Status: RECOMMENDED
- CR13. Countermeasure name: Prevent data breaches
- Status: RECOMMENDED

## **Component: Database**

≪ Use case: Tampering

CRT11. Threat name: Attacker exploit misconfiguration and/or vulnerable third-party plugins

- Inherent risk: ^ High
- Current risk: 🔼 High
- Projected risk: ^ High
- State: Expose
- CR14. Countermeasure name: Implement regular review and updates for system configuration and dependencies
- Status: RECOMMENDED

CRT12. Threat name: Attackers inject malicious content, e.g., SQLi

- Inherent risk: ^ High
- Current risk: 🔼 High
- Projected risk: ^ High
- State: Expose
- CR15. Countermeasure name: Implement proper input validation
- Status: RECOMMENDED
- CR16. Countermeasure name: Use prepared statements and parameterized queries
- Status: RECOMMENDED

# ∘**§ Use case:** Elevation of Privilege

CRT13. Threat name: Attackers gain unauthorized access or elevated privileges

- Inherent risk: ^ High
- Current risk: 🔼 High
- Projected risk: ^ High
- State: Expose
- CR17. Countermeasure name: Create a workflow for a comprehensive security framework for your database management system
- Status: RECOMMENDED

#### ∘ **g Use case:** Information Disclosure

CRT14. Threat name: Attackers gather useful information from inadequate error handling

- Inherent risk: ^ High
- Current risk: A High



```
• Projected risk: ^ High
    • State: Expose
    • CR18. Countermeasure name: Implement secure error handling
      • Status: RECOMMENDED
 CRT15. Threat name: Attackers take advantage of insecure communication channels or inadequate data encryption practices
    • Inherent risk: ^ High
     • Projected risk: ^ High
    • State: Expose
    • CR19. Countermeasure name: Enforce TLS for all Communications
      • Status: RECOMMENDED

    CR20. Countermeasure name: Implement strong encryption mechanisms and practices

      • Status: RECOMMENDED
  CRT16. Threat name: Denial of service via resource exhaustion
    • Inherent risk: ^ High
    • Current risk: 🔼 High
    • Projected risk: ^ High
    • State: Expose

    CR21. Countermeasure name: Implement rate and resource limiting

    Status: RECOMMENDED

  → Use case: Repudiation
  CRT17. Threat name: Lack of evidences of misuse due to insufficient auditing and logging or poor log protection
    • Inherent risk: = Medium
     • Current risk: 

Medium
    • Projected risk: = Medium
    • State: Expose
    • CR22. Countermeasure name: Implement review, monitoring, and logging mechanisms

    Status: RECOMMENDED

Component: DMZ Zone

√⊗ Use case: Elevation of Privilege

 CRT18. Threat name: Attackers access the system taking advantage of broken authentication
    • Current risk: Critical

    Projected risk: 
    Critical

    • State: Expose

    CR23. Countermeasure name: Implement server-side access control checks

      • Status: RECOMMENDED
  CRT19. Threat name: Attackers exploit flaws in access control systems

    Inherent risk: 
    Critical

    • Current risk: 🔼 Critical

    Projected risk: 
    Critical

    • State: Expose

    CR24. Countermeasure name: Implement secure session management

      • Status: RECOMMENDED
    • CR25. Countermeasure name: Implement Multi-Factor Authentication (MFA)

    Status: RECOMMENDED

  of Use case: Tampering
 CRT20. Threat name: Attackers capitalize on security misconfigurations
     • Inherent risk: ^ High
    • Current risk: A High
    • Projected risk: ^ High
    • State: Expose

    CR26. Countermeasure name: Conduct regular security audits and reviews

      • Status: RECOMMENDED
  og Use case: Information Disclosure
  CRT21. Threat name: Attackers get access to sensitive data
```

Current risk: Critical



- Projected risk: ♠ Critical
- State: Expose
- CR27. Countermeasure name: Use encryption to protect sensitive data
- Status: RECOMMENDED

#### **Component: Document Management**

of Use case: Information Disclosure

CRT22. Threat name: Attackers could gain access to sensitive data through a man in the middle attack

- Inherent risk: ^ High
- Current risk: <a> High</a>
- Projected risk: ^ High
- State: Expose
- CR28. Countermeasure name: Enable mTLS authentication for Document Management Service
- Status: RECOMMENDED

CRT23. Threat name: Sensitive data is compromised through unauthorized access to data

- Inherent risk: ♠ Critical
- Current risk: 🔼 Critical
- State: Expose
- CR29. Countermeasure name: Use encryption for Document Management Service
- Status: RECOMMENDED

#### **Component: Document Upload Interface**

≪ Use case: Elevation of Privilege

CRT24. Threat name: An attacker bypasses authentication to download sensitive documents

- Current risk: Critical
- Projected risk: 
   Critical
- State: Expose
- CR30. Countermeasure name: Implement multi-factor authentication (MFA) for document download access
- Status: RECOMMENDED

#### 

CRT25. Threat name: An attacker exploits an insecure file storage path to download unauthorized files

- Inherent risk: ♠ Critical
- Current risk: 🔼 Critical
- State: Expose
- CR31. Countermeasure name: Validate and sanitize all file paths to prevent unauthorized access
- Status: RECOMMENDED

 $\textbf{CRT26. Threat name:} \ \textbf{Sensitive files are served without encryption, allowing data interception}$ 

- Current risk: 🛭 Critical
- **Projected risk:** ♠ Critical
- State: Expose
- CR32. Countermeasure name: Enforce HTTPS and encrypt documents during transit
- Status: RECOMMENDED

#### ∘ **g Use case:** Denial of Service

CRT27. Threat name: An attacker performs a denial-of-service (DoS) attack on the document download service

- Current risk: 🔼 Critical
- **Projected risk:** ♠ Critical
- State: Expose
- CR33. Countermeasure name: Implement rate limiting and request throttling for the download service
- Status: RECOMMENDED

# 

CRT28. Threat name: Log tampering allows attackers to cover their tracks after unauthorized downloads

- Inherent risk: ^ High
- Current risk: 🔼 High
- Projected risk: ^ High
- State: Expose



- CR34. Countermeasure name: Implement immutable logging and ensure logs are securely stored
- Status: RECOMMENDED

#### Component: Login/Signup UI

#### ∘**§ Use case:** Elevation of Privilege

CRT29. Threat name: Attackers access the system taking advantage of broken authentication

- Inherent risk: ♠ Critical
- Current risk: 🔯 Critical
- Projected risk: 
   Critical
- State: Expose
- CR35. Countermeasure name: Implement server-side access control checks
- Status: RECOMMENDED

#### CRT30. Threat name: Attackers exploit flaws in access control systems

- Current risk: 🔼 Critical
- State: Expose
- CR36. Countermeasure name: Implement secure session management
- Status: RECOMMENDED
- CR37. Countermeasure name: Implement Multi-Factor Authentication (MFA)
- Status: RECOMMENDED

#### → Use case: Tampering

#### CRT31. Threat name: Attackers capitalize on security misconfigurations

- Inherent risk: ^ High
- Current risk: 🔼 High
- Projected risk: ^ High
- State: Expose
- CR38. Countermeasure name: Conduct regular security audits and reviews
- Status: RECOMMENDED

#### ≪ Use case: Information Disclosure

#### CRT32. Threat name: Attackers get access to sensitive data

- Current risk: Critical
- Projected risk: 
   Critical
- State: Expose
- CR39. Countermeasure name: Use encryption to protect sensitive data
- Status: RECOMMENDED

## Component: MFA

#### 

## CRT33. Threat name: An attacker gains access through compromised MFA methods

- Inherent risk: ^ High
- Current risk: 🔼 High
- Projected risk: ^ High
- State: Expose
- CR40. Countermeasure name: Enhanced MFA resilience
- Status: RECOMMENDED

# **CRT34. Threat name:** MFA bypass due to inadequate fallback mechanisms

- Inherent risk: ^ High
- Current risk: <a> High</a>
- Projected risk: ^ High
- State: Expose
- CR41. Countermeasure name: Secure MFA fallbacks
- Status: RECOMMENDED

## CRT35. Threat name: Unauthorized access through social engineering

- Current risk: 🔼 Critical
- Projected risk: 
   <sup>♠</sup> Critical
- State: Expose
- CR42. Countermeasure name: User training and awareness programs
- Status: RECOMMENDED



```
CRT36. Threat name: Denial of service on MFA systems
    • Inherent risk: ^ High
    • Current risk: A High
    • Projected risk: ^ High

    State: Expose

    CR43. Countermeasure name: Rate limiting and throttling for MFA

      • Status: RECOMMENDED
  CRT37. Threat name: Session hijacking despite MFA implementation
    • Inherent risk: ^ High
    • Current risk: A High
    • Projected risk: ^ High
    • State: Expose
    • CR44. Countermeasure name: Session security enhancement
      • Status: RECOMMENDED
Component: OCR & OpenCV Analysis
  ∘ g Use case: Information Disclosure
 CRT38. Threat name: Exposure of personally identifiable information (PII)
    • Inherent risk: ^ High
    • Current risk: <a> High</a>
    • Projected risk: ^ High
    • State: Expose

    CR45. Countermeasure name: Redact PII from documents processed by AWS Textract

      • Status: RECOMMENDED
 CRT39. Threat name: Exposure of sensitive data post-processing
    • Inherent risk: ^ High
    • Current risk: A High
    • Projected risk: ^ High
    • State: Expose
    • CR46. Countermeasure name: Apply metadata tags to classify sensitive data extracted by AWS Textract
      • Status: RECOMMENDED
 CRT40. Threat name: Non-compliance with data residency requirements
    • Current risk: 🔊 Critical

    CR47. Countermeasure name: Limit document processing to specific AWS Regions for compliance

    Status: RECOMMENDED

Component: Public Zone
  ∘ Use case: Spoofing
  CRT41. Threat name: Attackers conduct phishing attacks through deceptive websites

    Inherent risk: 
    Critical

    • Current risk: 🔼 Critical

    Projected risk: 
    Critical

    • State: Expose
    • CR48. Countermeasure name: Deploy anti-phishing protection

    Status: RECOMMENDED

    • CR49. Countermeasure name: Activate URL filtering mechanisms
      • Status: RECOMMENDED
 CRT42. Threat name: Attackers intercept browser communications through man-in-the-middle (MitM) attacks
    • Current risk: 🔼 Critical

    Projected risk: 
    Critical

    • State: Expose

    CR50. Countermeasure name: Enforce strict certificate validation

      • Status: RECOMMENDED

    CR51. Countermeasure name: Utilize encrypted communication tools

      • Status: RECOMMENDED
```

∘ **Use case:** Denial of Service

# IriusRisk< ≪ Use case: Tampering CRT43. Threat name: Attackers distribute malware through compromised browser extensions Inherent risk: Critical • Current risk: 🔼 Critical Projected risk: Critical • State: Expose CR52. Countermeasure name: Manage browser extensions securely • Status: RECOMMENDED CR53. Countermeasure name: Implement extension whitelisting policies Status: RECOMMENDED og Use case: Elevation of Privilege CRT44. Threat name: Attackers exploit browser vulnerabilities to execute malicious code • Current risk: A Critical Projected risk: Critical • State: Expose CR54. Countermeasure name: Configure automatic browser updates Status: RECOMMENDED CR55. Countermeasure name: Apply security hardening measures Status: RECOMMENDED « Use case: Information Disclosure CRT45. Threat name: Attackers inject malicious scripts via cross-site scripting (XSS) • Inherent risk: ^ High • Current risk: A High • Projected risk: ^ High • State: Expose • CR56. Countermeasure name: Activate built-in browser security filters • Status: RECOMMENDED CR57. Countermeasure name: Implement client-side script blockers Status: RECOMMENDED Component: Result Display UI ≪ Use case: Spoofing CRT46. Threat name: Attackers can deceive users into clicking on hidden elements • Inherent risk: ^ High • Current risk: A High • Projected risk: ^ High

- State: Expose
- CR58. Countermeasure name: Employ frame-busting scripts, set X-Frame-Options header, and enforce Content Security Policy
- Status: RECOMMENDED

#### ≪ Use case: Tampering

CRT47. Threat name: Attackers can exploit vulnerabilities in third-party dependencies leading to security breaches

- Inherent risk: ^ High
- Current risk: A High
- Projected risk: ^ High
- State: Expose
- CR59. Countermeasure name: Regularly update dependencies, use dependency scanning tools, and follow best practices for secure coding
- Status: RECOMMENDED

CRT48. Threat name: Attackers can inject malicious scripts into web pages viewed by other users

- Inherent risk: ^ High
- Current risk: 🔼 High
- Projected risk: ^ High
- CR60. Countermeasure name: Implement input validation, output encoding, and enforce Content Security Policy (CSP)
- Status: RECOMMENDED

# og Use case: Elevation of Privilege

CRT49. Threat name: Attackers may exploit weaknesses in authentication and authorization mechanisms

- Inherent risk: ^ High



- Projected risk: ^ High
- State: Expose
- CR61. Countermeasure name: Implement strong authentication mechanisms and follow the least privilege principle
- Status: RECOMMENDED

#### Component: Result Engine

→ Use case: Tampering

CRT50. Threat name: Attackers bypass the validation process

- Inherent risk: ♠ Critical
- Current risk: Critical
- Projected risk: 
   Critical
- State: Expose
- CR62. Countermeasure name: Harden the input validation mechanisms, setup, and pipeline
- Status: RECOMMENDED

CRT51. Threat name: Attackers inject malicious content, e.g., SQL injection

- Inherent risk: ♠ Critical
- Current risk: 🔼 Critical
- State: Expose
- CR63. Countermeasure name: Proper use of sanitization and validation mechanisms
- Status: RECOMMENDED

CRT52. Threat name: Attackers exploit performance bottlenecks or vulnerable validation processing functionality

- Current risk: 🔼 Critical
- Projected risk: 
   Critical
- State: Expose
- CR64. Countermeasure name: Optimize validation steps
- Status: RECOMMENDED

### Component: Secure Data Zone

CRT53. Threat name: An attacker exploits weak access controls to retrieve sensitive secrets

- Inherent risk: ♠ Critical
- Current risk: 🔼 Critical
- State: Expose
- CR65. Countermeasure name: Implement strict access control policies
- Status: RECOMMENDED

CRT54. Threat name: Compromised systems reuse leaked or old secrets

- Inherent risk: ^ High
- Current risk: 🔼 High
- Projected risk: ^ High
- State: Expose
- CR66. Countermeasure name: Implement automatic secret rotation
- Status: RECOMMENDED

**CRT55. Threat name:** Overly permissive secrets sharing between services leads to data leakage

- Current risk: 🔼 Critical
- State: Expose
- CR67. Countermeasure name: Restrict secret sharing based on least privilege
- Status: RECOMMENDED

CRT56. Threat name: Secrets are stored without encryption, leading to potential exposure

- Inherent risk: ♠ Critical
- Current risk: 🔼 Critical
- Projected risk: ♠ Critical
- State: Expose
- CR68. Countermeasure name: Enforce encryption of secrets at rest and in transit
- Status: RECOMMENDED



# CRT57. Threat name: Attackers exploit vulnerabilities in the Secrets Manager API

- Inherent risk: ♠ Critical
- Current risk: 
  Critical
- Projected risk: 
   Critical
- State: Expose
- CR69. Countermeasure name: Secure the API with strong authentication and input validation
- Status: RECOMMENDED

#### Component: User Management

#### og Use case: Elevation of Privilege

#### CRT58. Threat name: Attackers gain elevated privilege

- Inherent risk: ^ High
- Current risk: A High
- Projected risk: ^ High
- State: Expose
- CR70. Countermeasure name: Enforce Anti-CSRF Measures
- Status: RECOMMENDED
- CR71. Countermeasure name: Implement Robust Access Control Mechanisms
- Status: RECOMMENDED

#### CRT59. Threat name: Attackers use improper Security Configuration for malicious activities

- Inherent risk: ^ High
- Current risk: <a> High</a>
- Projected risk: ^ High
- State: Expose
- CR72. Countermeasure name: Regular Configuration and Vulnerability Assessment
- Status: RECOMMENDED
- CR73. Countermeasure name: Use of Secure Defaults and Hardening Guides
- Status: RECOMMENDED
- CR74. Countermeasure name: Automated Configuration Management Tools
- Status: RECOMMENDED

#### 

#### CRT60. Threat name: Attackers obtain unauthorized access

- Inherent risk: ^ High
- Current risk: <a> High</a>
- Projected risk: ^ High
- State: Expose
- CR75. Countermeasure name: Secure Session Management Practices
- Status: RECOMMENDED
- CR76. Countermeasure name: Implement Multi-Factor Authentication (MFA)
- Status: RECOMMENDED

#### CRT61. Threat name: Attackers take advantage of poor protected data and insecure communications

- Inherent risk: ^ High
- Current risk: A High
- Projected risk: ^ High
- State: Expose
- CR77. Countermeasure name: Implement Comprehensive Encryption Strategies
- Status: RECOMMENDED
- CR78. Countermeasure name: Proactive Risk Assessments for Data Protection
- Status: RECOMMENDED
- CR79. Countermeasure name: Data Handling Best Practices
- Status: RECOMMENDED

#### CRT62. Threat name: Information Disclosure through Improper Handling of User Data and Error Messages

- Inherent risk: ^ High
- Current risk: A High
- Projected risk: ^ High
- State: Expose
- CR80. Countermeasure name: Implement Custom Error Handling and Generic Messaging
- Status: RECOMMENDED

## of Use case: Tampering

## CRT63. Threat name: Injection Attacks

- Inherent risk: ^ High
- Current risk: A High
- Projected risk: ^ High
- State: Expose
- CR81. Countermeasure name: Implement Prepared Statements and Parameterized Queries



- Status: RECOMMENDED
- CR82. Countermeasure name: Implement Content Security Policy (CSP)
- Status: RECOMMENDED
- CR83. Countermeasure name: Comprehensive Input Validation and Sanitization
- Status: RECOMMENDED

#### 

CRT64. Threat name: Resource Exhaustion through Account Enumeration Attacks

- Inherent risk: ^ High
- Current risk: 🔼 High
- Projected risk: ^ High
- State: Expose
- CR84. Countermeasure name: Implement Rate Limiting and Captcha
- Status: RECOMMENDED

#### of Use case: Repudiation

CRT65. Threat name: Unnoticed misbehaviour due to Insufficient Logging and Monitoring

- Inherent risk: = Medium
- Current risk: 🗖 Medium
- Projected risk: = Medium
- State: Expose
- CR85. Countermeasure name: Implement Comprehensive Logging and Monitoring
- Status: RECOMMENDED

#### **Component: Verification Orchestrator**

#### → **Use case:** Denial of Service

CRT66. Threat name: Attackers conduct a Denial of Service Attack

- Inherent risk: ^ High
- Current risk: 🔼 High
- Projected risk: ^ High
- State: Expose
- CR86. Countermeasure name: Implement Comprehensive Resource Management and Protection Mechanisms
- Status: RECOMMENDED

## ∘**《 Use case:** Information Disclosure

CRT67. Threat name: Attackers exploit misconfiguration

- Inherent risk: ^ High
- Current risk: A High
- Projected risk: ^ High
- State: Expose
- CR87. Countermeasure name: Regular Configuration and Security Reviews
- Status: RECOMMENDED

CRT68. Threat name: Attackers take advantage of insecure communication channels

- Inherent risk: ^ High
- Current risk: 🔼 High
- Projected risk: ^ High
- State: Expose
- CR88. Countermeasure name: Implement Comprehensive Data Protection Measures
- Status: RECOMMENDED

#### 

CRT69. Threat name: Attackers gain elevated privileges

- Inherent risk: ^ High
- Current risk: 🔼 High
- Projected risk: ^ High
- State: Expose
- CR89. Countermeasure name: Regular Patch Management and Vulnerability Assessment
- Status: RECOMMENDED

#### ∘ Use case: Spoofing

CRT70. Threat name: Attackers gain Unauthorized access by Identity Spoofing

• Inherent risk: ^ High



- Current risk: High
- Projected risk: ^ High
- State: Expose
- CR90. Countermeasure name: Enforce Multi-Factor Authentication
- Status: RECOMMENDED

#### ≪ Use case: Tampering

CRT71. Threat name: Attackers perform Unauthorized Data Modification

- Inherent risk: = Medium
- Current risk: 

  Medium
- Projected risk: = Medium
- State: Expose
- CR91. Countermeasure name: Implement Data Integrity Checks
- Status: RECOMMENDED

#### 

CRT72. Threat name: Lack of evidences of misuse due to insufficient Auditing and Logging

- Inherent risk: = Medium
- Current risk: 

  Medium
- Projected risk: = Medium
- State: Expose
- CR92. Countermeasure name: Implement Comprehensive Logging and Auditing
- Status: RECOMMENDED

#### Component: Web Browser

#### ≪ Use case: Spoofing

CRT73. Threat name: Attackers conduct phishing attacks through deceptive websites

- Current risk: 🔊 Critical
- Projected risk: 
   Critical
- State: Expose
- CR93. Countermeasure name: Deploy anti-phishing protection
- Status: RECOMMENDED
- CR94. Countermeasure name: Activate URL filtering mechanisms
- Status: RECOMMENDED

 $\textbf{CRT74. Threat name:} \ \textbf{Attackers intercept browser communications through man-in-the-middle (MitM) attacks}$ 

- Current risk: 🔼 Critical
- **Projected risk:** ♠ Critical
- State: Expose
- CR95. Countermeasure name: Enforce strict certificate validation
- Status: RECOMMENDED
- CR96. Countermeasure name: Utilize encrypted communication tools
- Status: RECOMMENDED

#### ≪ Use case: Tampering

CRT75. Threat name: Attackers distribute malware through compromised browser extensions

- Inherent risk: ♠ Critical
- Current risk: 🔼 Critical
- State: Expose
- CR97. Countermeasure name: Manage browser extensions securely
- Status: RECOMMENDED
- CR98. Countermeasure name: Implement extension whitelisting policies
- Status: RECOMMENDED

# ${\circ}{\emptyset}$ **Use case:** Elevation of Privilege

CRT76. Threat name: Attackers exploit browser vulnerabilities to execute malicious code

- Current risk: 🔊 Critical
- State: Expose
- CR99. Countermeasure name: Apply security hardening measures
- Status: RECOMMENDED
- CR100. Countermeasure name: Configure automatic browser updates



• Status: RECOMMENDED

#### ${\ensuremath{\,\scriptscriptstyle{\circ}}}{\ensuremath{\,^{\circ}}}{\en$

CRT77. Threat name: Attackers inject malicious scripts via cross-site scripting (XSS)

- Inherent risk: ^ High
- Current risk: 🔼 High
- Projected risk: ^ High
- State: Expose
- CR101. Countermeasure name: Activate built-in browser security filters
- Status: RECOMMENDED
- CR102. Countermeasure name: Implement client-side script blockers
- Status: RECOMMENDED

Report: DocuDino 17 of 19



End of Current Risk Report



Report: DocuDino 19 of 19