AzureIR

Executive Security Assessment Report

Identity Threat Exposure | Root Cause | Defensive Guidance

Prepared For

Contoso Manufacturing Group (Demo Tenant)

Reference: AIR-SAMPLE-2026-041

Generated: 2026-04-29 17:15 UTC

Report Objective

Provide leadership and security teams with a framework-driven view of risk posture, attack progression, root cause, and remediation priorities.

Executive Summary

AzureIR consolidates Microsoft 365 identity telemetry, suspicious activity, and change events into a unified investigation narrative. This enables teams to move from fragmented alerts to prioritized decisions with clear accountability and measurable security outcomes.
The current sample dataset indicates measurable identity risk, recurring suspicious sign-ins, and policy governance opportunities that can be addressed through control hardening and operational playbook maturity.

Assessment Snapshot

- Total sign-ins reviewed: 1248
- Failed sign-ins: 163
- Risk-elevated sign-ins (medium/high): 89
- Audit events analyzed: 542
- Open alerts requiring triage: 17
- Observed sign-in success rate: 86.9%

Cyber Kill Chain Process

- Reconnaissance: suspicious probing against sign-in surfaces and public tenant metadata.
- Weaponization and Delivery: credential stuffing and phishing-aligned access attempts.
- Exploitation and Installation: risky successful authentications indicate token/session abuse exposure.
- Command and Control: anomalous behavior and geo-velocity patterns can support persistence.
- Actions on Objectives: privileged and policy changes require validation for unauthorized impact.

MITRE ATT&CK Framework Mapping

- T1078 Valid Accounts: possible misuse of legitimate credentials.
- T1110 Brute Force: repeated failed sign-ins consistent with password spray activity.
- T1098 Account Manipulation: role, credential, or account setting modifications.
- T1556 Modify Authentication Process: weakening identity controls via policy adjustments.

Vulnerabilities and Root Cause

- Inconsistent MFA adoption exposes critical user journeys to credential compromise.
- Conditional Access exceptions and legacy authentication pathways weaken preventive controls.
- Alert triage ownership and escalation criteria are not consistently applied across teams.
- Reporting fragmentation limits confidence in full attack timeline reconstruction.
- [HIGH] Impossible travel pattern for privileged identity | User: admin@contoso.com | Status: investigating
- [MEDIUM] Password spray behavior detected | User: operations@contoso.com | Status: new

Complementary Security Guidance

- Enforce phishing-resistant MFA for privileged identities and high-risk sign-in conditions.
- Apply Conditional Access using user risk, sign-in risk, device compliance, and network trust signals.
- Block legacy authentication and require modern protocols where technically feasible.
- Implement least-privilege governance with periodic access certification and break-glass controls.
- Operationalize response playbooks for impossible travel, password spray, and privileged anomalies.

Reference Articles and Standards

- Microsoft Entra Conditional Access design guidance and baseline policy recommendations.
- Microsoft MFA and Identity Protection implementation articles.
- MITRE ATT&CK Enterprise Matrix for technique-to-control validation.
- NIST Cybersecurity Framework and CIS Controls for governance alignment.
- This report is a sample document generated from synthetic data for demonstration only.