| **Section** | **What You’ll Do** | **Tools Used** |
| --- | --- | --- |
| **1. GRC Governance Setup** | Create risk register, define NIST mappings, document audit procedures | Excel, Word |
| **2. IAM Governance** | Set up Entra ID with Conditional Access, PIM, Access Reviews, and JML automation | Microsoft Entra ID Dev Tenant |
| **3. Cloud Security** | Secure AWS workload (3-tier app), set up CloudTrail, Guard Duty, and IAM least privilege | AWS Free Tier |
| **4. SOC Monitoring** | Ingest logs, configure Splunk alerts, simulate attacks, and create incident tickets | Splunk, Sysmon, TryHackMe or SimuLand |
| **5. Linux Hardening + Forensics** | Harden Linux VM, log activity, and detect tampering | Ubuntu VM |
| **6. Documentation + Reporting** | Create full audit, executive report, incident report, and project plan | Word, Excel, GitHub Pages |
| **7. Resume + LinkedIn Portfolio** | Publish to GitHub or website, reference project in resume, post on LinkedIn | GitHub/Portfolio site |

**. GRC Governance Setup**

**Create Internal Users in Microsoft Entra ID**

**🔹 Summary:**

* Created 6 internal users in Microsoft Entra ID using “+ New User” (not guest invitation).
* Configured user profiles with custom properties: department, job title, and location.
* Organized users by department (HR, IT, Sales) with unique usernames and roles.

A screenshot of a computer

AI-generated content may be incorrect.

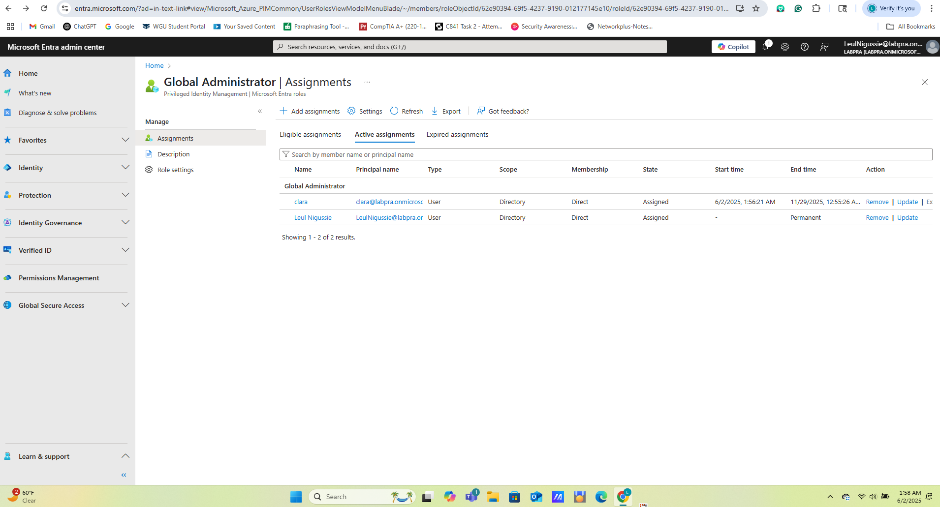
**Screenshot #** “All users” list showing the newly created accounts

**Assign RBAC Roles in Microsoft Entra ID**

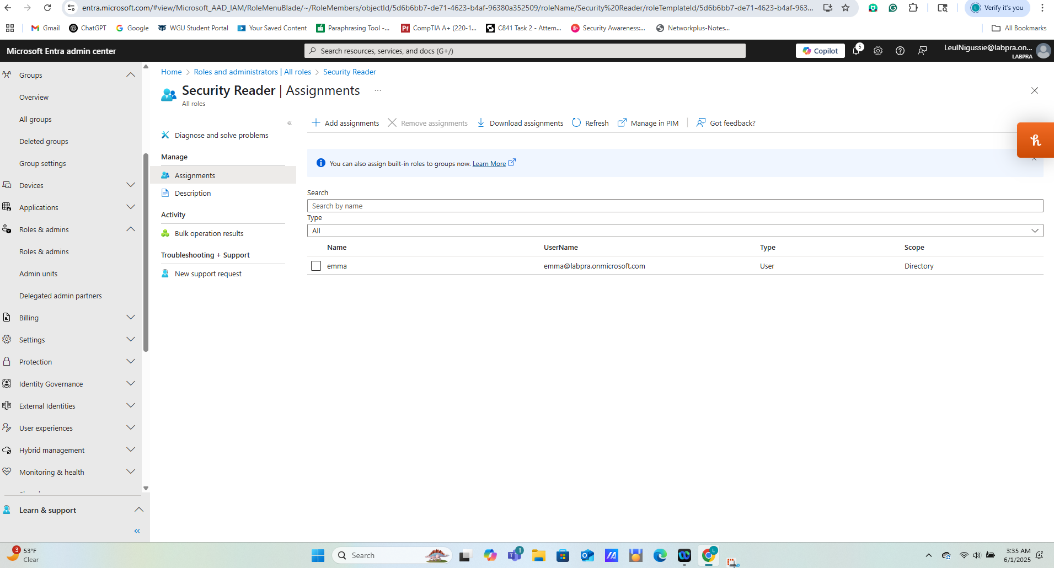
**🔹 Summary:**

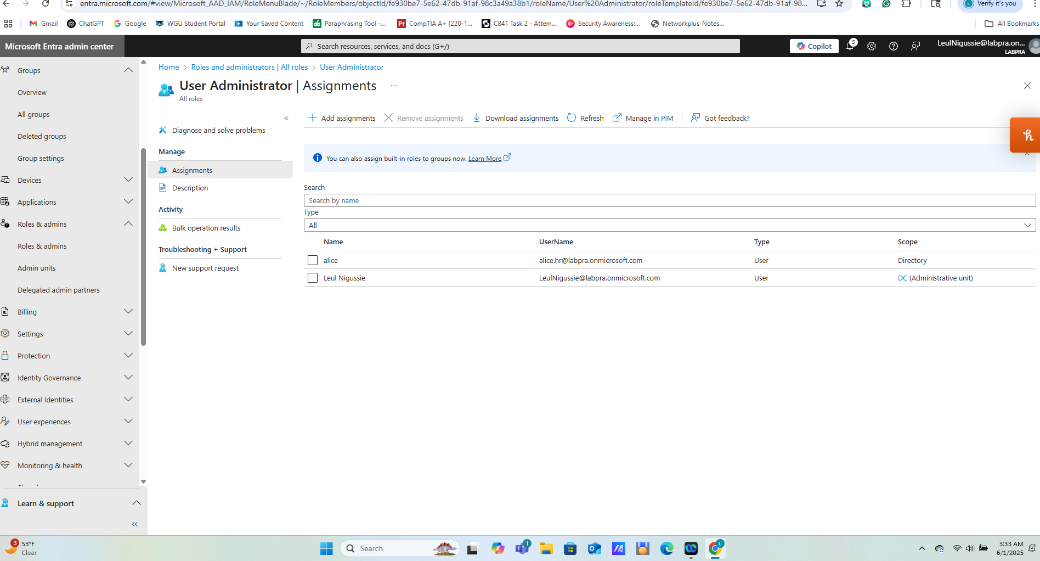
* Assigned **Global Administrator** role to IT department head.
* Assigned **User Administrator** role to HR team lead.
* Assigned **Security Reader** role to the Compliance Officer.
* Used Microsoft Entra’s **Roles & Administrators** panel to manage role-based access securely

**Screenshot:** *Global Administrator* role → “Assignments” tab showing **Clara IT**



**Screenshot: *Security Reader* role → “Assignments” tab showing Emma Compliance**



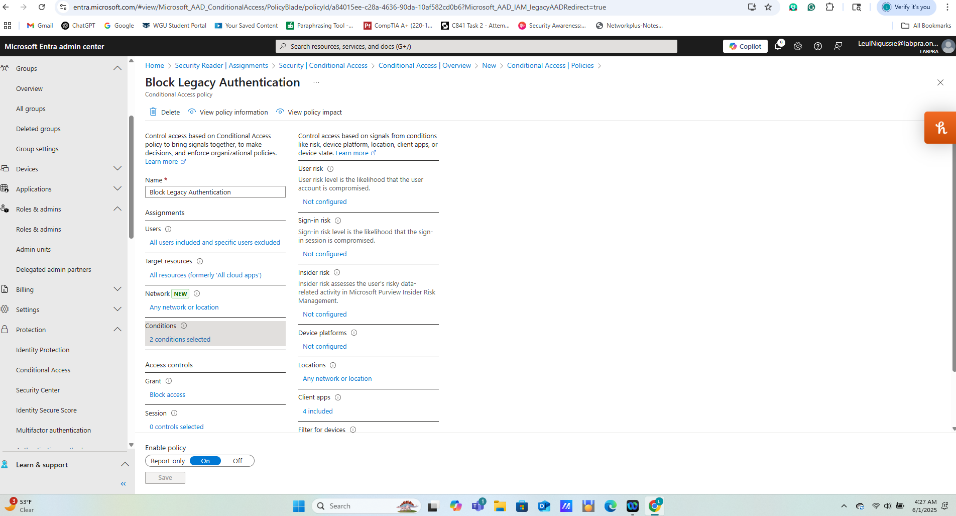
**Screenshot:** *User Administrator* role → “Assignments” tab showing **Alice HR**

**Create and Configure Conditional Access Policies in Microsoft Entra ID**

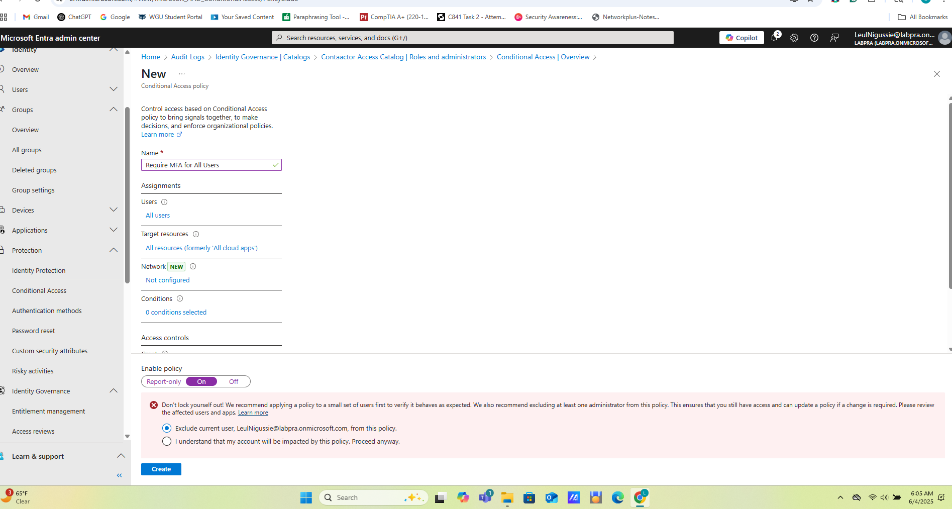
**🔹 Summary:**

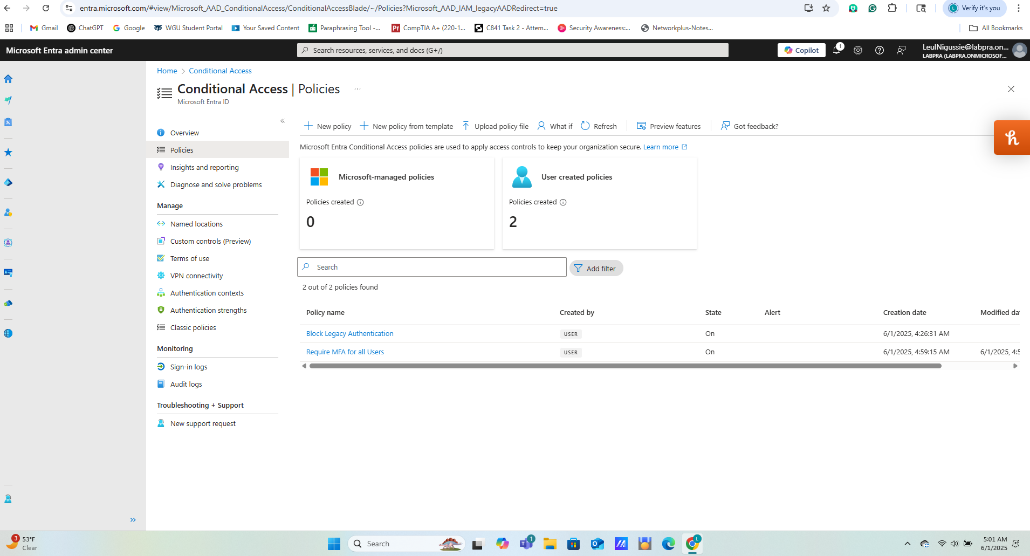
* Designed and implemented **5 Conditional Access Policies** to enforce secure access across Microsoft 365 resources.
* Policies include:
  1. **Block Legacy Authentication**
  2. **Require MFA for All Users**
  3. **Admins Secure Access Policy** with MFA + compliant device
* Utilized **identity-driven conditions** like client app type, location, device compliance, and role-based targeting.
* Ensured granular access control using Microsoft Entra’s built-in **Zero Trust policy engine**.

**Screenshot of** Conditional Access policy blocking legacy authentication clients



**Screenshot of** Conditional Access policy enforcing MFA + device compliance for admin roles



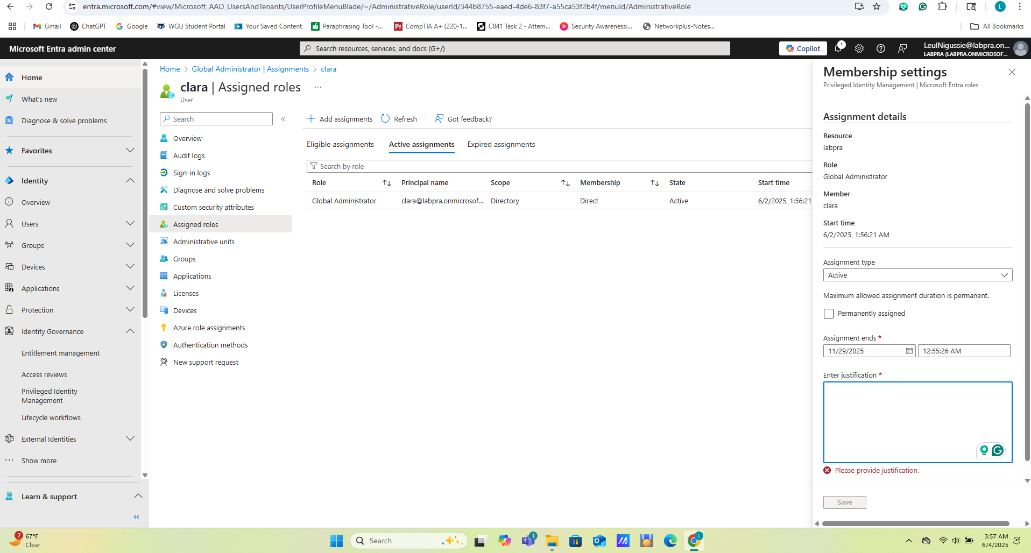
**Screenshot of** Conditional Access policy requiring MFA except in trusted locations

**Configure Privileged Identity Management (PIM) in Microsoft Entra ID**

**🔹 Summary:**

* Enabled **Just-In-Time (JIT)** access to sensitive roles using Microsoft Entra’s **Privileged Identity Management (PIM)**.
* Assigned eligible roles (Global Admin & Security Admin) with enhanced security controls:
  + **Approval required**
  + **Multi-factor authentication (MFA) required**
  + **1-hour activation window**
  + **Justification enforced**
  + **Notifications on activation**
* Verified PIM role assignment settings and reviewed activation logs for auditing.

Screenshot of Privileged Identity Management (PIM) settings and activation history showing eligible role assignments, MFA enforcement, approval requirement, and 1-hour JIT activation.



**Configure Access Reviews for Group Membership in Microsoft Entra ID**

**🔹 Summary:**

* Created a recurring **Access Review** for the **Sales Department group** in Microsoft Entra ID.
* Review was configured to:
  + 🔁 **Run quarterly**
  + 👥 **Scope**: Group membership of the Sales Department
  + 👤 **Reviewer**: Assigned to the Sales Manager
  + ⏳ **Duration**: 14 days to complete each review
  + ⚙️ **Automation**: Auto-apply results and remove access for unreviewed users
* This ensures only authorized users retain access and supports **least privilege** and **compliance** principles.

ScreenshotQuarterly Access Review configuration for Sales Department group showing scope, reviewer assignment, recurrence, and auto-remove settings

A screenshot of a computer

AI-generated content may be incorrect.

**Monitored and exported Audit Logs in Microsoft Entra ID to support compliance and security operations.**

Reviewed recent activities related to Directory Management, Authentication and Authorization, and Role and Application Management.

Applied filters to identify specific high-impact events and verified successful completion of sensitive actions.

Exported filtered logs for documentation and compliance purposes.

Used the logs to support identity governance, audit readiness, and security incident review processes.

Microsoft Entra ID – Audit Logs Overview

A screenshot of a computer

AI-generated content may be incorrect.

**Create VPC and Subnets in AWS**

🔹 **Summary:**  
• Created a custom Virtual Private Cloud named **VPC for Leul** to support a secure multi-tier architecture.  
• Enabled **DNS hostname support** for name resolution within the VPC.  
• Added the following subnets:  
 o **1 Public Subnet** – for internet-facing (Web) tier  
 o **2 Private Subnets** – for internal App and DB tiers  
• Ensured subnets were placed in **separate Availability Zones** for high availability and fault tolerance.

Screenshot of Virtual Private Cloud named **VPC for Leul**

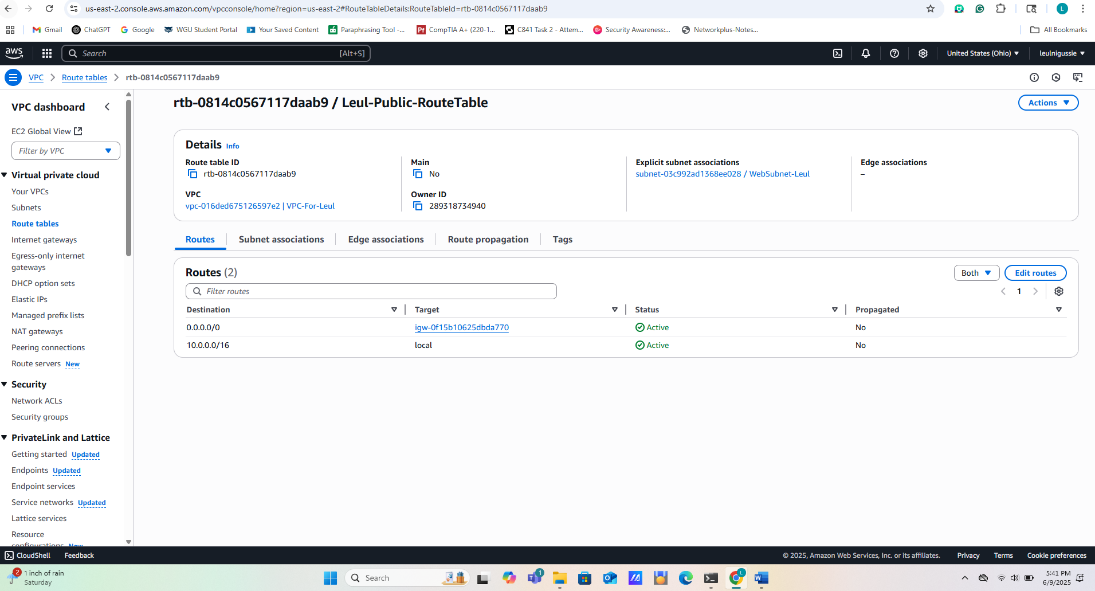
A screenshot of a computer

AI-generated content may be incorrect.

**Configure Route Table and Internet Gateway**

🔹 **Summary:**  
• Created a custom **route table** for the **public subnet** in VPC for Leul.  
• Attached an **Internet Gateway (IGW)** to enable outbound internet access.  
• Added a route for 0.0.0.0/0 in the public route table, pointing to the IGW.  
• Confirmed that **only the public subnet** is associated with this route table to enforce proper network segmentation.

📸 **Screenshots to include:**  
• **Screenshot #**  
 Route Tables → **Routes tab** → Show 0.0.0.0/0 route pointing to Internet Gateway

  
• **Screenshot**   
 Internet Gateway → Show **attachment** to VPC for Leul

A screenshot of a computer

AI-generated content may be incorrect.

**Security Groups**

**What you did:**

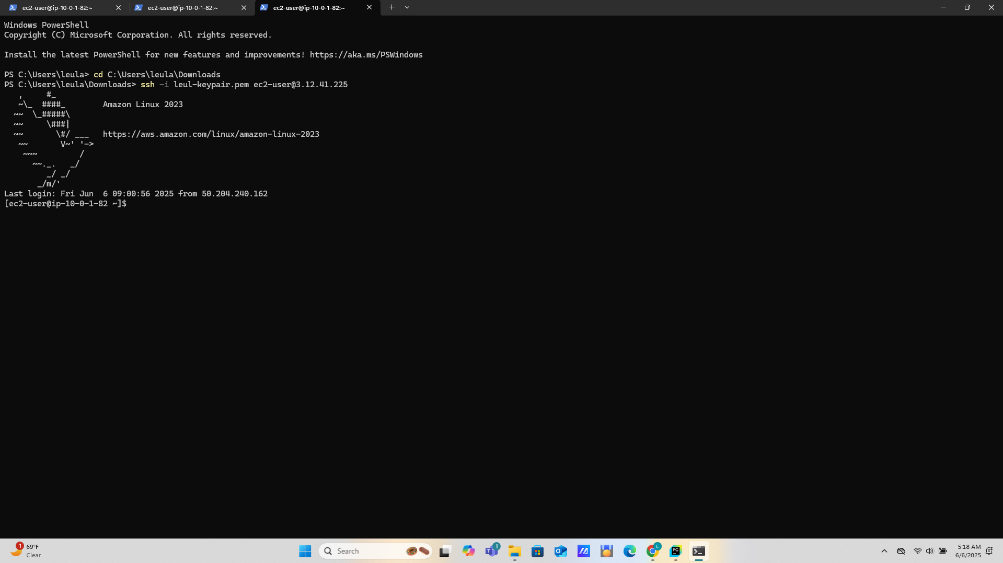
* Created Security Groups with least privilege:
  + Web SG: Allow HTTP/HTTPS from the internet
  + App SG: Allow from Web SG only
  + DB SG: Allow from App SG only (e.g., port 3306 for MySQL)

📸 **Screenshot #:**  
**Security Groups → Inbound Rules tab for Web, App, and DB**

A screenshot of a computer

AI-generated content may be incorrect.

**SSH connection** to **Web EC2 instance**



**Summary:**  
• Verified **internal communication** between EC2 instances and **public access** to the web server:  
 o SSH into **Web EC2** → Successfully **pinged/curl’d App EC2** using its private IP  
 o Confirmed that **Web server is accessible from the internet** using its public IP📸 **Screenshot #8:**  
**Ping/curl test result from Web to App (terminal)**

A computer screen shot of a black screen

AI-generated content may be incorrect.

📸 **Screenshot #10:**  
**Browser showing Web server page using Public IP**

A screenshot of a computer

AI-generated content may be incorrect.

**Enable AWS Guard Duty**

**Summary:**  
• Enabled **Amazon GuardDuty** to detect and alert on suspicious activity in the AWS environment.  
• GuardDuty began monitoring:

1. **VPC Flow Logs**
2. **DNS Query Logs**
3. **AWS CloudTrail Logs**  
   • Viewed active findings and optionally triggered sample findings to test threat detection.

📸 **Screenshots to include:**  
• **Screenshot #1:** GuardDuty Dashboard showing "**GuardDuty is enabled**" and findings count

A screenshot of a computer

AI-generated content may be incorrect.  
• **Screenshot #2:** Findings tab showing **1–2 findings**

A screenshot of a computer

AI-generated content may be incorrect.

**Enable AWS CloudTrail**

**Summary:**  
• Enabled **AWS CloudTrail** to capture audit logs of all account activity for security and compliance.  
• Configured a new trail named MySecureTrail:

1. Created or selected an **S3 bucket** for log storage
2. Applied the trail to **all AWS regions**
3. Enabled both **management events** and **data events** for comprehensive logging

📸 **Screenshots to include:**  
• **Screenshot #** CloudTrail Dashboard → **Trail list** showing trail name, status, and S3 destination

A screenshot of a computer

AI-generated content may be incorrect.  
• **Screenshot #** S3 console → Show **CloudTrail logs folder structure** or open a sample log file

A screenshot of a computer

AI-generated content may be incorrect.

Splunk Internal Audit Log Monitoring

Enabled internal audit log monitoring in Splunk to track administrative activity, user behavior, and system changes for security operations and compliance oversight.  
• Queried the audittrail sourcetype (index=\_audit) to identify user search actions, login attempts, role changes, and application access.  
• Leveraged this data to support GRC audit readiness, detect insider threat patterns, and build alerts for unusual user activity.  
• Demonstrated integration of audit logs into centralized SOC dashboards for real-time visibility and historical review.

**Screenshot #** Splunk Internal Audit Log Monitoring

A screenshot of a computer

AI-generated content may be incorrect.

**plunk Sysmon Process Creation Monitoring**

Enabled process creation monitoring using **Sysmon Event ID 1** logs ingested into **Splunk** to support endpoint visibility, threat detection, and forensic analysis.  
• Configured Sysmon with SwiftOnSecurity XML to capture detailed process creation events on Windows systems.  
• Queried logs in Splunk using index=sysmon EventCode=1 to identify execution of suspicious binaries such as PowerShell, cmd.exe, and encoded scripts.  
• Built real-time alerts for abnormal child-parent process relationships and potential living-off-the-land (LOLBins) activity.  
• Integrated Sysmon process data into Splunk dashboards to support SOC investigations and MITRE ATT&CK technique mapping.

A screenshot of a computer

AI-generated content may be incorrect.