

Next Review Date Uses: Inherent Risk


HighCharts Delivery Method: HighCharts CDN

jQuery Delivery method: jQuery CDN

Bootstrap Delivery Method: jsDelivr CDN

SimpleRisk Base URL: https://192.168.1.92

Risk Appetite: Low (2)



Update

Impostato il livello di risk appetite a 2, possiamo procedere con la mitigazione del rischio. Il valore di partenza del rischio legato ad accessi non autorizzati è pari a 6.4 inizialmente.

Inherent Risk

6.4

Medium


Residual Risk

1.92

Low

ID #: 1001

Status: Mitigation Planned

Subject : Accesso non autorizzato 

[View Risk Scoring Details](#)
[Show Risk Score Over Time](#)

Details

Mitigation

Review

Mitigation Submission Date: 05/20/2024

Planned Mitigation Date: 06/01/2024

Planning Strategy: Mitigate

Mitigation Effort: Considerable

Mitigation Cost:

Select for Mitigation Controls

✓ AC-3: Access Enforcement

✓ AC-6: Least Privilege

✓ AC-7: Unsuccessful Login Attempts

✓ AU-6: Audit Review, Analysis, and Reporting

✓ IA-2: Identification and Authentication

✓ IA-3: Device Identification and Authentication

✓ IA-4: Identifier Management

All selected (7)


Mitigation Owner:





Mitigation Team:

Mitigation Percent:

Mitigation Controls:


Current Solution:





↶ ↷ B I U A 

MFA, IAM

Security Requirements:

↶ ↷ B I U A 

Nella figura affianco, i controlli implementati

Implementati i controlli,
possiamo procedere alla
mitigazione del rischio.

I controlli effettuati, quindi,
con le susseguenti soluzioni
di implementazione di MFA e
IAM, portano la percentuale
di rischio a 1.92, quindi un
livello accettabile.

Inherent Risk

6.4

Medium


Residual Risk

3.2

Low

ID #: 1001

Status: Mitigation Planned

Subject : Accesso non autorizzato 

► View Risk Scoring Details

► Show Risk Score Over Time

Details

Mitigation

Review

Risk Mapping: Privilege escalation, Unauthorized access, Data loss / corruption , System compromise, Information loss / corruption, Denial of service, Data breach, System compromise due to technical attack, Lack of a security-minded workforce

Threat Mapping: Hacking & Other Cybersecurity Crimes

Submission Date: 05/20/2024

Submitted By: babbo

Category: Access Management

Risk Source: External

Site/Location: All Sites

Risk Scoring Method: Classic

External Reference ID:

Current Likelihood: Likely

Control Regulation: NIST SP 800-53

Current Impact: Major

Control Number:

Risk Assessment:

Affected Assets: Database ERP-BR ERP-HQ

Additional Notes:

Supporting Documentation: None

Technology: Remote Access

Team: Information Security, IT Systems Management

Additional Stakeholders:

Inherent Risk

6.4

Medium


Residual Risk

1.92

Low

ID #: 1001

Status: Mitigation Planned

Subject : Accesso non autorizzato 

► View Risk Scoring Details

► Show Risk Score Over Time

Details

Mitigation

Review

Mitigation Submission Date: 05/20/2024

Current Solution: MFA, IAM

Planned Mitigation Date: 06/01/2024

Security Requirements:

Planning Strategy: Mitigate

Security Recommendations:

Mitigation Effort: Considerable

Supporting Documentation: None

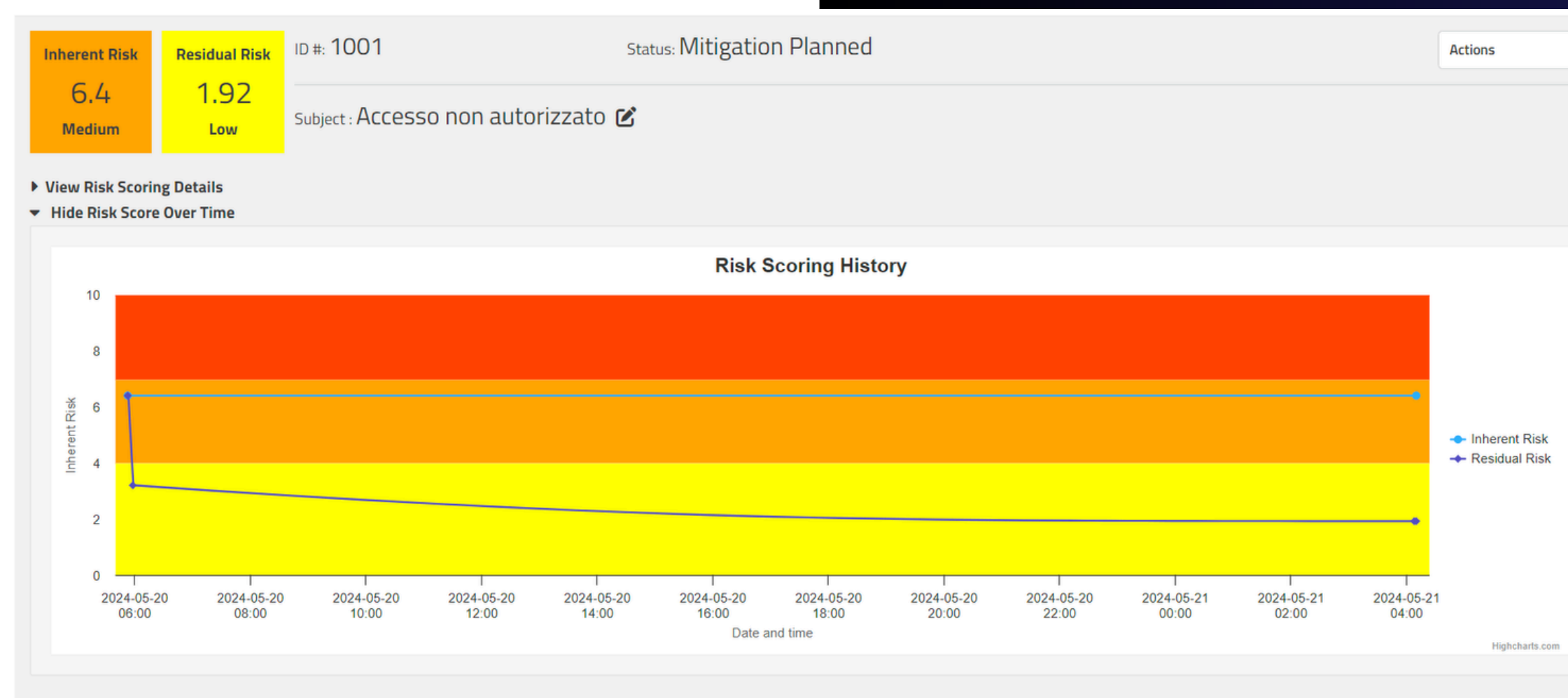
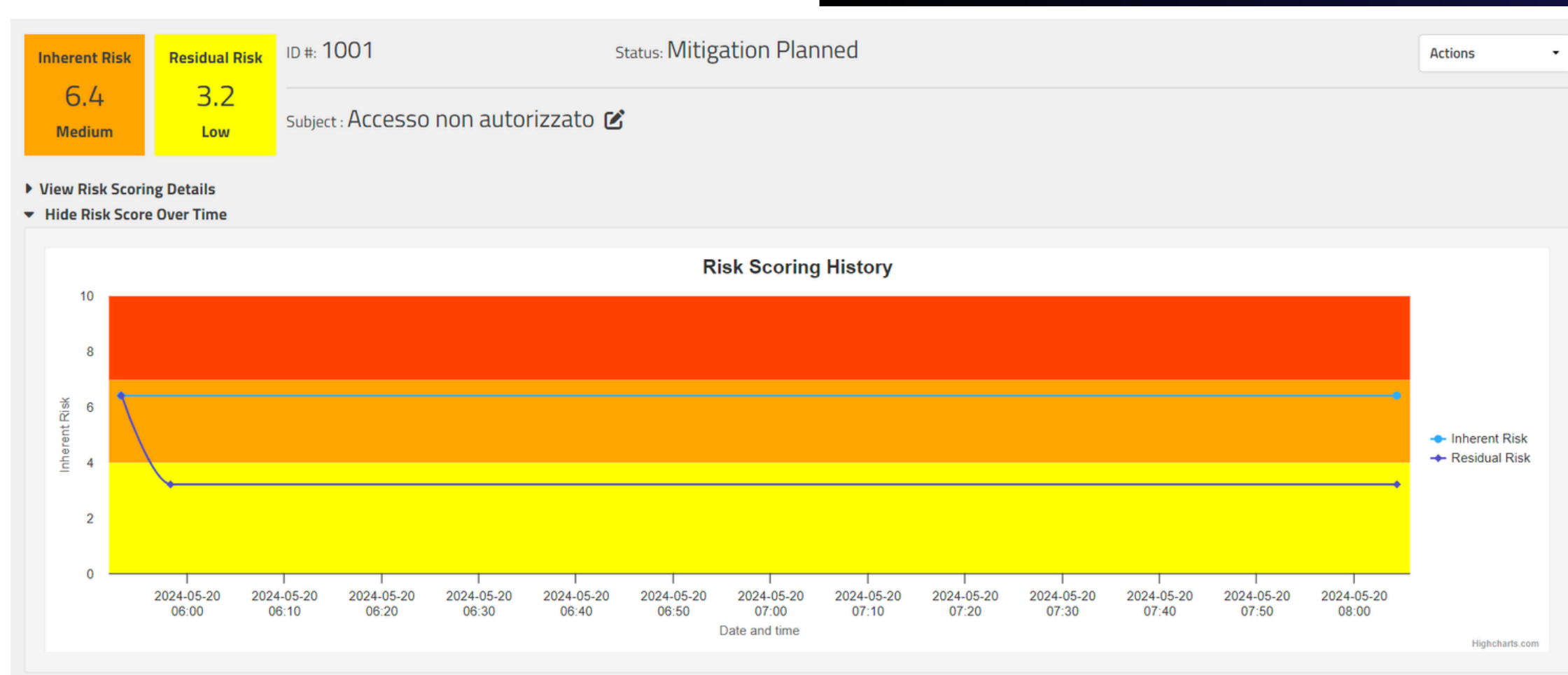
Mitigation Cost: \$0 to \$100,000

Mitigation Owner: babbo

Mitigation Team: Information Security, IT Systems Management

Mitigation Percent: 70%

Accept Mitigation



Affianco, anche un grafico progressivo dei controlli implementati e di come il rischio vada mitigandosi fino a un livello accettabile (pari o inferiore a 2).