Initial Assessment Items Overview

AREAS ASSESSED

Initial

- Data Classification and Governance
- Data Access by Profile
- Profile Configuration
- Permission Set Configuration
- Remote Site Settings
- API Access
- IP Restrictions
- Login Time Restrictions
- User Login History
- Reporting Access
- System Admin Access
- Session Settings
- Connected Applications
- Misconfigured External Access
- Event Monitoring Configuration
- Field Audit Trail Configuration

Data Classification and Governance

- Have you classified your data? This is key to protecting it.

Data Access by Profile

- Which profiles have broad access to data? What are the object's standard sharing rules?

Profile and Permission Set Configuration

- General checks on security focused settings.

Remote Site Settings

- Are all settings secured and approved?

API Access

- Which users have API access and is it needed?

IP and Login Time Restrictions

- Have these been enabled for users?

User Login History

- Thorough assessment of the last 90 days of logins to highlight issues such as users logging in from regions that are not permitted.

Reporting Access

- Who can run reports and can export them.

System Administrator Access

- Which users are System Administrators as this maximum privileged account should have minimal users.

Session Settings

- Assess the session settings for security best practice.

Connected Applications

- Assess the applications that are currently being used by which users.

Misconfigured External Access

- Assess the Experience Cloud (aka Communities) access to data for security issues.

Event Monitoring and Field Audit Trail Configuration

- Assess if these tools have been purchased and if they have, are the settings optimal.

Platinum7™
PO Box 6143
Hawthorn West 3122
Australia
Phone: +61 404 005 435
Email: info@platinum7.com.au
Web: https://www.platinum7.com.au

Detailed Assessment Items Overview

AREAS ASSESSED

Detailed

- All the Initial Assessment Focus Areas
- Transaction Security Policies
- Code Scan for Vulnerabilities
- Integration with Other Systems
- Protection of Data outside Salesforce
- Development Governance
- Separation of Duties for Admins and Developers
- Sandbox Configuration
- Sandbox Access
- Mobile Configuration
- Mobile Access
- Business Continuity Plans

Transaction Security Policies

- Assess the current policies to see if they meet best practice.

Code Scan for Vulnerabilities

- Use static code scanning tools to assess the quality and security of the Apex code in the org.

Integration with Other Systems

- Verify which external systems are integrated with Salesforce and assess the security of the data being accessed and its lifecycle.

Protection of Data outside Salesforce

- Assess the security applied to data when it is outside Salesforce. This could be in-house data lakes or external companies accessing via API. Protecting the data within Salesforce is key, however the data should also be appropriately protected when it is outside Salesforce.

Development Governance

- Assess the current development lifecycle and tools used for development to understand how production data is protected in Sandboxes. Also assess the capabilities of the development tools when it comes to securing the Salesforce Metadata.

Separation of Duties for Admins and Developers

- Assess how the Administrators and Developers interact with the systems and provide commentary on the separation of duties when it comes to data in production and the deploying of code into production. Admins should not be developers and developers should not be admins.

Sandbox Configuration

- Provide commentary on the current usage of Sandboxes. This will cover the age and freshness of the current sandboxes and best practices around managing these assets.

Sandbox Access

- Assess who has access to which Sandboxes and provide best practice guidance on minimising access to these environments.

Mobile Configuration and Access

- Who has access to run Salesforce Mobile and assess the security of the settings.

Business Continuity Plans

- Assess the company's Business Continuity Plans to understand how and where Salesforce's service is considered and provide commentary on best practices.

Platinum7™
PO Box 6143
Hawthorn West 3122
Australia
Phone: +61 404 005 435
Email: info@platinum7.com.au
Web: https://www.platinum7.com.au

Sample finding from the assessment

Powerful profiles used for API integrations

Severity: CRITICAL

Description:

All integrations use a user account to authenticate with Salesforce. This account provides the authorisation for data access and application permissions within Salesforce. Allowing highly privileged accounts access to the system via the API is very high risk for data exfiltration and/or corruption.

Details:

It was observed during the assessment, that there were multiple applications using user accounts that have System Administrator privileges. Also, System Administrator user accounts were used for application integration as well as regular UI logins.

Please see the *Login History.xlsx* file for more information.

- xxxxxxx has System Administrator permissions and is used by the *AAAAA*, *BBBBB* and *CCCCC* applications.
- xxxxxxx has System Administrator permissions and is used by the *DDDDD* and *EEEEE* applications and also is a regular UI user.
- xxxxxxx has the YYYYY profile (which has wide access to data), and this is being used for an unknown SOAP based integration and is also a regular UI user.

Business Risk:

Allowing access for multiple applications via one user means that any data that is updated by that application will not be discernible from the other applications. The applications that connect via users with System Administrator permissions gain excessive access and are an extremely high-risk threat vector for supply chain attacks. Having an integration use the same user account as a human user means that you are also unable to discern which did any changes to data.

Technical Risk:

Any application that connects through a System Administrator account can deactivate all other users, exfiltrate and/or corrupt and/or delete all data in the system.

Remediation:

- The recently introduced Salesforce Integration User licence is a perfect candidate for the majority of integrations as it is lower cost than a standard user, at present, the cost is approximately US$120/year for each additional licence. CLIENTNAME have five of these licences already allocated to the Salesforce org and none have been utilised.
- Use a single account for each integration and limit the access and permissions required to the bare minimum following least privilege principles. When using the Salesforce Integration User licence, assign the *Salesforce API Integration* Permission Set Licence to the user and then a permission set with just the appropriate objects and fields (read only by default and probably View All for the objects to bypass sharing rules). Please make sure you follow the information in the Spring '24 Release notes regarding the appropriate profile for the Integration User. The profile should be *Minimum Access - API Only Integrations*.
- All API users should have the *API Only* permission enabled in their permission set. This prevents UI logins with the credentials provided.

Additional information regarding the new licence is available at:

https://admin.salesforce.com/blog/2023/best-practices-for-configuring-your-integration-user

Platinum7™
PO Box 6143
Hawthorn West 3122
Australia
Phone: +61 404 005 435
Email: info@platinum7.com.au
Web: https://www.platinum7.com.au