# Platinum7 Service Offerings

May 2024

# Security Assessment

## Description

Get a good understanding of where your Salesforce org stands in relation to security. This is especially important if you have Salesforce Digital Experiences/Communities or Sites as these are often misconfigured and provide an easy way for an attacker to cause a data breach.

## Why?

Understanding the security implications of the set up of your Salesforce org allows you to decide if it complies with your company standards, compliance requirements and also your cyber insurance prerequisites. Keeping your data safe is imperative since it is where the majority of Salesforce customer's IP lives. Please see https://links.platinum7.com.au/assessments for information on what the assessments cover and an example finding.

## When?

Assessments are best done when the application is in use. Doing an assessment of an org while it is getting built does not provide value. Assessments should be done regularly between once and four times a year depending on change. For multiple assessments per year, see Security as a Service.

## Output

A detailed report listing all the findings with recommendations for remediation will be provided along with the data used to come to these conclusions.

## Details

There is a 90 minute kick-off meeting where a System Administrator account is created for the consultant and some required apps are installed. After this meeting, the consultant will spend the next week gathering information and writing the report. A second 90 minute meeting will be held to read back the findings and present the recommendations. It is expected that follow up meetings will be required for questions that arise after getting the report.

## Timeframe

The assessment will take one week to complete.

# Security as a Service

## Description

Get multiple, regular security assessments over a year as well as a number of days per quarter for anything you require in regards to security.  Also included is a backup service for your Event Monitoring logs.

## Why?

Regular assessments are required to make sure that you are aware of any changes to the org's security stance due to updates to the org.  Have you decided to launch a new community, or launch Service Cloud.  After these changes, you should confirm that the changes did not negatively impact your security stance.  Also you can confirm that the remediations undertaken after the first assessment are achieving their target.

Getting access for ad-hoc consultancy on an hourly basis allows you to not to worry about who can answer your security questions or provide guidance.

## When?

Assessments are best done when the application is in use.  Doing an assessment of an org while it is getting built does not provide value.  Assessments should be done regularly between once and four time a year.

## Output

A detailed report listing all the findings with recommendations for remediation will be provided along with the data used to come to these conclusions.

## Details

Please see the Security Assessment offering for more information on what an assessment entails.

## Timeframe

Each assessment will take one week to complete and they are pre planned so as to spread them appropriately across the year.

# Security Guidance

## Description

When embarking on a new module build or setting up a new Salesforce feature like Salesforce Digital Experiences/Communities, get guidance from a Best in Class Security Expert to ensure the development team uses Best Practices during the build process.

## Why?

It is much easier to correct issues when they are caught in the early stages of a build.  Deploying an insecure Digital Experience could result in a data breach.

## When?

This offering is best done as part of the initial design and throughout the build process.

## Output

You'll receive documented recommendations for your development team.  Workshop-style guidance can also be provided.

## Details

This is a general consultancy engagement where the engagement is estimated and then performed on a time and material basis.

## Timeframe

Typically this is a 2-4 day engagement where time is drawn down in two hour blocks.

# Platform Encryption Implementation

## Description

Your company purchased Salesforce Platform Encryption. Now what? This engagement assist you in understanding the encryption capabilities and possible issues to allow you to make an informed decision as to what you need to encrypt and how to manage the environment moving forward.

## Why?

Platform Encryption is the only tool that Salesforce sells that will cause issues with the current deployment of Salesforce. The strong encryption capabilities will affect code, API access, reporting as well as list view functionality. Other issues may also come to bear depending on the products used in your environment.

## When?

If you are thinking about getting Platform Encryption or already have it and want to make use of it, then this is a great time to engage.

## Output

This engagement is run as a workshop consultancy and can also give written guidance as well, if required.

## Details

This is more of a general consultancy engagement where the engagement is estimated and then done on a time and material basis.

## Timeframe

A free 30 minute general guidance call before purchase is available. For an implementation, this would be around a 2-10 day engagement where time is drawn down in two hour blocks.

# Transaction Security Policies

## Description

Your company purchased Salesforce Event Monitoring. Now what? This engagement will assist you in understanding how you can leverage the most powerful Salesforce security tool – Event Monitoring with Transaction Security Policies.

## Why?

Transaction Security Policies will enable you to block users from doing things that you do not want them to do even though you have given them access to the data to do their job. A simple example is blocking the export of more than 100 contacts. A more detailed example is the ability to block the export of any reports that have a field that is flagged as containing personally identifying information. This policy can have overrides for certain groups of users to allow them to "break the rules" a number of times or for a period of time. The more complex policies are what are included in this package.

## When?

As soon as you buy Event Monitoring so you can get immediate value from it.

## Output

There is no output as such from this engagement.

## Details

The policies are deployed as managed packages with a perpetual licence and ongoing support.

## Timeframe

A free 30 minute general guidance call after you purchase Event Monitoring is available which will give the basics for setting up Event Monitoring and discussing policies and how they can stop data loss.

# Event Monitoring Backup

## Description

Your company purchased Salesforce Event Monitoring. Now what? This tool will provide the capability for you can keep all the log files forever using a robust backup capability. There are other tools being planned to use this backup – the ability to see who has seen a certain record during a certain period or what records has a certain user seen during a certain period. Seeing a record means that it was shown in a list view, was edited, was seen by going to it from a link, was seen in a report preview, was exported in a report or was accessed via the API.

## Why?

The ability for you to have a click-by-click path of the journey taken by each user – internal, external (community or guest user), and API users and to keep this forever means you can have a forensic history of what has happened inside your Salesforce environment at any time. These logs vanish after a period of time though, so backing up is essential.

## When?

As soon as you buy Event Monitoring there are things that need to be done to get the best out of the tool.

## Output

There is no output as such from this engagement.

## Details

The backup tool is provided with a perpetual licence and ongoing support. It runs on Windows and Linux and can be scheduled. It also uses the most secure authentication protocol for API based tools – JWT OAuth tokens.

## Timeframe

A free 30 minute general guidance call after the purchase of Event Monitoring is available which will give the basics for setting up Event Monitoring.

# How to get in touch


Email: doug@platinum7.com.au

Mobile: +61 404 005 435

Web: https://www.platinum7.com.au

Blogs: https://doug-merrett.medium.com/