Good Consulting

Incident Report

Incident: GC-SEC-2026-001	**Incident date:** 14 January, 2026
Reporter: Cloud Operations Monitoring	**Reported on:** 10 February, 2026
Priority: High	**Status:** Resolved

Affected services: Cloud Identity Management Platform and Microsoft 365 Authentication Services

Incident Description

On 14 January 2026, Good Consulting detected unauthorized login attempts against a cloud-based identity service used for internal collaboration tools. Automated security alerts indicated multiple failed authentication attempts originating from an external IP range not previously associated with Good Consulting operations.

No confirmed data exfiltration occurred. However, the incident was classified as a **security incident** due to the potential risk to user accounts and access controls.

Impact Assessment

Business Impact:

- Temporary account lockouts for 3 internal users
- Elevated authentication latency for approximately 18 minutes
- No customer-facing services were disrupted

Data Impact:

- No evidence of data loss or unauthorized data access
- No personal or customer data exposed

Users Affected:

- Internal employees only
- No external clients impacted

Root Cause Analysis

The incident was caused by a **credential-stuffing attempt** targeting cloud identity endpoints using previously compromised credentials from an external breach unrelated to Good Consulting.

Contributing factors:

- User account without enforced MFA at the time of the incident
- Attack originated from a known malicious IP range

Actions Taken

Immediate Response:

- Blocked offending IP addresses at the firewall level
- Forced password resets for affected accounts
- Temporarily locked targeted user accounts
- Increased authentication logging and monitoring thresholds

Resolution Actions:

- Enforced Multi-Factor Authentication (MFA) across all user accounts
- Reviewed access logs for anomalous behavior
- Conducted security verification of all impacted services

Time to Resolution: 47 minutes

Communication & Escalation

Internal Notifications:

- Cloud Operations Team
- Security & Compliance Team
- IT Leadership

External Notifications:

- Not required (no customer or regulatory impact)

Lessons Learned

- MFA enforcement is critical for all identity services
- Earlier detection thresholds could reduce response time
- User security awareness training should be reinforced
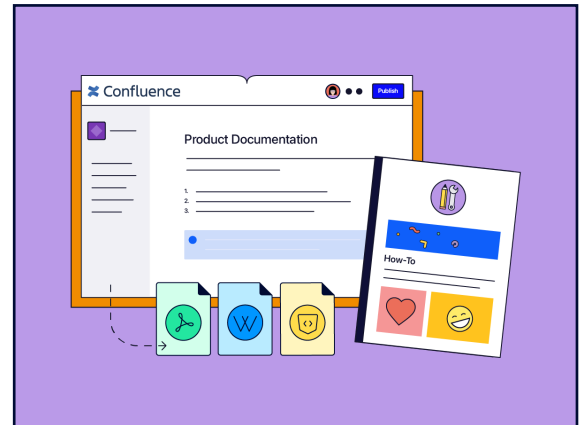
Preventive & Follow-Up Actions

Action	Owner	Status
Enforce MFA for all users	Security Team	Completed
Update security monitoring rules	Cloud Ops	Completed
Conduct internal security awareness refresher	IT Management	Planned
Quarterly identity access review	Compliance	Scheduled

Thanks for Checking Out This PDF Export Example

This PDF was written in Confluence and exported using Scroll PDF Exporter.

Create Beautiful, Branded PDFs from Confluence

Turn your Confluence content into professionally designed PDFs that match your brand and look great every time with **Scroll PDF Exporter**.

Try it free for 30 days →

Want To Do Even More With Your Exports?

Scroll Exporter Extensions is a free Marketplace app that gives you extra control over how content is used and formatted during export – directly in your Confluence page content.

Install it now →

By the Way...

If PDFs aren't the only thing you export, we've got you covered.

Check out Scroll Word Exporter and Scroll HTML Exporter for quick, clean exports in other offline formats.

And if you want to publish Confluence content online, Scroll Sites helps you create beautiful help centers, knowledge bases, blogs, and more.

Liked This Template?

There are even more templates to explore – head to the PDF Template Library.

Browse Templates →

✓ Reports   ✓ Letterheads   ✓ Onboarding Plans   ✓ User Manuals   ✓ Product Fact Sheets