

# Staying Ahead of Recent Salesforce Social Engineering Attacks

## Background

Recent high-profile incidents, including the ShinyHunters-led theft of sensitive data from Salesforce environments at major organizations [1, 2], highlight a growing and sophisticated threat: social engineering combined with misuse of connected applications. In these attacks, a threat actor convinces a targeted user to access Salesforce's Connect setup page and enter a "connection code," thereby linking the attacker-controlled Data Loader to the victim's Salesforce environment. Once connected, this access can enable large-scale exfiltration of sensitive data without triggering traditional perimeter-based alerts. While Salesforce recommends [3] measures such as enforcing trusted IP ranges, enabling MFA, restricting connected apps, and leveraging Salesforce Shield, these threats underscore that misconfiguration, excessive permissions, and lack of continuous monitoring remain significant risk factors. This is where Reco's Dynamic SaaS Security capabilities provide added layers of protection, detecting posture drift, monitoring connected apps and risky API usage, and identifying anomalies before they escalate into breaches.

## 1 Enforcing Trusted IP Ranges for Logins

### Salesforce Control

- Restrict login attempts to trusted IP ranges.

### Reco Control

- Salesforce - IP Range Enforcement Enabled for Every Request (Posture)

### How Reco Helps

- Detects when IP range enforcement is missing or weakened. Ensures every request is validated against trusted ranges to block unauthorized network access.



## 2 Principle of Least Privilege for App Permissions (PoLP)



### Salesforce Controls

- Multiple checks ensuring minimal permissions are granted to users and integrations.

### Reco Controls

Risk Area	Reco Posture Check	Description
Excessive app scopes	Salesforce - OAuth Connected Apps Use Least Privilege Scopes	Flags apps requesting more access than needed.
MFA bypass	Salesforce - No Users With Bypass MFA Permission	Identifies users who can log in without MFA.
PII exposure	Salesforce - More than 15 users have permission to view (PII) data	Tracks exposure of personal data to too many users.
Bulk deletions	Salesforce - Max 15 Users With Bulk API Hard Delete Permission	Limits destructive mass operations.
Account deletions	Salesforce - More than 5 users have permission to delete accounts	Controls customer data loss risk.
Data export	Salesforce - Max 15 Users with Weekly Data Export Permission	Reduces chances of full data dumps.
Manage dataspace	Salesforce - Max 15 Users with Manage Dataspace Scope Permission	Restricts changes to data segmentation.
Data Cloud profile	Salesforce - Max 15 Users with Data Cloud Profile Explorer Permission	Limits data browsing by non-essential users.
Modify all data	Salesforce - Maximum 10 Users Have Modify All Data Permission	Prevents overuse of highest privilege.
API access	Salesforce - Users With API Access Permissions	Restricts external API integrations to approved accounts.



## 3 Enabling Multi-Factor Authentication (MFA)

### Salesforce Controls

- Enforce MFA for all accounts.

### Reco Controls

- Posture Check - Salesforce - Users without MFA - Flags non-compliant users for remediation.
- Identities Dashboard - Identities without MFA in Salesforce dashboard - Visualizes accounts lacking MFA.

App: Salesforce Overview

App Owner: + New App Owner

Response Plan Posture Checks Accounts Policies Alerts SaaS-to-SaaS Events Compliance Public Links

41 Accounts 0 NO MFA 2 INACTIVE 0 GUEST 18 ADMIN 0 ADMIN - INACTIVE 0 ADMIN - NO MFA

Showing 41 Accounts Search Name, Email, Id Saved View: Exclude: Deactivated + Filters Reset Export

Name	Account Email	Last Login	Analysis	Open Alerts	Role	Profile	Permission Sets
A		3 hours ago	+ Label	0	Sales Manager	System Administratrc	Knock_Account_Fielf +5
A		an hour ago	+ Label	0	Sales Manager +1	BDR +1	Knock_Account_Fielf +10
A		2 hours ago	+ Label	0	Sales Rep	BDR	Knock_Account_Fielf +9
S		NA	SERVICE X EXTERNAL X + Label	0			
B		2 hours ago	+ Label	0	Sales Manager	Account Executive	Knock_Account_Fielf +7
B		3 hours ago	+ Label	0	Admin	System Administratrc	Knock_Account_Fielf +7
C		17 hours ago	+ Label	0	Sales Rep	Account Executive	Knock_Account_Fielf +8
D		2 hours ago	+ Label	1		System Administratrc	Knock_Account_Fielf +3
D		2 hours ago	+ Label	0	Sales Rep	Account Executive	Knock_Account_Fielf +5
G		3 hours ago	+ Label	0	Admin	System Administratrc	Knock_Account_Fielf +8
I		an hour ago	SERVICE X + Label	0		Sales Insights Integr.	

4

## Restricting Use of Connected Apps and Managing Access Policies

### Salesforce Controls

- Ensure connected apps are secure and API access is restricted.

### Reco Controls

- Posture Check - Salesforce - Connected Applications Securely Configured - Detects insecure settings in connected apps.
- Posture Check - Salesforce - Connected Apps Use API-Only Integration Users - Prevents apps from using full human accounts.
- Posture Check - Salesforce - API Access Restricted to Admin-Approved Connected Apps - Ensures only vetted apps connect.
- SaaS-to-SaaS applications dashboard** - Lists and risk-ranks all connected third-party apps.

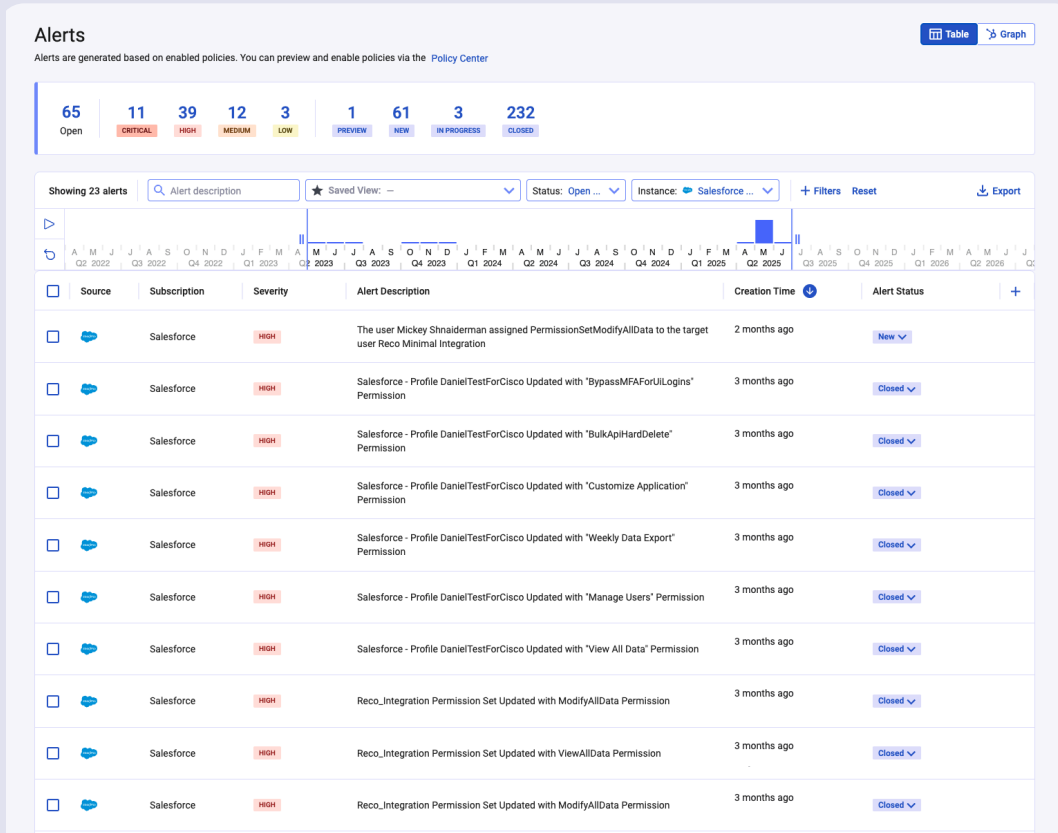
# 5

## Using Salesforce Shield for Threat Detection and Event Monitoring

### Salesforce Controls

- Monitor events, enforce policies, and detect suspicious activity.

### Reco Controls



### Former Employee & Risky Account Monitoring

- Reco - Former Employees with Active Access to Salesforce (Advanced Analytics Policy) - Detects active accounts of terminated users.
- Salesforce - Former Org User Successfully Logged In (Policy) - Real-time alert on logins from former employees.
- Salesforce - Inactive User Successfully Logged In / Salesforce - Inactive External User Successfully Logged In - Flags dormant accounts suddenly used.

### Anomalous & Malicious Activity Detection

- Salesforce - API Anomaly Event - Spots abnormal API usage patterns.
- Salesforce - Mass File Activity in Salesforce - Detects bulk file operations.
- Salesforce - Excessive Report Export Activity - Alerts on unusual data report downloads.

- Salesforce - Risky / Leaving Employee Excessive Download - Targets insider data theft scenarios.
- Salesforce - Potentially Customer Emails Exported by Leaving/Risky User - High-risk communication data leakage.

## Privilege Escalation & Misconfiguration Changes

Detects assignment or update of high-privilege permissions:

- ModifyAllData
- ViewAllData
- CustomizeApplication
- ManageUsers
- BulkApiHardDelete
- DataExport
- BypassMFAForUiLogins
- AuthorApex
- Read Logs/Events

### Example policies

Salesforce - Permission Set Updated with "ModifyAllData" Permission, Salesforce - Profile Updated with "CustomizeApplication" Permission.

## Session & Login Risks

- Salesforce - Session Hijacking Event - Identifies potential account takeover.
- Salesforce - Multiple Failed Logins by Same User - Brute force detection.
- Salesforce - Successful 3rd Party App Login to Salesforce with Stale User Credentials - Detects outdated credential usage.
- Salesforce - Successful 3rd Party App Login to Salesforce with Stale Admin Credentials - Admin credential risk detection.
- Salesforce - Attempted 3rd Party App Login to Salesforce with Inactive User Credentials - Flags blocked, but suspicious, access attempts.
- Salesforce - User Successfully Logged In without SSO - Detects MFA/SSO bypass.

### Salesforce - Events Dashboard

App: Salesforce Overview

App Owner: New App Owner

Response Plan Posture Checks Accounts Policies Alerts SaaS-to-SaaS **Events** Compliance Public Links

Showing Over 100K Events Search by actor Saved View: Event type contains: login X + Filters Reset Export

Event Time	Instance	Actor	IP Address	Event Type	Application	View
3 minutes ago	Salesforce		35.238.57.88	login_success	Chili Piper - Sales Acceleration 3.0	<a href="#">View Event</a>
6 minutes ago	Salesforce		20.221.201.113	login_success	N/A	<a href="#">View Event</a>
6 minutes ago	Salesforce		98.84.152.14	login_success	Slack	<a href="#">View Event</a>
12 minutes ago	Salesforce		35.238.57.88	login_success	Chili Piper - Sales Acceleration 3.0	<a href="#">View Event</a>
14 minutes ago	Salesforce		34.223.203.1	login_success	Segment	<a href="#">View Event</a>
16 minutes ago	Salesforce		3.230.119.177	login_success	Slack	<a href="#">View Event</a>
18 minutes ago	Salesforce		18.234.128.44	login_success	Slack	<a href="#">View Event</a>
19 minutes ago	Salesforce		54.86.144.88	login_success	Slack	<a href="#">View Event</a>
24 minutes ago	Salesforce		34.223.203.1	login_success	Segment	<a href="#">View Event</a>
35 minutes ago	Salesforce		20.221.201.113	login_success	N/A	<a href="#">View Event</a>
35 minutes ago	Salesforce		20.221.201.113	login_success	N/A	<a href="#">View Event</a>
36 minutes ago	Salesforce		44.236.183.129	login_success	SfdcSIQActivitySyncEngine	<a href="#">View Event</a>
39 minutes ago	Salesforce		18.212.174.20	login_success	Slack	<a href="#">View Event</a>
39 minutes ago	Salesforce		18.212.174.20	login_success	Slack	<a href="#">View Event</a>
40 minutes ago	Salesforce		54.188.206.87	login_success	Prospect	<a href="#">View Event</a>
40 minutes ago	Salesforce		54.188.206.87	login_success	Prospect	<a href="#">View Event</a>
44 minutes ago	Salesforce		100.21.196.196	login_success	SfdcSIQActivitySyncEngine	<a href="#">View Event</a>

## Data Exposure Prevention

- Salesforce - File Shared Publicly Without Password
- Salesforce - File Shared Publicly Without Expiry Date
- Both prevent uncontrolled external data exposure.
- Salesforce - Public Links dashboard

## 6 SaaS-to-SaaS Risk Visibility

### Salesforce Controls

Monitor and secure third-party integrations.

### Reco Controls

- SaaS-to-SaaS risky permissions dashboard - Shows integrations requesting excessive scopes.
- SaaS-to-SaaS applications dashboard - Comprehensive inventory of all integrated apps, including those bypassing security review.

App: Salesforce Overview

App Owner: + New App Owner

Response Plan Posture Checks Accounts Policies Alerts SaaS-to-SaaS Events Compliance Public Links

Showing 9 Links  + Filters Reset

File name	Actor	Last modified time	Created by	Password required	Number of views
check_upload 6/25/2023				True	0
12412 6/21/2023				False	21
20845 6/21/2023				False	3
contacts_list copy 6/14/2023				False	15
accounts_list copy 2 6/14/2022				False	8
accounts_list copy 5 5/25/2022				False	4
confidential_bizzabo_test 1/23				False	18
RecoLabs Brochure 4/25/2022				False	16
RecoLabs 1-pager 4/25/2022				False	8

< Page 1 > 50 / page

App: Salesforce Overview

App Owner: + New App Owner

Response Plan Posture Checks Accounts Policies Alerts SaaS-to-SaaS Events Compliance Public Links

67 Total 2 Risky 23 Unused 35 Sanctioned 4 Unsanctioned 28 To Review

Showing 9 Apps  Exclude: All App Category: 12 selected + Filters Reset Export

App	Instance	Category	Auth Type	Accounts	First Seen	Last Seen	Status
Superhuman	Salesforce	Email services	OAuth 2.0	1	a year ago	a year ago	To Review
Segment	Salesforce	Productivity tools	OAuth 2.0	1	a year ago	10 months ago	To Review
Pylon	Salesforce	Collaboration	OAuth 2.0	1	3 months ago	2 months ago	To Review
Wave Web	Salesforce	Education	OAuth 2.0	5	2 years ago	17 days ago	Unsanctioned
FactorsAI Production	Salesforce	IT	OAuth 2.0	1	2 years ago	15 hours ago	To Review
Slack	Salesforce	Collaboration	OAuth 2.0	25	3 years ago	13 hours ago	Sanctioned
Zapier	Salesforce	Productivity tools	OAuth 2.0	0	NA	NA	Sanctioned

## 7 Compliance

### Reco Controls

- Salesforce Health Check: Security Best Practices [4]
- Reco - Salesforce Best Practices [5]

Compliance

Reco tracks components of compliance framework relating to SaaS security. View compliance status and their corresponding policies on this page.

+ New Compliance Framework

Frameworks  X

Tracking

- CIS 5.0 - Microsoft 365 Founda... 2/10
- CIS 5.0 - Microsoft Dynamics 36... 0/4
- CIS Snowflake Foundations Ben... 0/7
- HIPAA 0/2
- HITRUST 2/10
- ISO 27001 1/8
- ISO 27002 0/2
- NIST-CSF-2.0 0/1
- PCI-DSS-4.0 2/6
- Reco - Salesforce Best Practices 2/11
- Salesforce Health Check: Securi... 1/4
- Scuba 7/49
- SOC2 Type II 0/3
- Not Tracking

Instance: All Time: Last 90 Days Reset

Salesforce Health Check: Security Best Practices

Salesforce Baseline Standard Settings are Salesforce's recommended configurations for security and functionality within your org. These settings, including security protocols, password policies, and access permissions, aim to balance usability with security, adhering to industry best practices.

Tracking Not Tracking

Checks Passed: 76% 41/54 Enabled 0 Off

Showing 4 Controls  Status: All Show: SaaS Security... Reset Expand All Export

- 1) Salesforce - High Risk Security Settings 18 Passed (100%) 0 Off
- 2) Salesforce - Medium Risk Security Settings 11 Passed (61%) 0 Off
- Administrators Can Log in as Any User 2 Passed (100%) 0 Off
- Enable Content Security Policy protection for email templates 2 Passed (100%) 0 Off
- Enable Content Sniffing protection 2 Passed (100%) 0 Off
- Enforce login IP ranges on every request 1 Passed (50%) 0 Off



## Summary & Next Actions

The Salesforce data theft campaign is a stark reminder that attackers increasingly exploit identity trust, connected app permissions, and misconfigurations, not just network vulnerabilities. With Reco, organizations can go beyond Salesforce's native controls to ensure:

- Continuous verification that security posture aligns with best practices (e.g., MFA enforcement, least-privilege permissions, IP range restrictions)
- Real-time detection of risky connected app activity, anomalous API calls, and privilege escalations
- Immediate alerting and remediation for suspicious logins, excessive data exports, or configuration changes
- Comprehensive visibility into SaaS-to-SaaS integrations and the identities involved

We recommend reviewing your current Salesforce posture in Reco, enabling all relevant detection policies, and scheduling ongoing posture drift reviews. Our team is here to help you make the most of Reco's capabilities, from ensuring the right controls are in place to providing guidance on maximizing detection and protection against connected app abuse scenarios.



[Schedule a Demo](#)