**Phase 9: Reporting, Dashboards & Security Review**

**Executive Summary**

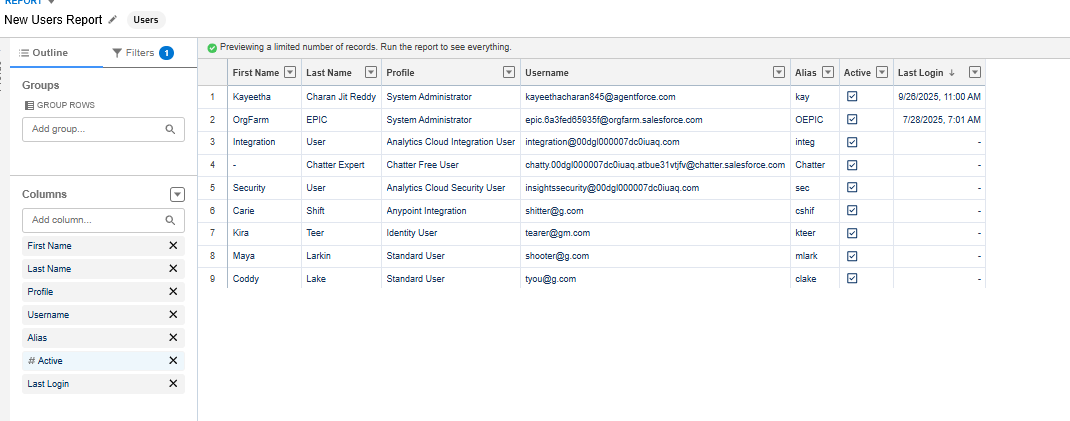
In this phase, we converted the raw phishing training and simulation data into **actionable intelligence** through reports and dashboards. We also conducted a **security review** to ensure that sensitive employee performance data is protected.

The objective was twofold:

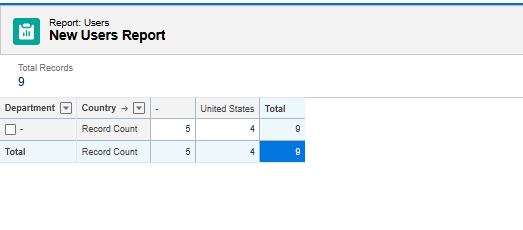
1. Provide managers with real-time visibility into training progress and awareness scores.
2. Strengthen the org’s security posture with strict access controls, session policies, and audit monitoring.

**Reports (Tabular, Summary, Matrix, Joined)**

1. **Tabular Report** – *Employee Training Data Export*
   * Navigation: **App Launcher → Reports → New Report**
   * Report Type: Employees with Completions
   * Fields: Employee Name, Department, Training Status, Overall Score
   * Purpose: Flat list for exporting raw data for compliance audits.



1. **Summary Report** – *Training Completion by Department*
   * Group by: Department
   * Summarize: Count of Completed vs Pending
   * Purpose: Managers can instantly see departmental progress.



1. **Matrix Report** – *Awareness Score by Department vs Status*
   * Rows: Department
   * Columns: Training Status
   * Values: AVG(Overall Training Score)
   * Purpose: Heatmap-style view to find weak areas.
2. **Joined Report** – *Assignments vs Completion Gaps*
   * Block 1: Assignments per Employee
   * Block 2: Completions per Employee
   * Purpose: Highlights employees with overdue or incomplete training.

**Report Types**

A **Custom Report Type** was created to analyze employees who were assigned training but have not completed it yet.

* Navigation: **Setup → Report Types → New Custom Report Type**
* Primary Object: Employee\_\_c
* Related Object: Completion\_\_c (optional)
* Relationship: “With or without related records” (outer join).
* Purpose: Allows reporting on both completed and uncompleted assignments.

A screenshot of a computer

AI-generated content may be incorrect.

**Dashboards**

We built a central dashboard called **Phishing Awareness Overview** to provide managers with an at-a-glance view.

**Components:**

1. **Gauge** – % Training Completed.
2. **Bar Chart** – Completion by Department.
3. **Donut Chart** – Training Status distribution (Assigned, In Progress, Completed).
4. **Lightning Table** – Top 5 employees with lowest awareness scores.

A screenshot of a computer

AI-generated content may be incorrect.

**Sharing Settings**

* Navigation: **Setup → Sharing Settings**
* Configurations:
  + OWD (Organization-Wide Defaults): Employee\_\_c = Private
  + Sharing Rule: If Department\_\_c = IT, share with IT Managers group.
* Purpose: Protects employee performance data while enabling departmental oversight.

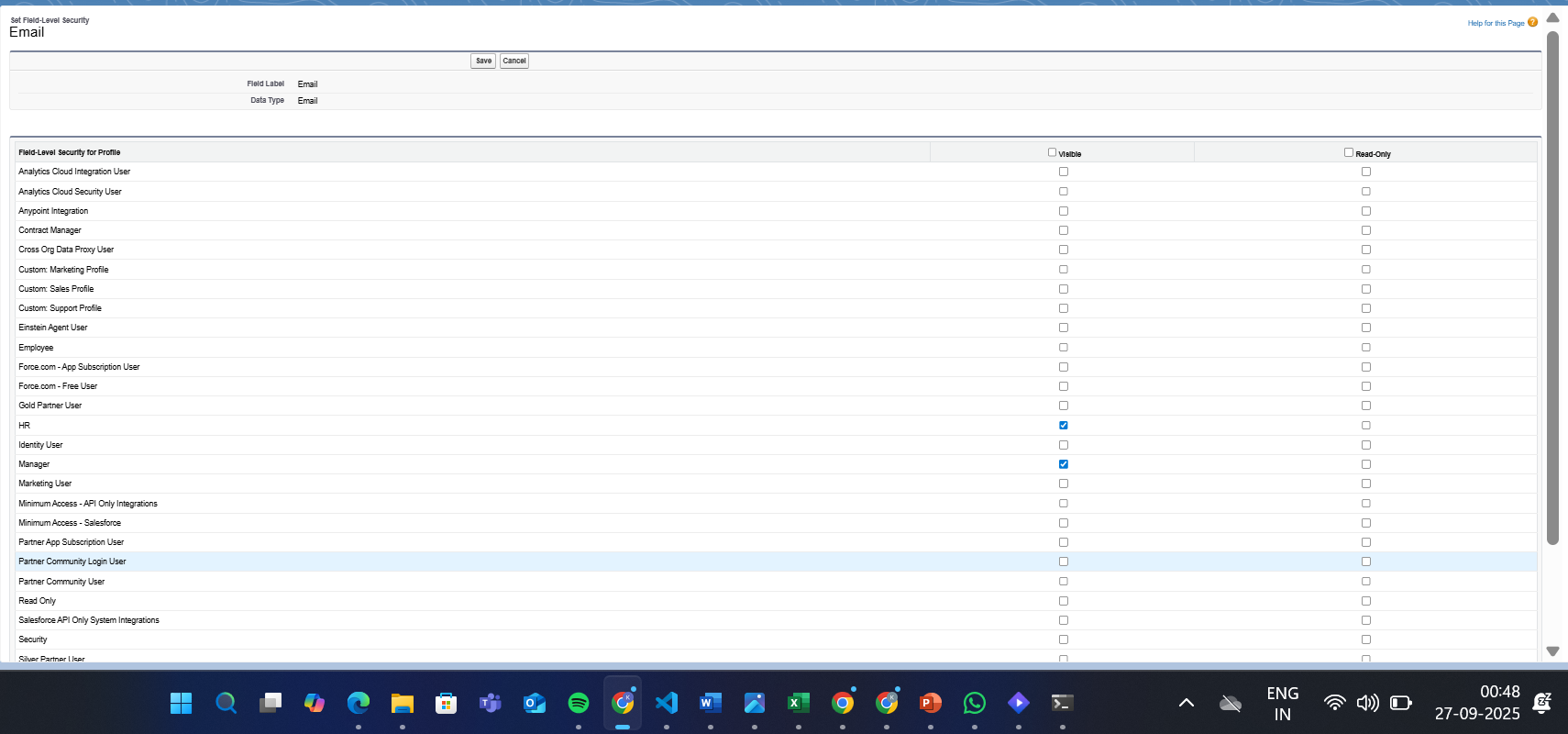
A screenshot of a computer

AI-generated content may be incorrect.

**Field-Level Security (FLS)**

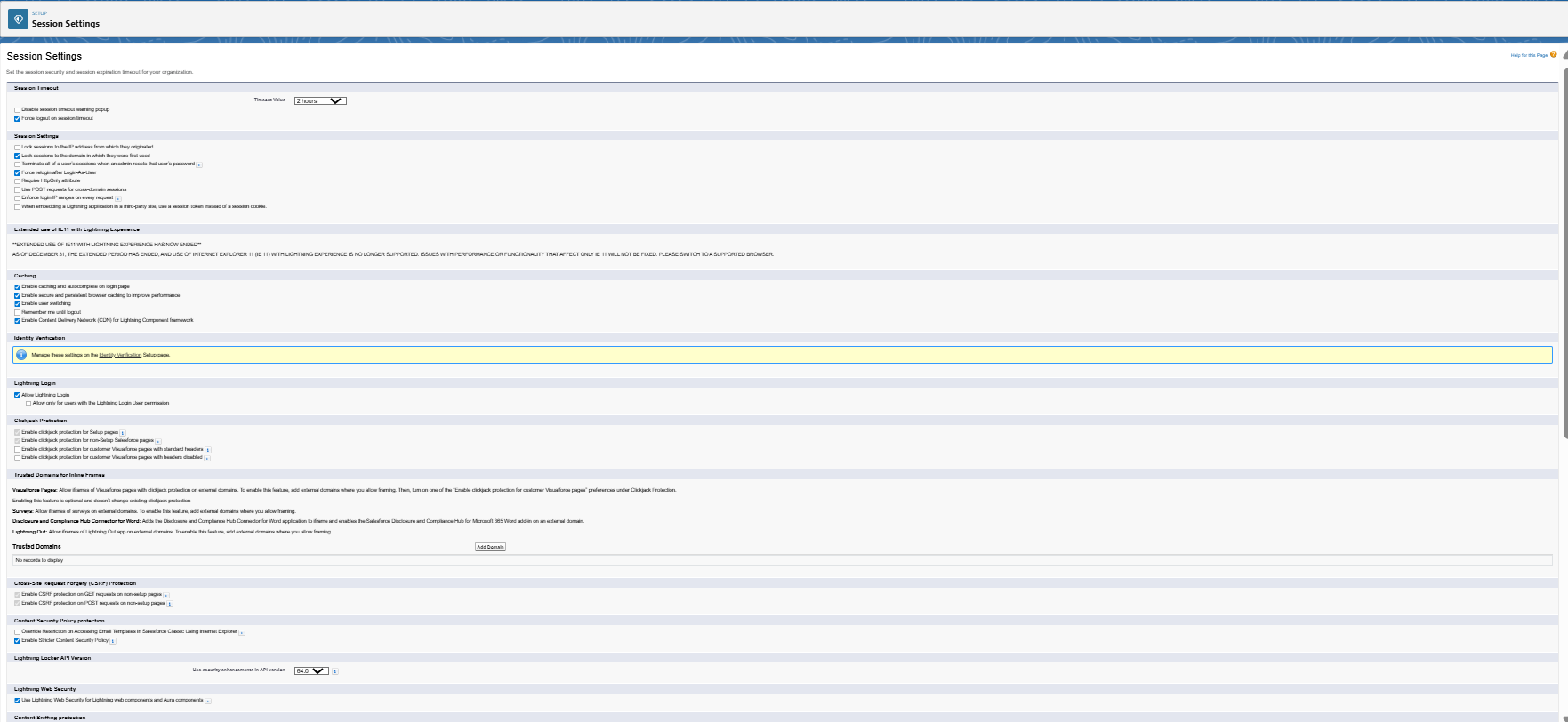
* Navigation: **Setup → Object Manager → Employee\_\_c → Fields & Relationships → Field-Level Security**
* Example Configurations:
  + Overall Training Score → visible only to Managers and Admins.
  + Email → hidden from Training Coordinators to maintain privacy.

A screenshot of a computer

AI-generated content may be incorrect.

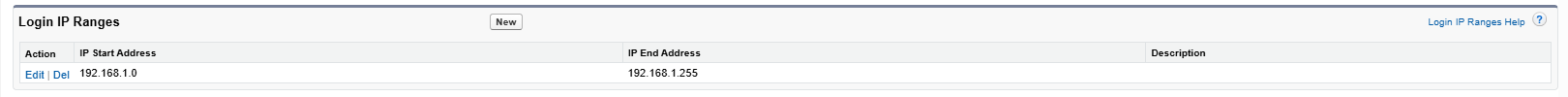
**Session Settings**

* Navigation: **Setup → Session Settings**
* Changes:
  + Reduced session timeout: 2 hours.
  + Enabled “Lock sessions to originating IP”.
* Purpose: Reduces risk of session hijacking.



**Login IP Ranges**

* Navigation: **Setup → Profiles → [Manager Profile] → Login IP Ranges**
* Restriction: Managers can only log in from office IP range.
* Example: Start: 192.168.1.1, End: 192.168.1.255.



**Audit Trail**

* Navigation: **Setup → View Setup Audit Trail**
* Purpose: Monitor and confirm all critical changes (e.g., sharing settings, FLS, session settings).
* Records can be downloaded (6-month history).

A screenshot of a computer

AI-generated content may be incorrect.

**Conclusion**

Phase 9 transformed raw project data into meaningful insights through reports and dashboards, while also performing a **security hardening review**. The system is now:

* **Transparent** – with powerful reporting & dashboards.
* **Secure** – with proper FLS, sharing, session, and audit controls.
* **Scalable** – ready for deployment in enterprise environments.