Communicate TECHNOLOGY

Identity Risk Review

Sample Report

Understanding Your Report

This report provides an assessment of your organisation's identity security posture and highlights areas of potential risk.

Risk Score

The overall Risk Score provides a high-level indication of your current identity security posture. A higher score indicates a greater number of security risks or exposures requiring attention.

Score Trend

The Score Trend indicates whether security posture is improving, remaining stable or deteriorating over time.

Risk Matrix

The Risk Matrix categorises findings based on likelihood of exploitation and potential business impact, helping to identify which risks should be prioritised first.

Environment Overview

The assessment provides visibility into:
- Users
- Accounts
- Endpoints
- Privileged Accounts

Reviewed as part of the security assessment.

Findings & Recommendations

Each finding includes:
- Severity rating
- Description of the issue
- Potential impact
- Recommended actions

This allows organisations to understand risks and prioritise remediation activities.

Communicate TECHNOLOGY

SAMPLE REPORT

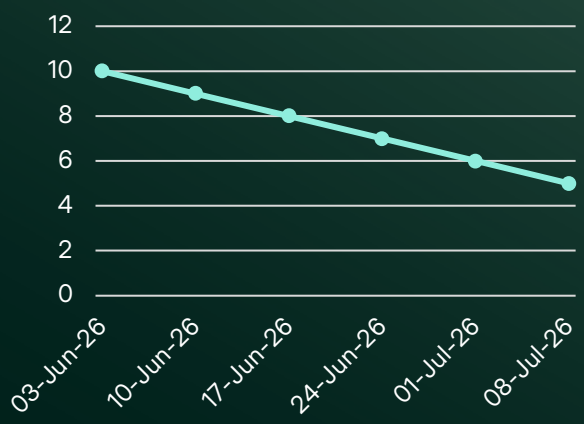
Security Assessment Report

This report summarises the results of an Identity Risk Review completed on the date and time shown above.

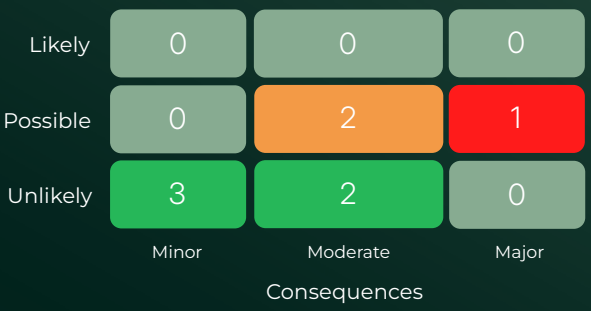
Risk Score

8.4/10

Score Trend



Risk Matrix



Entities

Accounts	248
Users	162
Endpoints	134
Privileged	27

This sample report contains fictional data and is provided for illustration purposes only.

Severity	Risk	Likelihood of exploitation	Consequences
High	Compromised Passwords	Possible	Major
Some user accounts have passwords that are known to have appeared in previous data breaches or are considered weak against modern attack techniques. Compromised passwords increase the risk of unauthorised access and account takeover.		• Require affected users to reset their passwords immediately. • Implement strong password policies across all user accounts. • Enable Multi-Factor Authentication (MFA) for all users. • Review privileged accounts as a priority and apply additional security controls.	
Medium	Overprivileged User Accounts	Possible	Moderate
Some user accounts have permissions that exceed their current business requirements. Excessive permissions can increase the potential impact of a compromised account and may allow unauthorised access to sensitive systems or information.		• Review user permissions and remove unnecessary access rights. • Apply the principle of least privilege across all accounts. • Regularly audit privileged and administrative accounts. • Implement role-based access controls where appropriate.	
Low	Inactive User Accounts	Unlikely	Moderate
A number of inactive or unused accounts may remain enabled within the environment. Dormant accounts can present a security risk if they are not properly managed or removed when no longer required.		• Identify and disable unused or inactive accounts. • Establish a regular account review process. • Remove accounts that are no longer required. • Ensure user lifecycle processes are aligned with joiner, mover and leaver procedures.	

Severity	Risk	Likelihood of exploitation	Consequences
High	Multi-Factor Authentication Not Enabled	Likely	Major

A number of user accounts do not have Multi-Factor Authentication (MFA) enabled. Password-only authentication significantly increases the risk of unauthorised account access, particularly where credentials have been compromised or reused across multiple services.

- Enable MFA for all user accounts.
- Prioritise administrator and privileged accounts.
- Review and remove any legacy authentication methods that bypass MFA.
- Regularly audit MFA enrollment and compliance.

Severity	Risk	Likelihood of exploitation	Consequences
Medium	Excessive Administrative Accounts	Possible	Moderate

The environment contains a higher than recommended number of accounts with administrative privileges. Excessive administrative access increases the attack surface and may lead to greater impact should an account become compromised.

- Review all accounts with administrative permissions.
- Remove administrative privileges where they are no longer required.
- Implement dedicated administrator accounts separate from everyday user accounts.
- Perform periodic access reviews to ensure privileges remain appropriate.

Severity	Risk	Likelihood of exploitation	Consequences
Low	Legacy Authentication	Unlikely	Moderate

Legacy authentication protocols may still be enabled within the environment to support older applications or devices. These protocols often lack modern security controls and can provide attackers with an alternative route into the environment.

- Identify systems and applications using legacy authentication.
- Develop a plan to migrate to modern authentication methods.
- Disable legacy protocols where business requirements permit.
- Monitor authentication logs for unusual activity involving legacy services.

Communicate TECHNOLOGY

Book your review

The Identity Risk Review is designed to help organisations gain visibility of identity-related risks, understand potential security gaps and receive practical recommendations to strengthen security posture.

Click here to book your review →

How it works

1. **Discovery call**

   We start with a short conversation to understand your environment and confirm the review is right for your organisation.

2. **Secure Onboarding**

   Our Security Operations Centre securely connects your identity platform to CrowdStrike for assessment.

3. **Assessment**

   We analyse your environment over a period of approximately two weeks to identify potential risks and areas for improvement.

4. **Findings Workshop**

   We'll walk you through the results, explain any identified risks and discuss recommendations and next steps.

5. **Detailed Report**

   You'll receive a comprehensive report containing findings, risk areas and prioritised recommendations.

One connected approach

We help organisations get more from technology through joined-up cyber, connectivity and cloud solutions.

Ready to book your review?

Get in touch to learn how the Identity Risk Review can help strengthen your organisation's security.

Learn More →

0800 404 8888
enquiries@communicate.technology
communicate.technology