Lopez, Vianka

Module 6: Cloud Security, IAM, and Incident Response

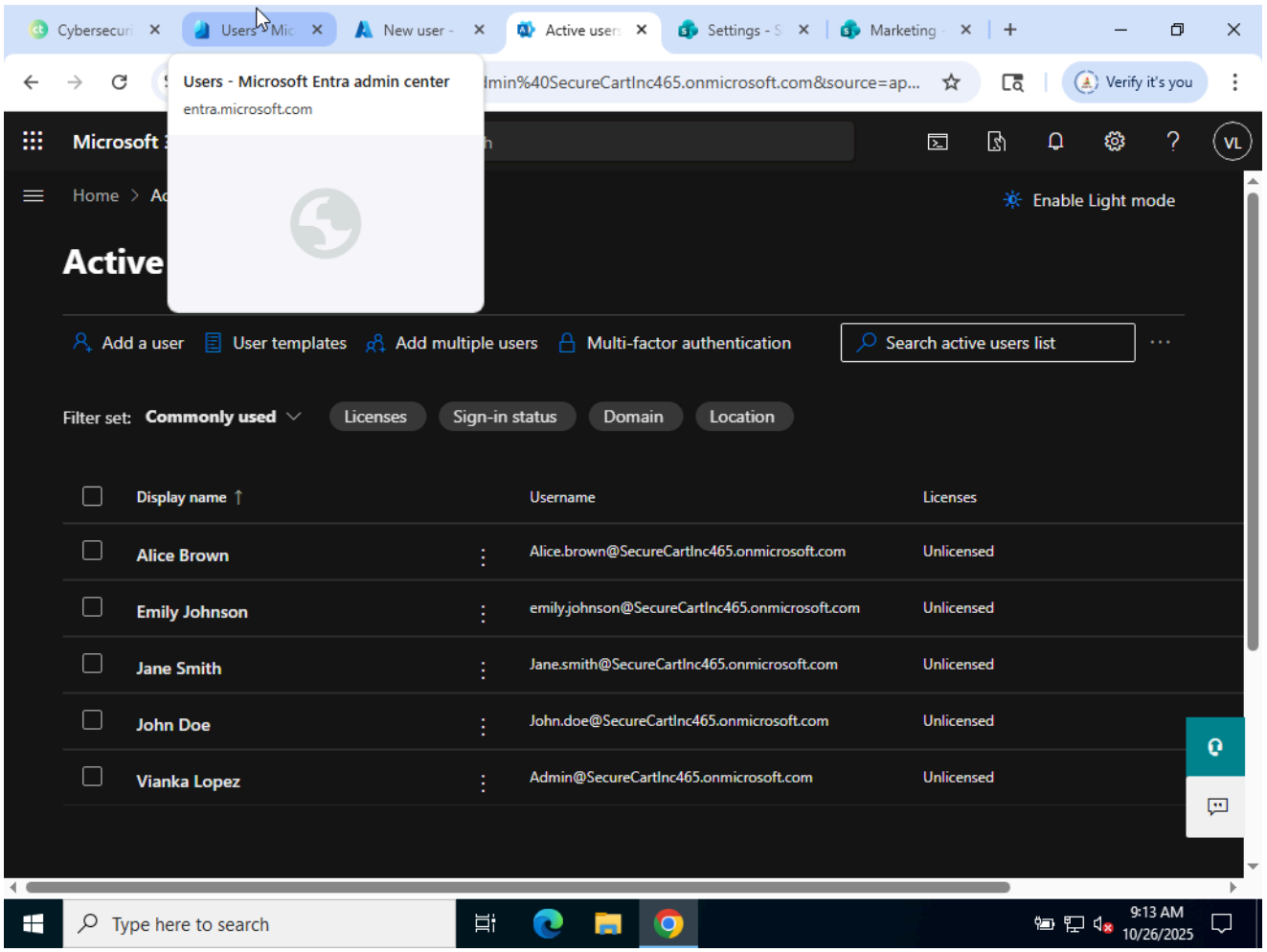
Executive Summary

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:

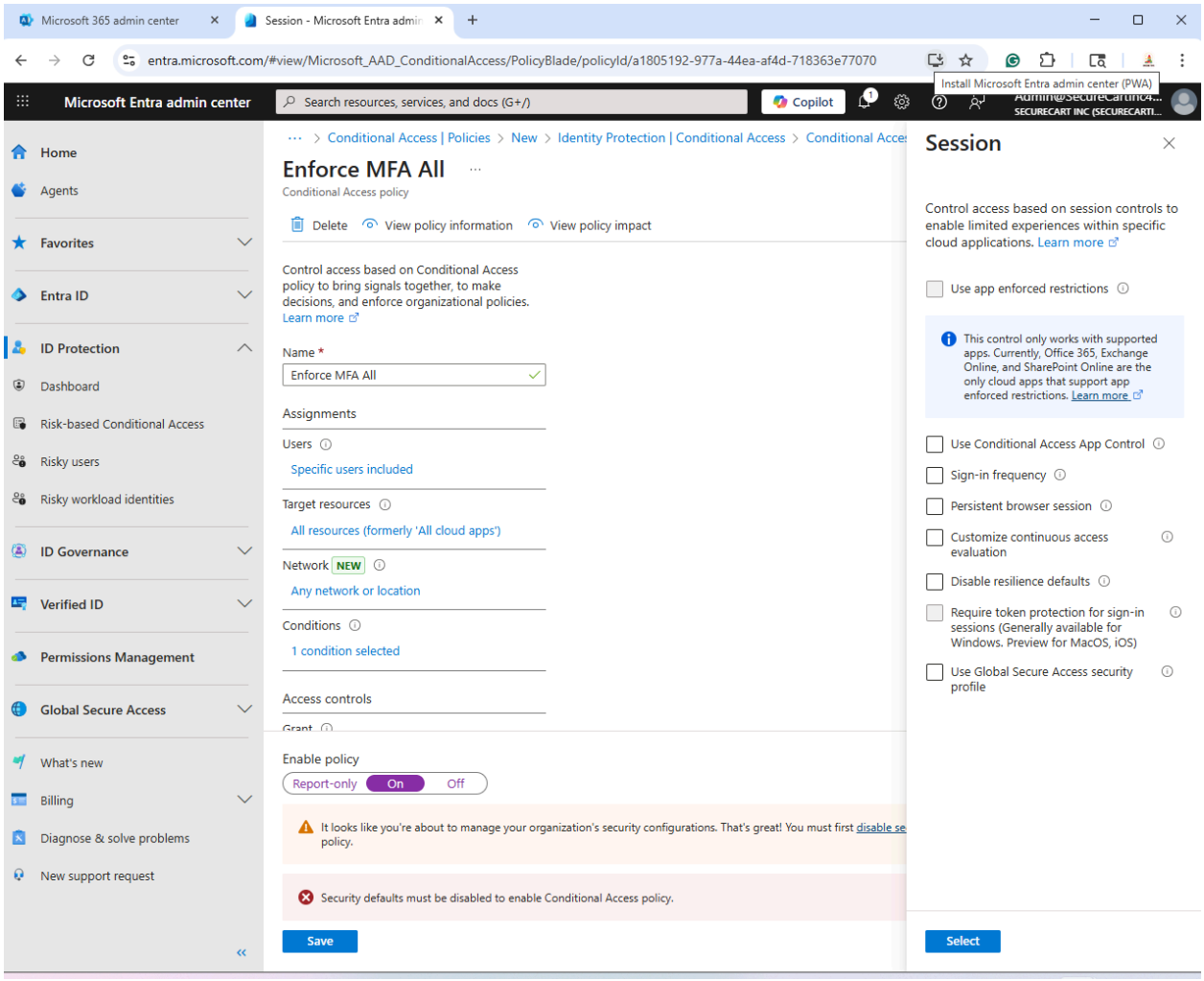
Role Fix: Alice Brown's role changed from Global Administrator to User Administrator. John Doe retains Global Administrator rights.
Fiance Group Fix: John Doe was removed from Fiance_ User; only verified Fiance staff remain.
Sales Group Fix: Emily Johnson added to Sales_Users
Support Group Creation: 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.



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:

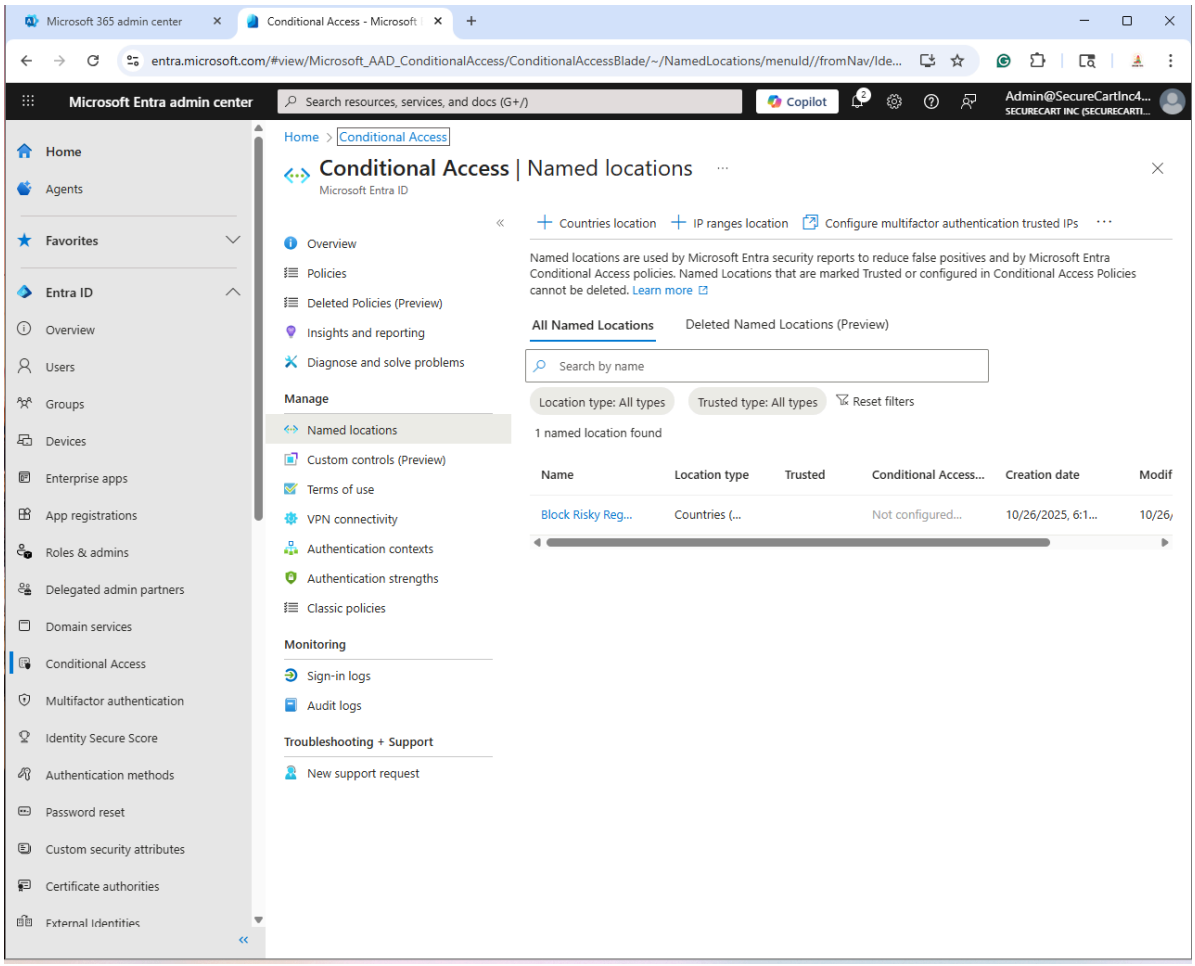
- **MFA:** Multi-Factor Authentication is required for all users using Microsoft Authenticator
- **Location-Based Access:** Sign-ins are restricted to regions (United States, Canada) and are blocked from high-risk regions.
- **Session Controls:** Session reauthentication is required every 12 hours to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



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:

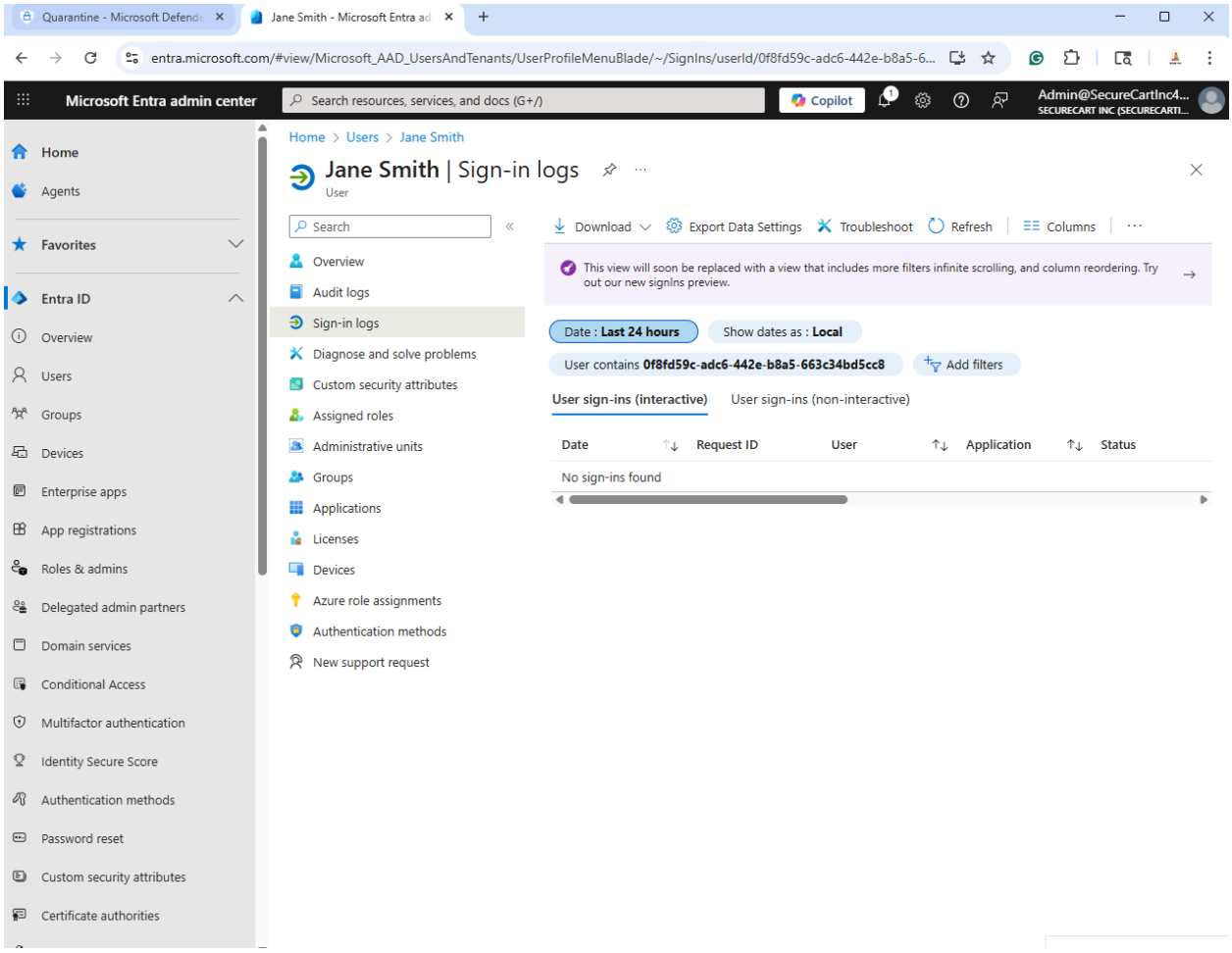
- **Preparation**: Defined roles, tools (Defender for Office 365, Entra ID logs, Security & Compliance Center)
- **Detection & Analysis:** Identified phishing email through quarantine and anti-phishing alerts. Reviewed Entra ID sign-in logs for suspicious activity.
- **Containment:** Quarantined malicious 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.



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.



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.