

Module 6: Cloud Security, IAM, and Incident Response

Executive Summary

This report provides a comprehensive overview of SecureCart Inc.'s cloud security posture. Identifying existing gaps in identity and Access Management (IAM), Conditional Access (CA) configuration, and incident Response preparedness. The assessment revealed multiple IAM misconfigurations, unrestricted guest access, and a lack of a formal phishing response plan. IAM roles were corrected to address these issues, Conditional Access policies were implemented, and a NIST 800-61-aligned Incident Response Plan (IRP) was developed. These actions enhance security resilience, ensure regulatory compliance, and reduce risks associated with unauthorized access and phishing threats.

Part 1: Identity and Access Management (IAM) Implementation

The following IAM corrections were made within Microsoft Entra ID to enforce the principle of least privilege and establish proper group-based access controls:

Role Fix: Alice Brown's role changed from Global Administrator to User Administrator.

John Doe retains Global Administrator rights.

Fiance Group Fix: John Doe was removed from Fiance_User; only verified Fiance staff remain.

Sales Group Fix: Emily Johnson added to Sales_Users

Support Group Creation: Support_Users group created and populated with relevant support staff.

Guest Access Restrictions: Marketing_Contractors group created with limited access to marketing-specific SharePoint and Teams resources.

The screenshot shows a Microsoft Edge browser window with several tabs open at the top: Cybersecu, Users - Mic, New user -, Active users, Settings - S, and Marketing -. The main content area displays the 'Active' users list in the Microsoft Entra admin center. The page title is 'Users - Microsoft Entra admin center' and the URL is 'https://entra.microsoft.com'. The interface is dark-themed. At the top, there are buttons for 'Add a user', 'User templates', 'Add multiple users', 'Multi-factor authentication', and a search bar 'Search active users list'. Below this, a filter dropdown says 'Filter set: Commonly used' with options for 'Licenses', 'Sign-in status', 'Domain', and 'Location'. The user list table has columns for 'Display name ↑', 'Username', and 'Licenses'. Six users are listed: Alice Brown, Emily Johnson, Jane Smith, John Doe, and Vianka Lopez. All users are marked as 'Unlicensed'. The bottom of the screen shows the Windows taskbar with icons for File Explorer, Edge, File Manager, and Google Chrome, along with system status icons like battery level and network connection.

Display name ↑	Username	Licenses
Alice Brown	Alice.brown@SecureCartInc465.onmicrosoft.com	Unlicensed
Emily Johnson	emily.johnson@SecureCartInc465.onmicrosoft.com	Unlicensed
Jane Smith	Jane.smith@SecureCartInc465.onmicrosoft.com	Unlicensed
John Doe	John.doe@SecureCartInc465.onmicrosoft.com	Unlicensed
Vianka Lopez	Admin@SecureCartInc465.onmicrosoft.com	Unlicensed

Part 2: Conditional Access (CA) Policies

Three Conditional Access policies were established using Microsoft Entra ID Premium (P1) features to protect user identities and control sign-in conditions:

- **MFA:** Multi-Factor Authentication is required for all users using Microsoft Authenticator
- **Location-Based Access:** Sign-ins are restricted to regions (United States, Canada) and are blocked from high-risk regions.
- **Session Controls:** Session reauthentication is required every 12 hours to minimize credential abuse risk.

The screenshot shows the Microsoft Entra admin center interface. The left sidebar navigation includes Home, Agents, Favorites (with Entra ID selected), ID Protection (Dashboard, Risk-based Conditional Access, Risky users, Risky workload identities), ID Governance (Verified ID, Permissions Management), Global Secure Access (What's new, Billing, Diagnose & solve problems, New support request), and a bottom section for What's new, Billing, and Diagnose & solve problems.

The main content area displays the 'Conditional Access | Policies' blade, specifically the 'Identity Protection | Conditional Access' section. A policy named 'Enforce MFA All' is being edited. The policy details are as follows:

- Name:** Enforce MFA All
- Conditional Access policy:** Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.
- Assignments:**
 - Users:** Specific users included
 - Target resources:** All resources (formerly 'All cloud apps')
 - Network:** Any network or location
- Conditions:** 1 condition selected
- Access controls:** Grant
- Enable policy:** Report-only (On)

Below the policy details, there are two warning messages:

- A yellow warning: "It looks like you're about to manage your organization's security configurations. That's great! You must first [disable security defaults](#) to enable Conditional Access policy."
- A red warning: "Security defaults must be disabled to enable Conditional Access policy."

At the bottom right, there are 'Save' and 'Select' buttons.

Part 3: Incident Response Plan (IRP)

A NIST SP 800-61-aligned IRP was developed for phishing incidents involving Microsoft 365 and Entra ID environments. The scenario involves a Finance Department employee, Jane Smith, who enters credentials into a phishing link. The response plan follows the NIST framework as outlined below:

- **Preparation:** Defined roles, tools (Defender for Office 365, Entra ID logs, Security & Compliance Center)
- **Detection & Analysis:** Identified phishing email through quarantine and anti-phishing alerts. Reviewed Entra ID sign-in logs for suspicious activity.
- **Containment:** Quarantined malicious emails and temporarily disabled Jane Smith's account.
- **Eradication:** Revoked active sessions and enforced password reset.
- **Recovery:** Restored account access after verifying no data compromise.
- **Post-Incident:** Conducted lessons learned review and improved phishing awareness.

The screenshot shows the Microsoft Entra admin center interface. The left sidebar is titled "Microsoft Entra admin center" and includes sections for Home, Agents, Favorites (Overview, Users, Groups, Devices, Enterprise apps, App registrations, Roles & admins, Delegated admin partners, Domain services), Conditional Access (selected), Multifactor authentication, Identity Secure Score, Authentication methods, Password reset, Custom security attributes, Certificate authorities, and External Identities. The main content area is titled "Conditional Access | Named locations" and shows a list of named locations. The table has columns for Name, Location type, Trusted, Conditional Access..., Creation date, and Modified. One entry is visible: "Block Risky Reg..." with "Countries (...)" as the location type, "Not configured..." as the trusted status, and creation and modification dates of "10/26/2025, 6:1...". There are also tabs for "All Named Locations" and "Deleted Named Locations (Preview)". The top navigation bar shows "Microsoft 365 admin center" and "Conditional Access - Microsoft" with a search bar and various icons.

Part 4: Incident Documentation

Incident documentation includes evidence from Entra ID and Defender for Office 365 demonstrating detection, containment, and resolution actions:

- Entra ID sign-in logs showing anomalous logins
- Defender alerts confirming phishing detection and containment
- Documentation of account disablement, session revocation, and password reset.
- Preventive recommendations: regular phishing simulations, user MFA enforcement, and security training.

The screenshot shows the Microsoft Entra admin center interface. The left sidebar is titled 'Entra ID' and lists various administrative tasks such as Overview, Users, Groups, Devices, Enterprise apps, App registrations, Roles & admins, Delegated admin partners, Domain services, Conditional Access, Multifactor authentication, Identity Secure Score, Authentication methods, Password reset, Custom security attributes, and Certificate authorities. The main content area is titled 'Jane Smith | Sign-in logs' and shows a search bar, download, export, troubleshoot, refresh, and column settings buttons. A message indicates that the current view will be replaced by one with more filters, infinite scrolling, and column reordering. It also shows a date filter set to 'Last 24 hours' and a search term 'User contains 0f8fd59c-adc6-442e-b8a5-663c34bd5cc8'. Below this, there are tabs for 'User sign-ins (interactive)' and 'User sign-ins (non-interactive)'. A table header is shown with columns: Date, Request ID, User, Application, and Status. The message 'No sign-ins found' is displayed at the bottom of the table area.

Part 5 Lessons Learned

The SecureCart project highlights the following key insights:

- **IAM Misconfigurations:** Excessive permissions can expose sensitive assets. Enforcing least privilege reduces insider and external threat risks.
- **Conditional Access:** MFA and geolocation controls significantly mitigate unauthorized login attempts.
- **Incident Response:** A structured IRP ensures timely containment and recovery, preserving business continuity.

Continuous improvement of IAM and response capabilities strengthens organizational resilience against evolving cloud threats.