Musa Jallow

Creating secure integrations

Case of Salesforce integrations

University of Jyväskylä

Faculty of Information Technology

ABSTRACT

Jallow, Musa

Creating secure integrations: Case of Salesforce integrations
Jyväskylä: University of Jyväskylä, 2022, 109 p.
Cybersecurity, Master’s Thesis
Supervisor: Frantti, Tapio

Organisation's demand for digital transformation is increasing. These days organisations are seeking ways to centralise their systems and operations. The need for cloud-based Customer Relationship Management (CRM) systems is, without a doubt increasing. These cloud-based systems offer many benefits like security by design and cost efficiency. Salesforce is the world's leading CRM platform, and it offers a high level of security and a large variety of functionalities to extend security even further. However, integrations between Salesforce and third-party software create vulnerabilities that organisations and developers creating integrations need to consider.

Organisations need to implement integration security into their information security policy (ISP) and obligate those creating integrations to follow security standards and best practices. Increasing security knowledge and resources will help transition towards more secure integrations.

This research finds out whether organisations and developers are considering security while creating integrations. The research includes a case study where organisations and developers were asked about their integration security expertise and where they think the responsibility of secure integrations lies. The research aimed to provide security best practices for integration creation and insight into sharing responsibilities between different stakeholders.

Research showed that the size of the organisation and the developer's information technology experience correlate with their security knowledge. However, results also show that organisations and developers do not focus on integration security as much as needed. This research recognised a need for further research due to the significant lack of research on the topic.

Keywords: Cyber security, vulnerabilities, integrations, integration security, secure development, security responsibilities, Salesforce, cloud security

FIGURES

TABLES

Table of Contents

1 Introduction

Digital transformation is one of the key aspects to providing success to modern organisations. Connecting different platforms such as social media, cloud technologies, and data analytics is something organisations are trying to achieve. These days all organisations are facing the need for digitalisation of existing and new business models to stay competitive (Rot & Sobinska (2020, 555-557). Different Cloud-based solutions and platforms are often the solutions organisations are seeking. Digitalisation provides optimization, better data management, and a better customer experience. Mydyti, Ajdari and Zenuni (2020, 1390), Rot and Sobinska (2020, 555-556), and Coltman (2006, 1-7) all highlight that digitalisation is one of the key features for organisations to reach higher business impact, to stay competitive and provide customers experience customers are demanding.

Customer Relationship Management (CRM) has an ever-growing role in the modern business world. CRM provides a modern framework for a better customer experience. It also helps organisations to include customer perspectives better into their business model. (Coltman 2006, 1-7). Alongside CRM, Knowledge management comes up when considering the key success factors of modern organisations (Rot & Sobinska 2020, 555-556). Knowledge management needs digital technologies to be effective and to provide good results (Rot & Sobinska 2020, 555-556). When using CRM organisations can get 360 view of their business. When conducting all the customer and business-related data under one platform, the data is more achievable and, therefore, easier to use. (Coltman 2006, 1-7; Rot & Sobinska 2020, 555-556).

One such CRM platform is Salesforce. Salesforce is one of the world's leading cloud-based CRMs that provides cloud services and application development. It provides different platforms, such as the world's first Platform as A Service (PaaS). A significant benefit of Salesforce is that it is cloud-based, provides demand service, offers in-built facilities, allows you to access it from anywhere and anytime, is cost efficient to use and maintain, and is secure. Salesforce is seen to provide one of the best CRM systems for any size of organisation to use. (Patel & Chouhan 2016, 1-8; Manohar & Chouhan 2017, 1-4).

Even though Salesforce can tackle most of the organisation's needs, there is also a need for other systems, applications, and services for organisations to use (Seth 2018, 7). Patel and Chouhan (2017, 1-6) bring up the need for integrations from Salesforce to third parties to use collected information Salesforce has. For this purpose, Salesforce provides a comprehensive application programming interface (API) to create integrations between Salesforce and other systems, services, or applications. A problem in this kind of integration relies on the validation of third-party software.

What happens if integration between Salesforce and third-party software is made, but third-party software is breached? Who is in charge of ensuring this type of situation cannot happen? Soni and Vala (2017, 1-4) state that application providers are responsible for application security. This kind of thinking can be seen as "normal" or a common way of shifting responsibility for security to the third party. On the other hand, Seify (2006, 440-445) brings up that data security level and security policy depends on the security policy of the organisation. Every organisation using CRM should have some sort of CRM risk management (Seify 2006, 440-445). However, sometimes an organisation does not have enough security knowledge and trusts that CRM is secure itself, so there is no need to validate the third parties, and/or they shift security to those in charge of developing their CRM. My hypothesis is that organisations are relying on and shifting security management to the developers and third-party application providers, and developers are shifting security management to the organisation and third-party application providers. Therefore, there might be a significant problem if a third-party operator has bad intentions or is not following security standards and precautions. So, the question arises, can we rely only on third-party operators in matters of security? Should we look beyond that and shift more responsibility to those who are creating integrations or demanding them?

Understanding how to create as secure as possible integrations between different systems is essential. The need for security arises mainly when the system has a large amount of sensitive data of customers and businesses. In the modern world, where systems and data are becoming a standard for doing and managing organisations at all sectors and levels, we need to find proper precautions, methods, and standards to move data from one system to another. This research will focus on Salesforce, but all the aspects of this research can also be used in other data-centralised digital platforms that are integrated with other systems, applications, and services.

2 Research

The research aims to study how security is considered in software development and include the author's expertise with the Salesforce platform. This research focuses on integration security because the scope of secure software development is too broad. Other than that, we can only make assumptions about Salesforce security by looking into the general security architecture of cloud-based platforms and thereby believe that Salesforce is pretty secure by itself. That's why this research focuses only on Salesforce integrations.

Although the research is done in the Salesforce context, the research and findings can be generalised to any integration security development.

2.1 Research background

The research aims to show how security responsibilities are split between stakeholders regarding Salesforce integrations. Integration's role for organisations is an essential part of modern information technology infrastructures. Organisations are often forced to use outsourced developers due to the high demand for developers or the cost-efficiency it can provide.

Another challenge organisations are facing is the ever-growing demand for security. We have seen an increase in cyber-attacks, and there are new attack vectors for professionals to cover every day. Integrations are not different. How do we ensure the security of integrations? What actions are needed from organisations, and what from developers? What is the third-party software provider's responsibility to create safe applications to integrate? These all are questions that organisations need to have answers to. For example, if the organisation's customer data is leaked, in the eyes of the customer's organisation is the one to blame.

The importance of this research comes from the lack of literature on integration security. For example, there can be found publications on security aspects and related to integrations, but not publications that cover them both in the same context. This creates a need for further research to give tools for organisations and developers to ensure the security of integrations.

Another thing is that because Salesforce is seen as secure itself, Salesforce developers and organisations might be relying on Salesforce for integration security. Salesforce indeed provides a different set of capabilities to ensure information security also in integrations. However, many attack vectors and vulnerabilities still need to be taken care of.

This type of research faces a problem where organisations might not be willing to respond to the survey; therefore, the sample of data can become too small to draw assumptions on a larger scale. The research can be seen more like a case study highlighting findings from some organisations using Salesforce. Also, the lack of literature and lack of research creates a challenge for the research.

2.2 Research questions and goal

This research aims to answer to the following questions:

- Is there mismatch between organisations and developers on where they see that responsibility lies on?
- How does Salesforce developers' experience affect their ability to take responsibility for integration security?
- How do an organisation's size and resources in use affect its ability to take responsibility for integration security?

The main hypothesis is that Salesforce developers think the main responsibility lies on organisations, and organisations think the main responsibility lies on Salesforce developers or partners. This research hypothesises that larger organisations think differently than smaller ones. At large organisation's main responsibility lies on the organisation and their security professionals, such as CIO and CISO.

The research tries to find correlations between organisations' size and security knowledge. Salesforce survey for developers aims to find correlations between experience in years and security knowledge. Findings from the developer and organisation surveys are then examined to determine whether there is a mismatch between responsibilities. *Salesforce survey for Mulesoft developers* mainly highlights good practices integration frameworks can offer.

The main goal of this research is to highlight best practices for the organisations and for the Salesforce developers to cover the security aspect of integrations better. The research literature will highlight how a secure development lifecycle can provide steps to ensure security in integration creation. With the findings in the literature, the goal is to show the responsibility of different stakeholders in the different parts of the development process.

2.3 Research methods and structure of the research

The research is split into a literature review and a case study. In the literature review, the research aims to provide a common understanding of why the demand for integrations and, therefore, demand for security is increasing. The literature review will also cover different parts of Salesforce security and how Salesforce and cloud-based platforms create security. The second part of the research is an empirical case study. The empirical case study contains three analyses of three different surveys with different focus groups. These focus groups are Salesforce developers, organisations, and Mulesoft developers. In addition, surveys for Salesforce developers and organisations are the primary source of data to be analysed. Finally, a survey for Mulesoft developers provides more insight into one of the world's leading integration platforms and the security implications we can learn from them.

The case study is created for this research because it looks into the phenomenon within its real-life context (Bass, Beecham & Noll 2018, p. 13-20). In this research, it means that the phenomenon this research investigates is integration security, and the real-life context is how integration security is ensured in Salesforce integrations. This research can be seen as using both embedded and holistic approaches. Organisations are examined with an embedded approach because research explores different organisations using Salesforce. Salesforce developers and Mulesoft developers can be examined with a holistic approach. This can be seen in a way that each developer works with Salesforce and creates integrations in a Salesforce context. The only way differencing developers is their background and how they are creating integrations. An empirical case study works well for this research because it typically uses surveys to describe and explain the phenomenon. Typically, these surveys are conducted quantitatively or numerically. This research uses mainly numerical questions to make responding to the survey as fast as possible. Results are then described in a quantitative research manner. Although it is essential to point out that this study can be called more "context specific", it speaks more directly to industry needs rather than uses formal methods. (Bass, Beecham & Noll 2018, p. 13-20). Bass, Beecham and Noll (2018, p. 13-20) bring up that, like in this research, a small sample of the organisations and developers can create biased results. With a small sample, it is also hard to generalise findings, so the descriptive approach is justified.

As a base of this research is the literature. Digitalisation and especially cloud-based digital systems, including Salesforce, are reviewed in chapter 3. Chapter 4 goes through integrations, security of integrations, features on Salesforce integrations, and brings out the core of Mulesoft. In chapters 5 and 6, all the surveys are analysed. Chapter 5 goes through findings from *Salesforce survey for organisations* and chapter 6 *Salesforce survey for developers* and *Salesforce survey for Mulesoft developers*. Chapter 7 cross-examines survey results and underlines findings.

2.4 Implementation of the study

As mentioned, this study contains three surveys. *Surveys are Salesforce survey for developers*, *Salesforce survey for organisations*, and *Salesforce survey for Mulesoft developers*. All surveys were created with Google Forms, and forms were stored in Google Drive. For the purposes of this research Google account provided by the University of Jyväskylä was used. Google Forms was selected because it offers all the needed capabilities, has a great overall look, is easy to manage and share, and provides good functionalities to form raw data into the excel format. Researcher was also familiar with Google Forms and Google Drive, which was an excellent fit for this purpose.

A survey was structured in a way that was fast and easy to answer. All background questions were multiple choice questions. Integration and security questions were primarily using rating scale questions, except in *Salesforce survey for organisations* there were also some open-ended questions. Responsibility question was made using matrix and best practice question with multiple choice. Multiple choice questions had scale from 1 to 6 where *1 = Strongly disagree, 2 = Disagree, 3 = Some what disagree, 4 = Some what agree, 5 = Agree, and 6 = Strongly agree*.

An idea for survey creation was to get three types of information; background information, integration and security knowledge and practices, and a view of how responsibilities should be distributed. The question about responsibility distribution and best practices is the same in all surveys. The question about responsibilities goes as follows: "*When creating integrations, there are different stakeholders involved in the process. Rate each stakeholder's role when making integration secure. (1 = Main responsibility, 2 = Some responsibility, 3 = Little responsibility, 4 = No responsibility)*". Question about best practices forces respondents to choose the three most valuable ways to ensure Information Security when creating integrations. These options are:

- Using solutions found from AppExchange
- Creating own set of validations
- Creating support ticket to Salesforce
- Asking about the security from a third-party software provider
- Auditing security of third-party software
- Extensive testing
- Searching best practices
- Encourage organisations using Salesforce to take care of it
- Monitoring integrations
- Option to describe other than any of the following

Salesforce survey for developers consist of following categories and questions:

- **Background questions**: Type of employer, Job title, Salesforce experience, Information technology experience, amount of integrations within Salesforce and outside of Salesforce context person has created and what percentage of Salesforce-related integrations have been made using integration platform, such as Mulesoft.
- **Integration and security questions**: Importance of integrations, integration security in Salesforce, knowledge about integration security threats, and how to ensure security of integrations.

Salesforce survey for organisations consist of following categories and questions:

- **Background questions**: Size of organisation, Salesforce experience in years, and amount of Salesforce users and in-house developers.
- **Integration and security questions** were divided into three categories; ISP, information security responsibilities in the organisation and integration security. ISP questions were as follows; the existence of ISP and how integration security is mentioned. Question-related to information security responsible in the organisation was split into two questions; Is there such personnel, and what is that individual's role in ensuring the security of integrations? The last three questions in this section related to integration security were about whether organisations do integrations in-house, using partners, or both, best practices used to ensure integration security, and how the organisation ensures that partners follow security precautions while creating integrations.

Salesforce survey for Mulesoft developers consists of similar questions to *Salesforce survey for developers*, with the difference that questions were related to the Mulesoft context rather than the Salesforce integration context. In the end, there was also one extra question: were Mulesoft developers had a chance to describe the benefits Mulesoft provides related to information security.

All three surveys had their target groups. *Salesforce survey for developers* targeted the individuals that have created at least one integration between Salesforce and third-party software. *Salesforce survey for organisations* target group were organisations that use Salesforce and have at

least one integration between their Salesforce and third-party software. The survey mentioned that the best fit to respond is someone familiar with the organisation's ISP and integrations in their Salesforce instance. If no such person is established in the organisation it was made clear that responding to the survey could also be a joint effort. Both of these surveys were promoted together and by themself depending on the target group.

First, I contacted by phone and email all the biggest Salesforce Partners in Finland. Those organisations contain hundreds or even thousands of Salesforce developers and have strong relationships with most of the organisations using Salesforce in Finland. I also emailed organisations using Salesforce directly. Both surveys were also promoted at the various Salesforce community groups on different social media platforms. Finally, all the surveys were open for one month to respond. Remainders to respond were made halfway through the response time and a week before the due date.

For the *Salesforce survey for Mulesoft developers*, I contacted Mulesoft Helsinki Meetup's co-leader. With his help, I got all the responses to the survey targeted to the Mulesoft developers.

3 Digitalisation

Digitalization is a term that does not have an explicit definition. Technology is an enabler of digitalization. However, digitalization can be seen as a desire to export processes and physical or non-physical assets into the digital space. Ilmarinen and Koskela (2015, p.17-22) state that digitalization is far more than online services and exporting analog assets into the digital space. Digitalization is a way to reform the way of working and thinking. It affects differently on different levels. At the societal level, it affects social structures and how people behave. On a market level, it affects overall logic and how markets work. Organisation-level digitalization is seen to affect business models. (Ilmarinen & Koskela 2015, p. 17-26). Lakaniemi (2014, p. 3-4) emphasises this statement by saying that digitalisation is not the only amount or increase of ICT technologies (Information and Communications Technology) organisations use. However, more than that, it extends and evolves organisations way of doing business, managing assets, and generating competitiveness and innovation ability. Digitalization can be seen to emphasise depth, scope, and effects in all aspects of organisations and ways of doing business (Lakaniemi 2014, p. 3-4). One could say that because digitalization is a holistic phenomenon, it changes industries as a whole, and more than that, it changes the way we see the market economy. Because digitalization creates significant value, organisations are becoming keener each day to transfer their way of thinking and doing business more into the digital space.

One key factor for organisations to have successful digital transformation is to get all different stakeholders included. Lakaniemi (2014, p. 24-25) states that organisations management needs to have basic knowledge about digitalisation and its benefits, and they need to have a desire to promote digitalization. Ilmarinen and Koskela (2015, p.25-27) also bring up the role of management to see digitalisation as a tool to improve business. One way to emphasise the business impact and value digitalization can bring is that it adds cost efficiency and quality, customer management and engagement, and better processes for the organisations, to name a few (Ilmarinen and Koskela (2015, p.24-26).

Technology is a crucial enabler of digitalization. Each day technology is taking significant leaps forward, which enables even better and more attractive ways to digitise organisations. In modern society, technology is getting cheaper, more flexible, and better accessible daily because rapidly advancing technological development markets and organisation's way of working need to follow ever-increasing customer demand. Many organisations are innovating new ways to use digital solutions to fill those customer needs, challenging traditional organisations and approaches. (Ilmarinen & Koskela 2015, p. 41-46). One fashion term is multi-channel. Multi-channel means that

an organisation has multiple channels to engage with the customers. Multi-channel came from the idea that, because customers are using multiple platforms and channels daily, organisations are expected to be accessible in different channels as well. (Ilmarinen & Koskela 2015, p. 74-80). In section 3.3 we will dive more in-depth into the multi-channel approach, its challenges, and its benefits. Also, we will bring up a one-platform approach where a single platform can be seen to tackle all the different needs of a multi-channel approach.

Information gathering and documentation are one of the benefits of digitalization. With digitalisation, organisations can transform information that is used to record in paper form into the digital space. This is both cost and time efficient and enables better and faster data processing. When information is saved in the digital space, it is more accessible. Organisations can get a better overall view and filtering by processing this information fast and with complex logic. (Ilmarinen & Koskela 2015, p. 83-122). Digitalization changes the way of leading. A key concept in modern leadership is knowledge management. Rot and Sobinska (2020, p.555-557) define knowledge management as processing information and intellectual assets to generate value for the customers and employees. This way, leaders of the organisations can have data-driven metrics to emphasise their message. In order to get total value from data to the organisation's decision-making and management organisations need to have a high amount of information, both internal and external information. Rot and Sobinska (2020, p.555-557) state that organizations have more information at their disposal today than ever. In knowledge management, an immense amount of information will lead to better processes and metrics, leading to better decision-making and management. It is also important to note that to have full access to the benefits of knowledge management. There is often a need to improve and reform business models and logic to work better with digitalization (Rot & Sobinska 2020, p.555-557).

When organisations are transforming into this new era of digitalization and conducting vast amounts of information into their digital systems, there is also a growing need to understand security. Security can be seen as a standard or essential requirement and should be taken care of at any cost (Ilmarinen & Koskela 2015, p. 155-159). Rot and Sobinska (2020, p.555-557) bring up that while digitalization is taking significant leaps forward, it is causing a rapid increase in cybercrimes. These cybercrimes create a substantial threat for organisations because the organisation's information, assets, and processes are even wider managed and stored in the digital space. Cybercrimes are estimated to create billions of dollars in business costs yearly.

On top of that, there can be significant impacts to the organisation’s reputation and, therefore even greater loss of gains. (Ilmarinen & Koskela 2015, p. 155-159). Protecting data and assets is a

significant concern in modern information security management, and it is becoming increasingly crucial while organisations are taking leaps towards digitalization.

3.1 Customer relationship management

Due to digitalisation, Customer behaviour is changing rapidly. A significant player in this change has been social media. When individuals spend more time on social media and the internet, their expectations for the services and goods they consume change. Organisations must participate in this development and move towards digital and customer-centric solutions. If one organisation is not working in line with customer's standards, the internet makes it easy to find organisations. These competitors can come from anywhere in the world; therefore, because of digitalisation, organisation's need to start seeing all similar organisations as their potential competitors. (Lakaniemi 2014, p. 35-36).

Customer Relationship Management (CRM) often comes up when discussing modern organisation digital transformation. Coltman (2006, 1-8) sees CRM as a platform that is an embedded strategic tool. CRM brings all the modern aspects of the customer-, operational- and data management into the use of organisation. In the past, CRM focused more on using technologies and software to enable a good customer experience and relationship with the customers. These days CRM is seen to be more about the experience, which means utilising engagement with the customers to provide the most value. This can mean engaging existing and new customers or creating interactive and fun customer experiences. Creating a forever-lasting partnership with each customer is something organisations are aiming to achieve. (Williams 2014, p. 1-10).

Williams (2014, p. 62-69) states that having a solid customer strategy is a significant part of developing a CRM framework. Because CRM is more than a technical tool or platform, organisations need a comprehensive strategy on how and to what extent they will implement customer relationship management into their organisation. Customer strategy includes customer portfolio management, segmentation, and segment strategy. Customer portfolio management quantifies the value customers bring to the organisation, the scale of investments to each customer, and steps to achieve set goals. Segmentation means understanding customers, their needs, and expectations for the organization's goods and services. Segment strategy, therefore, means how the organisation executes accordingly aspects that were brought into the light. (Williams 2014, p. 71-75).

Customer Relationship Management (CRM) is something organisations that want to be relevant need to take care of. CRM provides necessary data and metrics for the decision makers to

refine business models and get a higher business impact for their business decisions (Coltman 2006, p. 1-8). In this research, we are looking into one of the leading CRM platforms in the world, Salesforce.

3.2 Cloud Computing

Computers have been evolving rapidly in a short time. We see computers as hardware that does all the calculations and functionalities for us to use. Since those early days, organisations and service providers have figured out that maintaining computer infrastructure is hard, especially in larger organisations. In-house solutions and on-premise software are seen as high costs and complex to maintain, use and set up because you need data centers, hardware, and software to set up proper infrastructure. For that problem, cloud computing is the answer. Cloud computing provides different services (as a service, aaS) such as infrastructure (IaaS), Platform (PaaS), and Software (SaaS). (Arora & Gupta 2013, p. 9-13; Rittinghouse & Ransome 2009, p. 1-24). Arora and Gupta (2013, p. 10) define Cloud computing as follows: "Cloud computing is the delivery of computing as a service rather than a product, whereby shared resources, software, and information are provided to computers and other devices as a utility (like the electricity grid) over a network (typically the Internet)." Gupta, Verma, and Kavita (2018, p. 23) continue the definition by stating that Cloud computing is a set of assets that can be accessed through the internet and offer different utilities for the customers. Different sources define Cloud computing a bit differently. Overall, Cloud computing means servers that can be accessed through the internet and run different software and databases.

Cloud computing has different characteristics: massive scale, homogeneity, virtualization, geographic distribution, advanced security, low-cost software, and service orientation (Gupta, Verma & Kavita 2018, p.23). Cloud computing has many standards, including application-, data-, solutions-, messaging- and communication standards. There are also different security standards set for Cloud computing, for example SAML (Security Assertion Markup Language), OAuth (Open Authentication), OpenID (usage of existing account to sign in), and SSL (Secure Sockets Layer)/TLS (Transport Layer Security). (Rittinghouse & Ransome 2009, p. 222-251). All the best practices and standards for Cloud computing have created it to be an efficient and secure way for the organisations to get infrastructure and services to use.

All the aspects brought up in Cloud computing are modern, cost-efficient, easy to use and manage and guarantee good performance for the organisations. Different service providers have started to use Cloud-based solutions in order to provide better services to their customers. Mydyti,

Ajdari, and Zenumi (2020, p.1390-1395) highlight Cloud computing's capabilities to boost organisations digitization and digital transformation. Cloud-based solutions are bringing better performance and faster deployment, lowering costs and adding customer and employee satisfaction. Cloud-based solutions are also often easier to scale, and many service providers offer ready-to-use solutions for their customers. Due to Cloud computing's nature to be easy to use and scalable, any organisation, from big to small, could benefit revolutionary solutions Cloud computing offers.

In this research, we look more in-depth at one Cloud computing platform called Salesforce. We dive more in-depth into Salesforce and its functionalities in the upcoming sections. However, for now, it is essential to understand the basis of Cloud computing and its main benefits. This helps to understand why Salesforce, for example, has been created to be a cloud-based platform with all its performance, accessibility, and security benefits.

3.2.1 Cloud Service Models

Today organisations are relying more on Cloud Computing and the services Cloud Computing provides. This has shifted from the traditional on-premises to the new cloud service model. Cloud service models offer scalability, cost efficiency, and pre-created infrastructures and applications for use by organisations. This all can be achieved much faster than traditionally by using on-premises models. Therefore, organisations are seeing the value Cloud service models offer and are learning to use services that have some of the cloud service models implemented to the services that have implemented all of them and the functionalities they offer. (Singh, Sharma, Kumar & Yadav 2016, p. 173-174; Gupta, Verma & Kavita 2018, p. 28-29; Rittinghouse & Ransome 2009, p. 34-36).

Due to the high demand, Cloud Computing offers different service models for different target groups and business needs. Whether you are an end user, director of the organisation, or developer Cloud Computing has something to offer. Like brought up earlier Cloud Computing have three types of service models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). (Gupta, Verma & Kavita 2018, p. 28-29). Next up, we take a look more in-depth at those three.

Gupta, Verma, and Kavita (2018, p. 28-29) describe Software as a Service (SaaS) in the following way: its way of providing applications over the internet. "Software as a service (or SaaS) is a way of delivering applications over the Internet as a service." There are three different characteristics of SaaS. Firstly, SaaS is not flexible when it comes to customisations. In SaaS, only the service provider can customise applications for the end-user. SaaS can also be described as "on-

demand self-service, " meaning that the end-user needs to give minimal effort to manage applications. The last characteristic of SaaS is that it is usually accessible from anywhere and with any device. (Singh, Sharma, Kumar & Yadav 2016, p. 173; Arora and Gupta 2013, p. 12-13).

Organisations use SaaS mainly because it offers a high level of automation and therefore eases the end-users use of applications. This is also disadvantageous in that if there is demand from the organisation to customise their SaaS further, this can be hard or impossible to achieve. Another advantage of SaaS is that it is extremely scalable and cost-efficient, making it a good solution for larger organisations. However, it is important to note that the organization needs an existing SaaS solution to use. Salesforce is ranked as the world's best CRM as SaaS. (Singh, Sharma, Kumar & Yadav 2016, p. 173-174; Gupta, Verma & Kavita 2018, p. 28-29; Manohar & Chouhan 2017).

Platform as a Service (PaaS) was created to eliminate the need for the end-user to have a particular operating system or version. The PaaS operating system is installed on the server, so the end-user needs only to log in to the server to access the application or service. PaaS works between IaaS and SaaS, hiding all the complexity of dealing with hardware and software (Arora and Gupta 2013, p. 12). Gupta, Verma, and Kavita (2018, p. 28-29) state that PaaS is a basic computer framework that contains equipment, such as hardware and operating system, and it can include development tools. When PaaS has development tools, creating customisations, systems, and functionalities is much easier. Developers working with PaaS can write code with any computer and at least in some cases with any programming language and then send the code to the centralised server where the server compiles the code. (Singh, Sharma, Kumar & Yadav 2016, p. 174-175; Gupta, Verma & Kavita 2018, p. 28-29). Salesforce's Force.com provides this service and is the world's first PaaS (Manohar & Chouhan 2017).

Infrastructure as a Service (IaaS) provides virtualization and storage in a way you need them, and this is all accessible through the internet because it is stored in the cloud. Arora and Gupta (2013, p. 11) bring up that IaaS usually includes servers, routers, storage, firewalls, computing resources, and other features in physical or virtualized form. IaaS is also scalable, which means buying resources, for example, more storage, is an easy and fast way to implement a more extensive infrastructure within minutes (Arora and Gupta 2013, p. 11; Sharma, Kumar & Yadav 2016, p. 174-175).

IaaS is often used to provide a framework for facilitating the applications and services the organisation has created. IaaS allows organisations to rent different resources such as data center space, servers, software, and network equipment, to name a few. (Rittinghouse & Ransome 2009, p.

34-36; Singh, Sharma, Kumar & Yadav 2016, p. 174-175). This makes it easier to set up an organisation's infrastructure and scale it.

3.2.2 Cloud Computing Security

Security of Cloud Computing comes down to the fact that personal information that is used and stored locally is now stored in the cloud. The main security threats in the cloud are confidentiality, integrity, availability, and privacy. Confidentiality means that information can not be accessed by unauthorized personnel. Completeness, correctness, and consistency of data are features known as integrity. Availability covers that data is achievable and that systems using and storing data are functioning correctly. Privacy can be threatened when there is loss of control, invalid storage, access control, and data boundary. (Barona & Anita 2017).

There are different ways to ensure the security of the cloud, but they come down to algorithms and security patterns to be used. Barona and Anita (2017) bring up nine concepts on how cloud providers should ensure the security of their platforms. Information-centric security is an approach that aims to shield the information. High-assurance remote server attestation means that there are methods to ensure that information is not being abused, spilled, or leaving an unalterable review trail when an incident occurs. Cloud suppliers are currently using the Statement of Auditing Standard (SAS-70). Privacy-enhanced business intelligence covers data encryption. Privacy and data protection state that there need to be embedded privacy-protection mechanisms in all cloud security solutions. Homomorphic encryption provides an encryption schema that allows users to store data in ciphertext format and perform necessary computations without decryption. Searchable/structured encryption ensures that the cloud is unaware of data and computations performed on the data. Proofs of storage is an agreement that the cloud service provider uses data without permission. Server aided secure computation is a mechanism that allows the computation of ciphertext without displaying data. Tools consist of different tools that are often used to add more security. These tools have different tasks such as pattern- and anomaly detection, encrypting authentication, and many others. (Barona & Anita 2017).

There are many standards (ISO/IEC standards on Cloud Computing) that cloud computing suppliers need to follow. These standards are there to ensure that needed actions, mechanisms, and frameworks are in place. Countries also have laws that guide cloud computing to protect personal information. These all, combined with best practices and expectations of an organisation using cloud solutions, are increasing security of Cloud Computing now and in the future.

3.3 Salesforce

On its website, Salesforce describes its platform, and its features as follows: "Salesforce is a company that makes cloud-based software designed to help businesses find more prospects, close more deals, and wow customers with amazing service. Customer 360, our complete suite of products, unites your sales, service, marketing, commerce, and IT teams with a single, shared view of customer information, helping you grow relationships with customers and employees alike." (https://www.salesforce.com).

Salesforce is one of the world's leading platforms for organisations on what comes about digitalisation of business models. While digitalisation and modern business models are growing in popularity among organisations, Salesforce is one of the platforms organisations considering. (Soni & Vala 2017, 1-4). Salesforce's capabilities are enabling successful digitalisation for organisations. When considering all the challenges digitalisation creates, Salesforce is tackling them efficiently. One of the critical features Salesforce has is its one-platform idea. Patel and Chouhan (2016, 1-8) bring up that Salesforce provides many features, which means that with the correct configuration, the Salesforce instance can handle everything that organisations are used to, needing multiple systems and service providers. Salesforce was established in 1999, and since then, it has been growing by acquiring applications and services such as Slack and Desk.com (https://www.salesforce.com/eu/company/our-story/).

Salesforce is a cloud-based service provider that offers a modern Cloud Computing platform to give all the benefits and advantages of Cloud Computing. Salesforce includes various solutions such as the world's leading Customer Relationship Management (CRM) system and marketing capabilities. Salesforce is one of the leading platforms for Cloud Computing based solutions. Salesforce offers all the Cloud service models (SaaS, PaaS, and IaaS) and functionalities such as development tools and security features. Salesforce is seen as the best SaaS in the world and the first PaaS provider. Significant benefits of Salesforce come from those Cloud Computing functionalities utilised. Easy and cheap to set up, no maintenance, no- and low-code functionalities, build-in development tools and APIs, and much more are all key features of Salesforce. (Manohar & Chouhan 2017; Patel & Chouhan 2016).

Customer Relationship Management (CRM) is where Salesforce started by offering an overall view of the customers. CRM provides capabilities to gather information about customers and potential customers. It also helps to track and manage all customer-related aspects the organisation

has in real-time and as a whole. The Salesforce data model makes the information easy to use and manage since Salesforce uses object and record models. (Patel & Chouhan 2016). In Salesforce, objects work like in object-oriented programming (OOP). They have their own identity, which makes them unique. Other characteristics of objects have their properties, such as variables, and their behavior, such as actions and automation. (Loshin 2022). In Salesforce, objects also have their layout, visualisation. On the other hand, records are stored using the corresponding objects framework. Records can also include relations to the other records, either under the same object or different ones.

Salesforce is full of different features and products (Patel & Chouhan 2016, 2-3). Figure 1 highlights the different products Salesforce have. It also has a marketplace called AppExchange (https://appexchange.salesforce.com/) which provides different build-in solutions, better known as packages, to customise organisations Salesforce even further. These pre-build packages are either managed or unmanaged packages. A significant difference between the two is that managed packages are restricted to specific changes. Unmanaged packages can be seen as open-source projects that can be edited without restrictions. (Fawcett 2014, p. 12-22).

Built-in integrations are something organisations are often looking to implement on their own Salesforce instance. Patel and Chouhan (2016, 1-6) state that AppExchange provides many benefits for the organisation, such as cost-efficiency and speed to develop fully working functionalities. All the packages in the AppExchange are reviewed and security checked by Salesforce. Different products Salesforce has are sales, service, marketing, commerce, analytics, and Slack, to name a few (https://www.salesforce.com/products/). Salesforce also provides solutions for most industries (https://www.salesforce.com/solutions/industries/?d=cta-body-promo-89). Because of the Salesforces wide variety of products and services, it is widely used worldwide (Patel & Chouhan 2017, 1-8).

Salesforce's popularity among the organisations makes it more attractive for criminals to abuse and learn to perform cyber crimes against the organisations using Salesforce. Therefore, it is important to highlight different threats and vulnerabilities organisations using Salesforce have. In the future, we will see more cyber crimes committed against organisations using Salesforce. (Violino 23.10.2022).

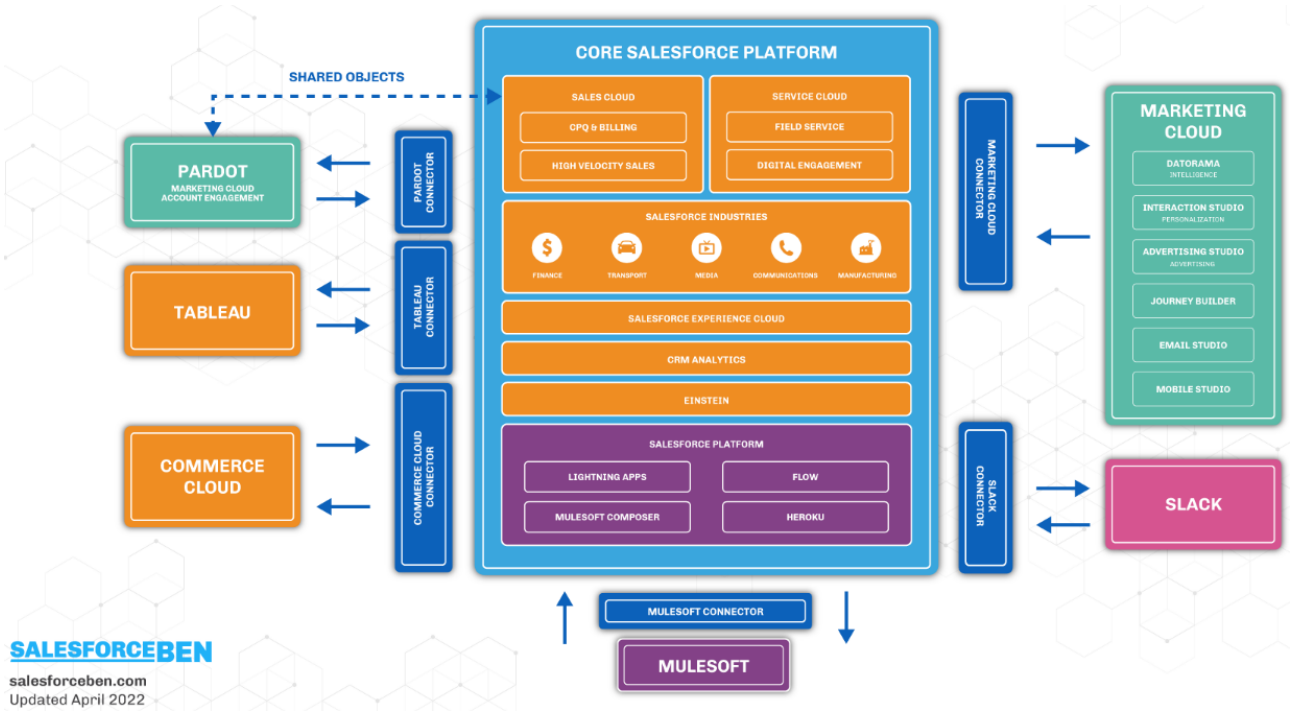

Figure 1: McCarthy, Ben (2022). Salesforce product landscape. Sited 23.10.2022. Source: https://www.salesforceben.com/salesforce-products/

3.3.1 Force.com

Force.com was created for the extension of Salesforce's SaaS capabilities. It was designed to offer more customisation options for the developers to leverage the Salesforce platform and offer more personalised solutions for the organisations. This opened new ways for the platform by enabling the development of enterprise-level applications. (Arora & Gupta 2013, p. 13). It is a product of Salesforce and its Platform as a Service (PaaS) part of the Salesforce ecosystem. It is created for the developers working with corporate applications and independent software vendors. Force.com differentiates from other PaaS by not provisioning CPU time, disk, or instances of running operating systems. However, Force.com works around the relational database, which is familiar with an application server stack. It mainly focuses only on business applications. The purpose of Force.com is that it provides development tools and makes development much simpler and more efficient. Force.com enables the development of websites and applications through a web-based integrated development platform (cloud IDE). (Arora & Gupta 2013, p. 13-16). Arora and Gupta (2013, p. 13) also state that studies show that Force.com compared to the traditional Java-based application development, is five times faster, enabling lower costs and better quality. A major benefit of Force.com is that it follows declarative principles, which make programming more straightforward and faster and raises the quality of applications. (Arora & Gupta 2013, p. 13-16). The major benefits

of declarative programming languages are minimising mutability, reducing state side-effects, and better code quality and scalability (Kashivskyy 2015). Force.com uses Java-based programming language Apex. Apex is the primary programming language for the back-end. SOQL handles database queries and Visualforce, and a newer version of Visualforce called Lightning Web Component (LWC) handles the front-end side of development (Soni & Vala 2017).

Force.com has an application server stack consisting of different technologies and service layers. There are six layers in force.com, which are shown in figure 2: infrastructure as a service, database as a service, integration as a service, logic as a service, user interface as a service, and development as a service. On the scope of this research, we are mainly interested in integration as a service layer. It utilises platform integration capabilities through open-standards-based web services API. Some of the APIs present at Force.com are Bulk API, Chatter API, Metadata API, Apex REST API, Apex SOAP API, Streaming API, and many others. In addition, SOAP and REST applications can be connected to Force.com to access data. Force.com also provides callout capabilities to integrate Salesforce with third-party web services. Integrations between Salesforce can be pre-created packages with existing connectors or fully customised integration interfaces. (Arora & Gupta 2013, p. 13-18).

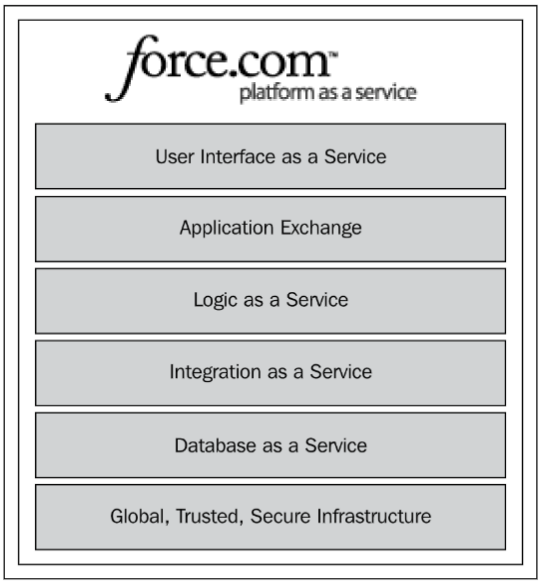

Figure 2: Services Salesforce provide as PaaS (Arora & Gupta 2013, p. 15)

3.3.2 Security

Information security is an essential aspect of Cloud Computing architecture when talking about Cloud Computing. Soni and Vala (2017) bring up that security is established only if the platform provider and application provider commit to information security and create necessary security precautions. The security precaution created by the platform provider contains the design and maintenance of platform security. The platform also needs strict policies protecting customers and their data. Application providers need to create secure applications by properly using platform features and implementing policies that increase the applications' security. (Soni & Vala 2017). Overall, Salesforce is seen as a highly secure platform, but some reports of security breaches have been reported. Hanna Andersson, a clothing brand, faced a significant data breach in 2019 that was exposed to the world (https://www.epiqglobal.com/en-us/resource-center/articles/salesforce-data-breach). Because of the increasing popularity of Cloud Computing and Salesforce, it is anticipated that we will see these kinds of data breaches more in the future.

Salesforce has created a security model to protect different layers and therefore make the platform secure as a whole. Salesforce security model consists of nine different layers described in the figure 3. Those security layers are users, auditing, record level security, object and field level security, authentication, encryption, 24/7 monitoring, and multitenancy (database level partitioning and secure data centers). Some of the layers are completely secured by Salesforce, and some of the layers need actions from the organisations and developers. (Soni & Vala 2017) For example, Salesforce's responsibility is to ensure that actions and security precautions are taken into consideration related to multitenancy (both database level partitioning and secure data centers). Salesforce also audits all apps downloaded into the AppExchange.

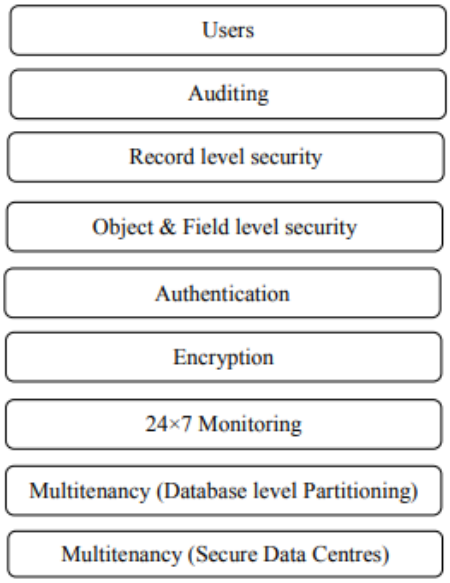

Figure 3: Different platform functionalities to increase security of Salesforce (Arora & Gupta 2013, p. 15)

In Salesforce, auditing means information about the systems. Salesforce provides various auditing features that administration users should enable and use to track possible security threats in their Salesforce instance. These auditing features include the following aspects (https://developer.salesforce.com/docs/atlas.en-us.securityImplGuide.meta/securityImplGuide/security_overview_auditing.htm):

Record information

Usernames and timestamps when a record is changed or created. This is standard and automatically appears on all the records at Salesforce.

Login history

Salesforce provides login history for up to six months. Login history shows authentication method used, HTTP login method, SAML Single Sign-on history, and My domain URL used. Other than those, you will see information about the login time, login type, source IP, login status, location, TLS Protocol, and TLS Cipher suit. (https://developer.salesforce.com/docs/atlas.en-us.securityImplGuide.meta/securityImplGuide/users_login_history.htm).

Field history tracking

Salesforce field history tracking is enabled by default, but field audit trail is not, so administrator needs to enable it for their Salesforce instance. When enabled, the field audit trail will display part of the change logs at the UI and store field history until it is deleted manually. If the audit trail is not enabled, field history is stored for up to 18 months up to 24 months via the API. It is important to note that some standard objects do not track the field history. (https://developer.salesforce.com/docs/atlas.en-us.securityImplGuide.meta/securityImplGuide/ tracking_field_history.htm).

Setup audit trail

A setup audit trail is used to see changes made to the organisation's Salesforce instance. It tracks many of the configurations administrators can you at Salesforce. For example, setup audit trail tracks change on user profiles. (https://developer.salesforce.com/docs/atlas.en-us.securityImplGuide.meta/

securityImplGuide/admin_monitorsetup.htm). A setup audit trail is used to see changes made to the organisation's Salesforce instance. It tracks many of the configurations administrators can you at Salesforce. For example, setup audit trail tracks change on user profiles. (https://developer.salesforce.com/docs/atlas.en-us.securityImplGuide.meta/securityImplGuide/ admin_monitorsetup.htm).

At Salesforce, authentication has different layers which organisations can leverage. For example, two-factor authentication, My domain, and single sign-on are all features every organisation should use to ensure secure logins to their Salesforce instance. (Soni & Vala 2017).

Two-factor authentication

Two-factor authentication (2FA) means that with the usual username and password, the user needs to include a separate code to log in. These days 2FA is a somewhat common thing to use on logins. At Salesforce, 2FA can be established in two different ways. The first way is to use Salesforce Authenticator App. The second way is to use some password management solution where a one-time authentication code can be established. (Soni & Vala 2017). One example of such a password management solution si Bitwarden. 2FA is something that Salesforce is pushing forward, which will soon be obligatory to use.

My domain

The organisation can custom its Salesforce instance URL (Soni & Vala 2017). Salesforce describes My Domain functionalities as follows: "Showcase your company's brand with a customer-specific subdomain name in your Salesforce org URLs. With My Domain, you can include your company name in your URLs, for example, https://mycompany.my.salesforce.com. With these org-specific URLs, you can set up a custom login page, set a custom login policy, offer single sign-on, and allow users to log in with a social account. My Domain also allows you to work in multiple Salesforce orgs in the same browser at the same time." (https://www.salesforce.com). Soni and Vala (2017) state that My Domain capabilities increase security by giving more control to the organisation's login process.

Single sign-on

Single sign-on (SSO) is an authentication scheme that uses user identity between different systems. At Salesforce, SSO is often used with Azure, where the users are managed and logging into Salesforce using the same credentials used in Azure.

With auditing features Salesforce also has many security options on the application level. In Salesforce application-level security provides functionalities to control data access inside and outside of Salesforce. On application level security, each data set can be shared or hidden for different groups or users. In order to get all benefits out of application-level security features, the organisation needs to know which kind of access different groups and users need. With this information, one can easily set up a data access policy, like CRUD (create, read, update and delete), to ensure that the right groups or users manage data. Application level security contains four levels: org level, object level, field level, and record level security. (Soni & Vala 2017).

Organisation level security

An administrator can list authorized users with organization-level security, set password policies, and limit login access.

Object and field level security

At object, a level administrator can grant or prevent access to the specific objects for the specific user or group of users. At the object level, the security administrator can control users or groups of users who read, create, edit, delete, view, and modify all accesses to the particular object. This can be obtained with profiles that indicate the permissions and settings of all the users that are assigned to that profile. Users can belong only to one profile at a time. Another way to obtain object-level security is with permission sets. A permission set is a collection of permissions and settings. Permission sets can be assigned to a specific user or group of users. (Soni & Vala 2017).

Field level security works similar way to object level security. The only difference between the two is that on a field level security administrator can manage which fields a user or group of users can access. Profiles and permissions set have a significant role also with field-level security. (Soni & Vala 2017).

Record level security

Record level security controls on which records users can see. Record level security is used on top of object level security. There are four ways to control record-level security: organization-wide defaults (OWD), role hierarchy and territory management, sharing rules, and manual sharing. OWD-specific default access level. Role hierarchy and territory management allow an administrator to create organisation hierarchy where rules on how access is granted can be established. For example, many organisation allows users at the higher in a hierarchy to access records that the users underneath them own. Sharing rules allow the creation of automation that calculates user access tables in real-time. Manual sharing is pretty straightforward. With manual sharing owner of the record can manually give access to the other users to access the record. (Soni & Vala 2017).

There are many under-the-hood security actions and measurements present at the Salesforce. This section looks at Salesforce's security strategy, programs, and controls. The whitepaper can be found at https://security.salesforce.com/.

Host and network security

Salesforce is using best practices to ensure host and network security. In the whitepaper (https://security.salesforce.com/) Salesforce describes their host and network security as follows:

“Salesforce services are powered by operating systems that are configured to standard build specifications and hardened in line with industry best practices, such as minimal configuration that removes unnecessary and default process, accounts, and protocols to reduce the attack surface of the equipment.” Precautions related to the host and network security are:

- Usage of operation systems that are using industry best practices
- Usage of TLS 1.2
- Firewalls and edge routers
- Encrypting data

Data center security

Data centers have been made secure using cloud service providers and have physical centers located carefully. Physical data centers have also been accessible only with the proper authorisation and contain a high level of physical and non-physical security measures.

Distributed Denial-of-Services protection (DDoS)

Salesforce uses a multilayer approach and multiple internet service providers. Salesforce describes that they use multiple internet services. There is also a constant network and another monitoring happening 24/7, and DDoS mitigation services are in place. If the DDoS attack occurs Salesforce’s plan is to route traffic through DDoS mitigation services to ensure smooth usage of the platform.

Other actions

Salesforce is conducting penetration tests on their systems and trying to find vulnerabilities. Other than that, Salesforce has proper Security risk management programs, documented policies they are following, and a secure development lifecycle (SSDL) process.

Salesforce ecosystem offers many different products to support ensuring security. From AppExchange, you can find 1127 Apps, 24 Bolt solutions, 41 components, 144 consultants, 44 content, five Flow solutions, and one lightning data search result when using the keyword “Security”. Many of these products are focusing ether security of documents, emails, or forms. So let's look at a few of the best-rated Apps found from AppExchange.

OwnBackup Secure – Fortify Data Security

OwnBackup Secure: Fortify Data Security (OwnBackup 2022) provides a guide for data classification, compliance requirements, encryption, and evidence-based reporting. OwnBackup Secure seems to help an administrator to manage record visibility and detect misconfigurations related to the access and visibility of records. There are also features in place that spots vulnerable data and blind spots of encryption. OwnBackup Secure also provides features to use the Salesforce Shield better. (OwnBackup 2022).

Metazoa Snapshot - Org Management for Admins

Metazoa Snapshot (Metazoa 2022) is a product that offers clean-up and optimization, release management, data migrations, profile, and user management, impact analysis, security, and compliance, and consulting. On the security side, Metazoa Snapshot has over 40 reports that give essential feedback to the administrator about who has access to what records. However, it is essential to note that the product only provides extensive reports for an administrator. For example, if a report shows that someone has access to the records, the administrator should not need to do actions to fix that manually. (Metazoa 2022).

WithSecure Cloud Protection | File Scanning and Malware Protection | Security

WithSecure Cloud Protection for Salesforce (WithSecure 2022) detects malicious uploads and downloads. It is designed to go through all files, links, and emails uploaded or downloaded into Salesforce. Content flagged as malicious is blocked, and information about the following actions is provided to the users. WithSecure Cloud Protection for Salesforce also provides extensive reporting. These reports contain information about all uploaded and downloaded content and whether they have been blocked or not. When WithSecure Cloud Protection for Salesforce has been downloaded to the Salesforce instance, it will start automatically scanning content when it is uploaded or downloaded. There are also options to do a manual or scheduled scan. (WithSecure 2022).

3.4 Summary

Digitalisation is a force that will change the way of doing business. Modern and flexible platforms will offer organisations a new way to gather, organise and use information and assets. Cloud computing is a modern and cost-efficient way to transform outdated systems and processes into highly scalable, low-maintenance, and cost-efficiency systems. Cloud computing also provides numerous ways to ensure security.

Salesforce, a world-leading CRM system, is an excellent example of high performance and a well-secured cloud-based platform. This chapter looked at how Salesforce as a cloud-based platform ensures security. In addition, the chapter highlighted different features Salesforce offers at the top of the security of cloud computing. Also, suppose the security functions Salesforce offers are not enough. In that case, one can find different security products, such as OwnBackup Secure, WithSecure Cloud Protection for Salesforce, and over a thousand others from AppExhange.

The next chapter will take a look at integrations. Integrations are a significant part of the organisation's information technology infrastructure and, therefore, an essential part of Salesforce. However, integrations create new vulnerabilities for organisations which we will see in the next chapter.

4 Integrations

Term integrations were first introduced somewhere in the 1950-1960 century. Integrations were made to connect and share information between two separated systems. One example of early full-scale integration could be the internet itself. The base idea of the internet was to connect different machines and users all around the world together. (Tähtinen 2005, p. 17-22).

Tähtinen (2005, p. 13-14) defines integration as follows; "the narrow definition is that a selection of technologies and methods of operations that are normally incompatible are made to communicate with each other in an automated manner." Integrations can be split into two categories that are system integration and application integration (Tähtinen 2005, p. 16). Those differentiate from each other according to the whether system or application must be integrated. In this thesis, both integration types are generalised with the term integration used throughout the thesis.

Integrations offer many benefits for the organisations. In the modern world, there is almost always a need for multiple systems, applications, services, and other solutions organisations need. To tackle the problem of data duplication in different systems, these systems need to communicate and share information with each other. Tähtinen (2005, p. 22-23) states that the value of information increases when it is shared. When multiple different systems are integrated a network forms. Network's value and capabilities grow as more and more systems are integrated. (Tähtinen 2005, p. 22-23). For example, one system can work as data storage, another is in charge of processing information, and the third is creating visual reports. When we connect these three systems and make them work with each other, we are increasing information's value because now we have capabilities to process and display the raw data we are gathered into the storage. As you can imagine, this makes information more accessible and saves a lot of manual work. This kind of automation often saves a lot of money and helps organisations to release resources, especially human resources, to be used elsewhere (Tähtinen 2005, p. 23-27).

Another critical factor why integrations are seen to be an efficient way to organise things is that with integrations, different systems can be transformed into a set of systems. This will make the system easier to update, maintain, and more secure. Tähtinen (2005, p. 31-33) highlights that with integrations, organisations can monitor their systems easier and track better information flows.

4.1 Standards

Many standards are related to the integrations and how they should be done. The biggest and probably most widespread standards are made by World Wide Web Consortium (W3C) which have implemented technologies such as XML (Extensible Markup Language), XSLT (Extensible Stylesheet Language Transformations), Web Services, Web Service Choreography, HTTP (Hypertext Transfer Protocol) and HTML (Hypertext Transfer Protocol) (Tähtinen 2005, p. 187). Other bodies are creating standards related to integrations. Tähtinen (2005, p.186) bring up the Internet Engineering Task Force (IETF), Object Management Group (OMG), Organisation for the Advancement of Structured Information Standards (OASIS), and Web Services Interoperability Organisation (WS-I) as an example of such bodies. There are several ISO (International Organization for Standardization) standards, such ISO/IEC 27001 and ISO 9000 that describe how to create high quality and secure software's. These standards can be seen to also include integration creation. Also, standards such as ISO 15926, ISO 55000, and ISO 14224 provide vital information for the integration creation due their focus on asset, data, and information management. Challenge is that integrations are seen to be part of overall data management and software development. There are not any specific standards for integration creation. Following list highlights some of the key features concerning integration creation those ISO standards have.

- **ISO/IEC 27001** is a series of standards for the information security. ISO 27001 brings up security side of information management. With ISO 27001 in place organisations IT-infrastructure, including integrations are created and managed in a way that security is considered. (International Organization for Standardization, 2013; Information technology — Security techniques — Information security management systems — Requirements 2013).
- **ISO 9001** is a series of standards which provides insight on how to ensure quality of products and services, such as integrations. ISO 9001 helps development to reach requirements and helps to create quality integrations. (International Organization for Standardization, 2015; Quality management systems — Requirements 2015).
- **ISO 15926** is a standard that focuses on enterprise life cycle information exchange. Standard also specifies an XML schema. (International Organization for Standardization, 2018; Industrial automation systems and integration — Integration of life-cycle data for process

plants including oil and gas production facilities — Part 13: Integrated asset planning life-cycle, 2018).

- **ISO 55000** is a standard for asset management. It has a strong relationship with ISO 55001 (International Organization for Standardization, 2014; Asset management — Management systems — Requirements, 2014) and ISO 55002 (International Organization for Standardization, 2018; Asset management — Management systems — Guidelines for the application of ISO 55001, 2018). ISO 55000 objective is to ensure that assets, such as information organisation, are appropriately managed. There needs to be a clear plan of how assets are used and what processes are where assets are used, such as integrations and mitigation of risks. (International Organization for Standardization, 2014; Asset management — Overview, principles, and terminology, 2014).
- **ISO 14224** is a standard for the reliability and maintenance of data. ISO 14224 takes a stand on requirements, formatting, collection, usage, safety, and data environment. (International Organization for Standardization, 2016; Petroleum, petrochemical, and natural gas industries — Collection and exchange reliability and maintenance data for equipment, 2016).

This list is incomplete but gives an idea of how different development- and asset-management-related ISO standards indirectly guide integration creation.

4.2 Implementation of integrations

When creating integrations it is good to take a look at best practices and how the integration-creating process should be done. Tähtinen (2005, p. 103-107) describes the technical requirements integrations need to follow. First, it is essential to understand the requirements organisation and the systems it uses. This will not only help to tackle challenges organisations environment sets for the integration but also ensure that integration architecture is in line with all the other systems in place.

After this phase comes the planning of integration, this part of the integration process will include overall planning and documentation of the following; design, functionality, technologies to be used, automation, and monitoring. Tähtinen (2005, p. 104) states that the person in charge of planning and implementing the integration needs to ensure that implementation takes into consideration that integration is as automated and maintenance-free as possible, fault tolerance reduces information interruptions, comprehensive monitoring is in place, implementation is scalable and easy to modify, and security and user management is done properly.

When integration is planned, it is time to start implementing the plan in action. Integrations are usually made in-house (organisation) by combining existing components, acquiring an integration supplier, or other suppliers that are part of the integration architecture. Integrations consist of different layers, which are:

1. ***Interface layer***, consists of connectors, adapters, and agents that are in charge of communication between systems.
2. ***Intermediate layer*** is about architectures that provide a schema for the integration to share information between systems.
3. ***Information processing- and transformation layer*** consists of tools that interpret and transform information into forms that different systems can use.
4. ***Controlling the integration process***, includes management tools (for example, business process management, BMT).
5. ***Representational layer*** that has tools for users to convey information. The representational layer also includes different portal solutions.

So, implementing the planned integration is about implementing and creating all these different layers into the system entity we call integration. Because so many different aspects come about creating integration, it's often seen as better to use either a supplier or a set of suppliers or a platform such as Mulesoft to be in charge of low-level technicalities. (Tähtinen 2005, 116-133).

The process, technicalities, and usage must be well documented during and after the integration creation. These days organisation's demands and usages for the integrations are rapidly changing, and well-documented integrations are more easily maintained and further developed. Also, the documentation needs to evolve with the implementation and usage of the integration. (Tähtinen 2005, 113). Another thing that needs to be taken into consideration during and after the integration creation is testing. All the functionalities and security of the integration should be tested alongside the creation process and regularly after the integration has been implemented. (Tähtinen 2005, p. 110-112, 133-137).

4.3 Security of integrations

Because we do not have a lot of literature about integration security, we need to look more into software security. There is much more literature and standards about software development, and because integrations belong under software development, it is acceptable to take this approach.

Software security is becoming increasingly recognised and organisations and developers are starting to act towards securing information and software. Common attack vectors related to the software are Cross-Site Scripting (XSS), Structured Query Language (SQL) injection, and buffer overflow exploitation. In these cases, information is often compromised, and the organisation and its data integrity are violated. Even today, these attacks are still approached mainly by responding and reacting to the attack. In SDL, vulnerabilities are software security flaws that an attacker has been able to manipulate. (Ransome, Schoenfield & Schmidt 2014, p. 19-21).

Security of integrations can not be only about reacting and responding to the attack; more than that, it needs to be considered at every stage of integration creation. Let's take a look at SDL, secure software development framework (SSDF), Building Security In Maturity Model (BSIMM), and OWASP Software Assurance Maturity Model (SAMM) to understand how security vulnerabilities could be managed during the creation of integration.

4.3.1 SDL

Creating secure integrations should be the intent of all parties. Secure Development Lifecycle (SDL) is a set of practices that help to reduce the number of vulnerabilities in software. SDL strongly relates to the generic software development lifecycle (SDLC). SDL principles were initially created by Microsoft (MS SDL), but we have started seeing new approaches and models to SDL over the years. SDL follows a development framework and extends security as a part of all the different stages in an SDLC. (Ransome, Schoenfield & Schmidt 2014, p. 19).

MS SDL consists of 12 practices developers should follow (Microsoft 2022).

1. ***Provide training***. Everyone needs to consider security. Organisations need to provide training for the developers to increase their expertise related to security.
2. ***Define security requirements***. Security requirements need to be defined at the same time when planning and designing implementation.
3. ***Define metrics and compliance reporting***. Risk management is part of security. Determining an acceptable minimum level of security, bugs, and vulnerabilities is essential and must be

defined during the planning phase. During the development, all the emerging security defects need to be fixed immediately.

4. ***Perform threat modeling***. Threat modeling is a practice that is used in environments where there is a significant security risk. Threat modeling makes it easier for developers to consider, document, and discuss security and vulnerabilities.
5. ***Establish design requirements***. Using security features should be done consistently, and there should be organisation level standards on which security features to use.
6. ***Define and use cryptography standards***. Encryption should be used with precautions, but developers should not be afraid of using it. Encryption- and other cryptography standards should be leveraged to add an extra layer of security.
7. ***Manage the security risk of using third-party components***. There are many different security components that developers can obtain and use. When using third-party components, it's essential to understand how they work, how to use them, and what they can offer to a specific implementation.
8. ***Use approved tools***. Using tools that have been approved and have went through security checks.
9. ***Perform static analysis security testing (SAST).*** Implementing SAST tools into the commit pipeline to identify vulnerabilities. SAST tools provide capabilities to analyze source code and ensure security policies are followed.
10. ***Perform dynamic analysis security testing (DAST).*** Testing implementation and all its components as a whole. DAST tools consist of pre-build attacks or monitoring tools.
11. ***Perform penetration testing***. Identifying and leveraging vulnerabilities with the attacker's mindset is an essential part of SDL. Penetration testing includes manual and automated code reviews and vulnerability scans, usually done by an external party.
12. ***Establish a standard incident response process***. Having a comprehensive incident response plan is crucial. A good incident response plan consists of different scenarios and attack vectors; more than that, it will state proper protocol and actions when an incident occurs.

Figure 4 shows how the agile SDL works. In Agile SDL there is three main components, architecture, development and verifying. Architecture is the first step. In includes all the SDL steps that provide requirements for the development. Development is done in sprints. Each sprint includes designing and implementing parts. Between designing and implementing the software or product is analysed, code reviewed, and tested. Last part, verifying includes overall testing of the software. This

should include penetration testing where all the functionalities and components are under series of attacks.

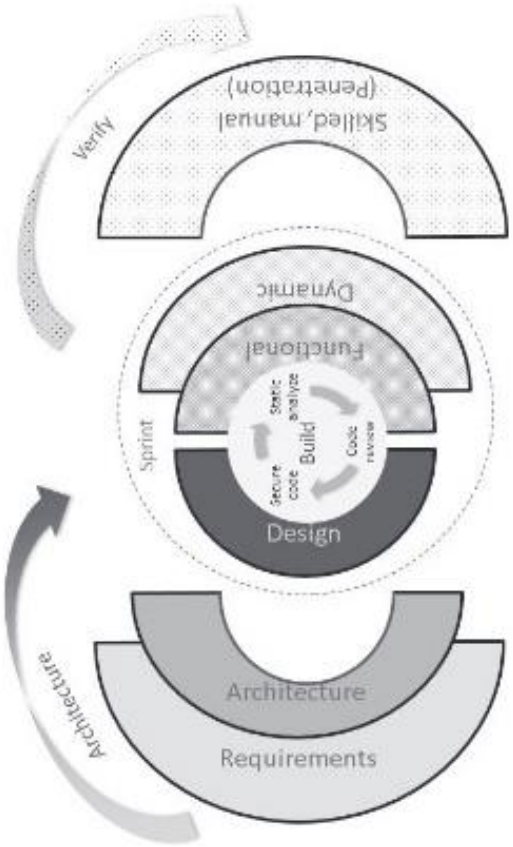

Figure 4: Agile SDL (Ransome, Schoenfield & Schmidt 2014, p. 313)

4.3.2 Secure Software Development Framework

A secure software development framework (SSDF) is a collection of secure software development documentation from organisations like BSA OWASP and SAFEcode. SSDF version 1.1 was released in early 2022, and NIST has plans to improve and evolve it further. SSDF follows in the same footsteps as SDLS with few addons; therefore, it should be integrated with SDLC implementations. The aim of SSDF is to reduce vulnerabilities in the developed software. SSDF is also seen to help security management and -communication because it provides a common language for describing secure software development practices. (NIST 2022).

SSDF practices are easy to implement, although there are different levels of practices. Organisations should consider carefully which practices best suit their needs and how to apply different practices. There are four different groups in SSDF which all have four different elements.

The groups are ***prepper the organisation (PO)***, ***protect the software (PS)***, ***produce well-secured software (PW)***, and ***respond to vulnerabilities (RV)***. All these groups follow these four elements: practice, task, notional implementation example, and reference. NIST (2022).

4.3.3 Building Security In Maturity Model

Building Security In Maturity Model (BSIMM) contains 12 practices organized into four domains (Ransome, Schoenfield & Schmidt 2014, p. 21-22). These 12 practices are strategy and metrics, compliance and policy, training, attack models, security features and design, standards and requirements, architecture analysis, code review, security testing, penetration testing, software environment and configuration, and vulnerability management.

BSIMM (2022) report brings up security tendencies related to secure software development. The report includes activities and trends from 128 organisations. In the report, BSIMM brings up ten activities on building security.

1. ***Implement lifecycle instrumentation and use it to define governance***, which includes a proactive approach to reduce vulnerabilities and create risk-based controls. This means that during the SDLC, developers collect data the software produces or/and uses, and with the data, they create and enforce software security policies.
2. ***Ensure hots and network security basics are in place***. This ensures that the network and host are correctly secured before creating software security.
3. ***Identify PII obligations***. Personally identifiable information (PII) needs to be recognized and controlled. There need to be proper controls in place to prevent unauthorized access to the PII.
4. ***Perform security feature review***. In software architecture analysis reviewing security features is essential. BSIMM (2022) highlights that, “For example a security feature review would

identify a system that was subject to escalation of privilege attacks or a mobile application that incorrectly puts PII in local storage".

5. ***Use external penetration testers to find problems***. Usage of external penetrations testers often brings up vulnerabilities that could not be found internally.
6. ***Create or interface with incident response***. Open communication and information sharing between the development-, response team, and other stakeholders is essential to lower response time.
7. ***Integrate and deliver security features***. Commonly used security features should be shared inside the organisations. There is no need to re-create similar security features over and over again.
8. ***Use automated tools***. In complex environments managing security manually is impossible. With the usage of automated tools, it becomes easier to manage security.
9. ***Ensure QA performs edge/boundary value condition testing***. Thinking like an attacker is crucial because it helps one think outside the box. This kind of thinking will help find vulnerabilities that would otherwise stay hidden.
10. ***Translate compliance constraints to requirements***. Many organisations are starting to approach software requirements from compliance constraints. Compliance constraints are considered with this kind of approach at the beginning of development.

4.3.4 OWASP Software Assurance Maturity Model

OWASP (2022) Software assurance maturity model (SAMM) provides a way to analyze and improve SDL. OWASP SAMM is an open framework, and it is an evolutive and risk-driven model. The model contains five business functions which are each split into three practices. The first business function is ***Governance***, and it has the following security practices; *strategy and metrics*, *policy and compliance*, *education and guidance*. Next up is ***Desing*** this business function contains *threat assessment*, *security requirements*, and *security architecture*. The third business function is ***Implementation*** which splits into *secure build*, *secure deployment*, and *defect management*. Following that comes ***Vertification***. Verification business functions subcategories are *architecture assessment*, *requirements-driven testing*, and *security testing*. Lastly is ***Operations***, which includes *incident management*, *environment management*, and *operation management*. (OWASP 2022).

Figure 5: OWASP (OWASP 2022)

The strength of OWASP SAMM lies in its comprehensiveness. The model also takes a stand on the different responsibilities of different actors. Governance is more an organisations responsibility to implement and share. The responsibility of Design also lies in organisation. OWASP (2022) states that under a design, security requirements bring up how to ensure that third-party or supplier needs to be evaluated. This also includes that in the agreements between organisation and third-party organisational requirements for security needs to be present.

Implementation highlights the responsibility of developers. This part contains practices about documentation, development patterns, development process, and metrics and tracking. Verification is all about assessment and testing (OWASP 2022). As stated earlier, testing should be done by developers, organisations, and external sources, and it should be done at all levels and stages of the development process. Operations is described as a joint effort, but the responsibility of it lies in organisation. How to manage incidents and which kind of incident response processes there is in place are questions organisations need to have the answer to. Developers need to continuously patch and update applications whenever vulnerability arises. On an operational level the documents and policies concerning security and data protection need to be kept up to date. The responsibility of these organisation-wide documents lies in organisation and they need to follow current laws and standards. (OWASP 2022).

4.4 Integrations in Salesforce

Force.com provides a wide variety of tools and concepts to create integrations. For example, you can create integrations using code or pre-created AppExchange packages. At the AppExchange, there is a section for integrations. This section has 200 different integration apps. For example, Patel and Chouhan (2017) found an existing package containing integration between Salesforce and Twitter from AppExchange, which they used in their research. Salesforce integrations can be split into architecture, capability, and pattern types. Salesforce has integration architecture which consists of three different types.

Point-to-point integration means a one-to-one relationship with Salesforce and another system where those two systems communicate through messages. Hub-and-spoke integration means an integration type where a centralised hub system is in charge of communication between systems. Hub in this kind of integration is in charge of routing traffic between systems. The third integration type is enterprise service bus integration (ESB). ESB is the next generation of hub-and-spoke integration. ESB, like hub-and-spoke, has a centralised connector in charge of routing traffic between systems. The difference is that in ESB, this centralized connector is an integration engine that can be used to create these connections between systems. A significant benefit of ESB is that it offers capabilities to improve integration security. With ESB, for example, one could create authentication and authorization inside the integration. (Renwick 2022).

Patterns provide a concept for integration. You also need to consider the integration's requirements when thinking about Salesforce integrations. This includes timing (synchronous vs. asynchronous), direction (inbound vs. outbound), and type. (Renwick 2022). Salesforce has its own pattern selection guide (https://developer.salesforce.com/docs/atlas.en-us.integration_patterns_and_practices.meta/integration_patterns_and_practices/integ_pat_selection_guide.htm) to help developers to choose the correct pattern for the use case. In the Salesforces pattern selection guide, the patterns are categorized by using two different dimensions; type and timing. The type has three different integration styles: process, data, and virtual. Process-based integrations provide possibilities to process functionality between more than one system. Data integrations integrate data between systems. Virtual integrations mean that Salesforce interacts with data in another system. The action always triggers virtual integrations inside of the Salesforce. (Renwick 2022). Renwick (2022) states that the most commonly used patterns are:

- ***Remote Call-In*** which data in the Salesforce is managed by a remote system.
- ***Request and reply*** where Salesforce invokes callout on a remote system and waits for the response.
- ***Fire and forget*** are similar to request and reply in the difference that it does not wait for a response.
- ***Batch Data Synchronization***, where data stored in Salesforce is managed in Salesforce, but changes are reflected in another system.
- ***UI updates are based on data changes***, meaning that changes to the data reflect the user interface (UI).
- ***Data virtualization*** is covered more when talking about Salesforce Connect.

4.4.1 Salesforce API's and integration capabilities

Salesforce provide eight different capabilities to create integrations. These are ***REST API, SOAP API, Bulk API, Streaming API, Outbound Message, Web Service Callouts, Salesforce Connect*** and ***Heroku Connect***. (Renwick 2022). Let's go more in depth with these different capabilities:

REST API

In Salesforce, REST is synchronous and focuses on data-based operations such as GET, POST, PUT, PATCH, and DELETE. ***REST API*** is used with mobile and web applications and uses XML and JSON. (Renwick 2022).

SOAP API

SOAP API provides good capabilities for system-to-system integrations, back-end system communication, and formal hand-off communication. SOAP API is not used as much these days. The reason is that SOAP API is slower and uses a lot more bandwidth than REST API. (Renwick 2022).

Bulk API

Bulk API is used to manage a large number of messages, and it works asynchronously. Bulk API is most commonly used for data migrations due to its ability to process jobs in serial or parallel. (Renwick 2022).

Streaming API

In Salesforce, there are four different ***Streaming API***s; Generic, PushTopic, Platform Events, and Change Data Capture. Streaming API has a basis in Event-Driven Architecture and is based on the publish/subscribe model. Streaming API is commonly used for notifications. (Renwick 2022).

Outbound Message

Salesforce provides a variety of capabilities to create processes inside the platform. Often there is a need for these processes to send messages into another system. These messages are sent through a SOAP-based server endpoint with a custom listener service. However, Salesforce advises that Streaming API should be used when there is a need for near real-time integration. (Renwick 2022).

Web Service Callouts

Web Service Callouts consist of actions created by the developer, which is efficient when a synchronous or quick response for asynchronous is needed. Web Service Callouts are used when Salesforce calls out to another system and when data load is small (Request and Response < 3 MB). (Renwick 2022).

Salesforce Connect

Salesforce calls ***Salesforce Connect*** "Data virtualization". This means that data can be shown in Salesforce even if it is not stored in Salesforce. The benefit of using Salesforce Connect is that it can save a lot of data storage space. When Salesforce Connect is established, it offers capabilities to many of the build-in features Salesforce has, such as relations between other objects and reporting. (Renwick 2022).

Heroku Connect

Heroku (https://www.heroku.com/) is PaaS that supports many different programming languages, and Salesforce has owned it since 2010. Heroku Connect is the connector between Salesforce and Heroku Postgres with the main benefit of using Heroku Connect is that developers bypass many infrastructure obstacles Salesforce has. (Renwick 2022).

4.4.2 Salesforce integrations security

Salesforce documentation (https://developer.salesforce.com/docs/atlas.en-us.integration_patterns_

and_practices.meta/integration_patterns_and_practices/integ_pat_security_considerations.html) brings up security tools, techniques and Salesforce-specific considerations related to the security of integrations. One such security consideration is the usage of the reverse proxy server. When creating Salesforce integrations and there is some client, the reverse proxy server can come in handy because it retrieves resources on behalf of the client and then returns those resources to the client as proxies' resources. Another way to ensure the security of the integrations is to use encryption. Salesforce has its own on-premises commercial encryption gateway service (Salesforce Shield Platform Encryption), which could be used. Developers can also use other encryption gateway services if wanted. These encryption engines or gateways provide encryption and decryption for the payload to make more secure transactions. There are also possibilities to use security protocols and SSL and IP restrictions.

Other than stating there is that much documentation or best practices on how to make secure integrations. As mentioned earlier, Salesforce itself is highly secure. However, when developing integrations, it is assumed that following the security precautions mentioned and proper user and visibility management is up to third-party service providers to ensure that their end of integration is secure. This is because if someone with malicious attends gets into the third-party system with administrator credentials, they can use integration as if they are administrator users. Furthermore, all the access and actions provided for the administrator user (often Salesforce integrations work under generic integration user profile) are there. On the Salesforce side, it is impossible to know whether the user is how it seems to be or a malicious actor with administrator credentials. Only some sort of anomaly detection cloud is a possible solution to find out if a malicious actor uses the API.

4.5 Salesforce integration tools

Salesforce has many integration tools that provide easier way to create integrations. Integration tools are point-and-click tools which means that there is no need of coding which means that they do not need such extended knowledge. Aim of integration tools is to format data and simplify data process in order to create compatible integrations. Integrations tools main capability is that they compile and format data in a way that target system can process it. Main benefit of using such tool is that integrations can be managed better, and changes and the connections are easier to maintain. Some of the top integration tools are Dell Boomi, Jitterbit, Tibco Scribe, Orbis, Commercient, RapidiOnline,

Blendo and Mulesoft Anypoint Platform which we will take a look closer in a next section. (Naeem 2019; Rodgers 2021).

Mulesoft Anypoint Platform (https://www.Mulesoft.com/) states that it is one of the world's leading SOA, SaaS, and API integration platforms. Knapp (2018) describes Mulesoft as follows: "Mulesoft is a vendor that provides an integration platform to help businesses connect data, applications and devices across on-premises and cloud computing environments". Mulesoft Anypoint Platform contains various development, management, and testing tools to create and maintain APIs. Salesforce owns Mulesoft; therefore, the Mulesoft Anypoint Platform is well supported by Salesforce and is part of Salesforce integration Cloud. (Knapp 2018). The main benefit of Mulesoft is that it provides full life cycle of API management. Mulesoft is divided into two main parts: Control Plane and Runtime Plane. Control Plane has metadata of the specific APIs and runs in AWS. Runtime Plane is run in either CloudHub, public or private cloud, or customers data center. Runtimes are based and operating in this instance.

Seth (2018) used Mulesoft to migrate data into Salesforce. Seth (2018) brings up how the batch process works in Mulesoft. In Mulesoft batch process consist of four different steps. At first, the optional step triggers fire processing via an inbound endpoint, and the payload is modified before entering the processing. The second step consists of loading and its implicit. This performs background work and splits the payload into the right size of data sets, and then queues these data sets for processing. The third step is the process itself, and this part is required part of Mulesoft batch process. In the process step, asynchronous processing for each data set is done. This is done by respecting queue and data set orders at the queue. Processing is done as often as there are data sets in the queue. The fourth and final step is complete, which is an optional step of the process. When all the data sets in the queue are processed, there is often a summary report about how the process went, which includes information about how much data was processed, what was fail and the success rate, and related error messages for the corresponding fails. (Seth 2018).

4.5.1 Mulesoft tools

Mulesoft contains many different tools. These tools are highlighted in figure 6 which shows Mulesoft's architecture. Knapp (2018) lists Mulesoft tools and their capabilities:

- ***API Designer*** that helps developers to design and document APIs. It also provides support to share design with the team and reuse specific components.
- ***API Manager*** offers an interface to manage and secure APIs.
- ***Anypoint Studio*** is a Java-based design environment that works as an editor to make and deploy APIs. It includes different features to help make the development process more straightforward and efficient.
- ***Anypoint Connectors*** means set of built-in connectors for developers to use. It has thousands of third-party REST and SOAP.
- ***Anypoint Analytics*** provides analytic tools to monitor and visualize how APIs are performing and used.
- ***Anypoint Runtime Manager*** is a central console. This console is there to help developers provision and monitor all different resources deployed.
- ***Anypoint Exchange*** is a marketplace where developers can find different APIs, templates, connectors, documentation, and resources.
- ***Anypoint Monitoring*** helps to monitor application health.
- ***Anypoint Visualizer*** maps APIs and their dependencies in real-time.
- ***CloudHub*** is a multi-tenant integration platform as a service (iPaaS).

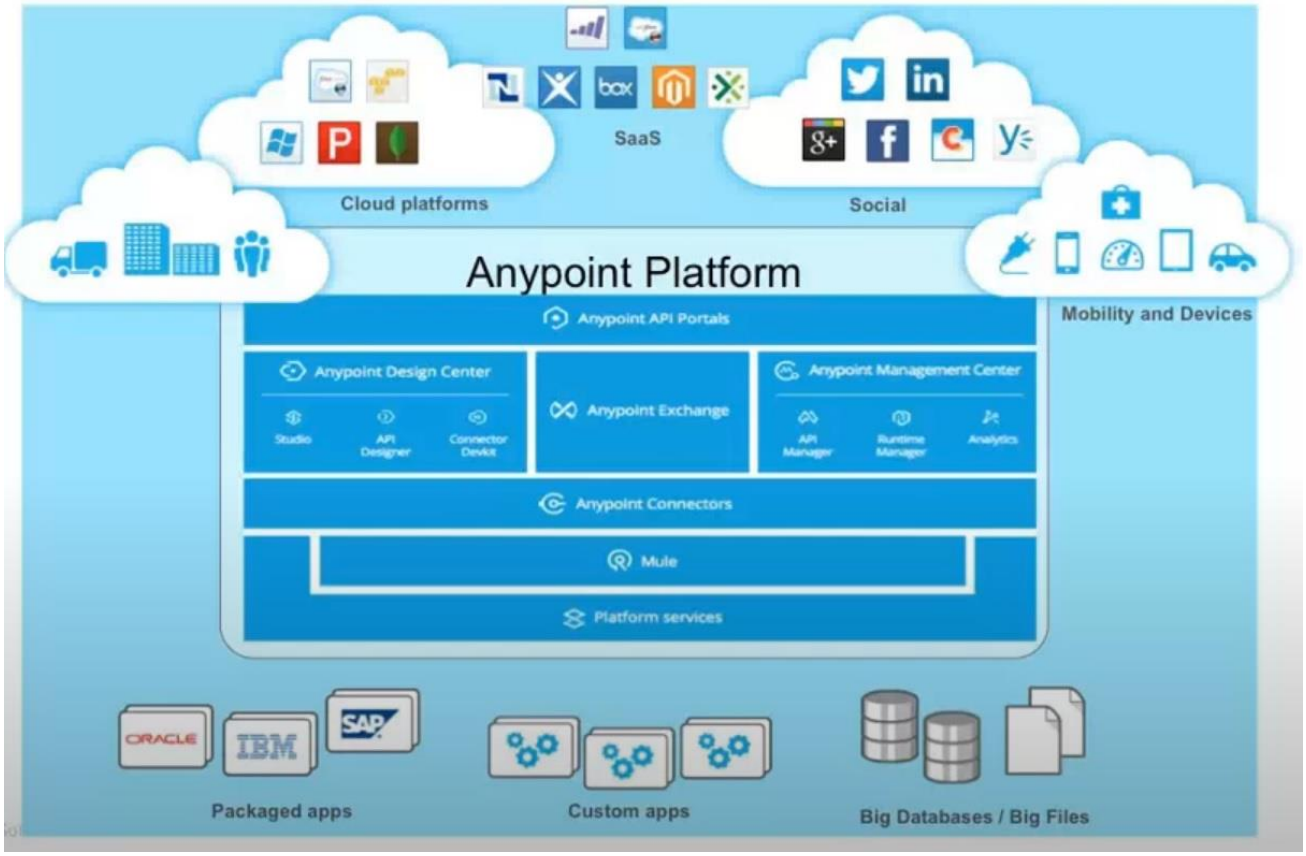

Figure 6: Sinha, Rupesh (2017). MuleSoft Architecture [Youtube-video]. Source: https://www.youtube.com/watch?v=g7PvkCXVPac

4.5.2 Mulesoft security

Among everything else, Mulesoft is seen to offer automated and consistent security for the APIs and data. Mulesoft (Mulesoft 2022) state that they use different features and customs which makes integrations made with Mulesoft secure. It is architected to be secure, and the security is obtained with different features, infrastructure choices, and best practices. Mulesoft uses Amazon Web Services (AWS), one of the most secure cloud infrastructures. It also has many out-of-the-box prebuild and custom policies that follow standards such as ISO 27001, SOC 2, PCI DSS, HIPAA, and GDPR. Mulesoft uses a shared responsibility model where Mulesoft offers a large variety of security features and its customer's responsibility to use them. (Mulesoft 2022).

Paige (2018) brings up zero trust security architecture. In zero trust architecture, security is a central part of the development. Paige (2018) states, "*All communications between APIs, and with data consumers, must be mutually authenticated, authorised and encrypted, and governed by policy".* Paige (2018) continues that this company-policy based access management needs to be centrally managed but handled decentralized manner. Zero trust architecture follows four principles (Paige 2018):

- ***Asset discovery*** means that there should be a complete list of all the APIs that are in use.
- ***Take a capabilities-led view*** that provides a view on APIs purpose and by that security precautions that APIs are being used in a way they are meant to. This will provide more precise and better-targeted security functions.
- ***Adopt a continuous approach*** means that APIs security needs to be maintained alongside modifications made to the APIs.
- ***Deploy a distributed enforcement model*** that focuses on securing APIs front-end and alongside the back-end. There should be a set of security features on both front- and back-end side in order to make API secure as a whole.

Overall, one could say that the Mulesoft Anypoint Platform offers a good level of security when used in the way it is meant to be used. Mulesoft provides a training platform (https://training.Mulesoft.com/home) where these best practices are taught. To become a Mulesoft developer, you must have certification and understand the security measures to be used when creating APIs with Mulesoft.

4.6 Summary

Integrations offer the possibility to connect organisations Salesforce with third-party applications. For organisations using different systems and applications alongside their Salesforce, integrations are essential for their business processes. There are different standards and best practices organisations, and developers must consider and follow when creating integrations. Salesforce itself provides comprehensive APIs and tools to create integrations.

Alongside all the benefits integrations enable, they also create new vulnerabilities for cybercriminals to leverage. In this chapter, we looked at some of these possible vulnerabilities and provided insight into how best practices, standards, and models can help decrease the amount of vulnerabilities integrations may create. With Salesforce's integration design patterns, developers can increase the security of the integrations. However, Salesforce relies on third-party application providers to ensure security at the other end of the integration.

To improve integration security and not rely on Salesforce or third-party application provider, organisations and developers need to take ownership of the integration security. SDL is a model organisations, and developers should follow when creating integrations. OWASP SAMM is a model derived from SDL and provides a great way to implement security into integration development. The

benefit of OWASP SAMM is that it provides clear steps to ensure security is considered from start to finish.

In the upcoming chapters, we look at research that focused on security practices and responsibility beliefs organisations and developers have.

5 How organisations ensure security of integrations?

In this chapter, we go through the result of the *Salesforce survey for organisations*. This chapter aims to highlight how organisations see their role in ensuring integration security and what are their prior knowledge on security.

5.1 Analysis and profiling of organisations who responded to the survey

In the *Salesforce survey for organisations*, there were a total of nine answers. Analysing organisations that responded, there was a clear indication that larger organisations and organisations with more than four years of Salesforce experience were more willing to answer the survey than smaller and less experienced ones.

The smallest organisations had ten to 50 employees. Three organisations fit into this size group. There were one of each organisation with a size of 51 to 100, 101 to 500 and 501 to 1000. The three biggest organisations fit all into the size of 1000 to 5000. In the analyse, organisations were categorised into three different groups; small, medium and large. The small category contains organisations with 10 to 50 employees, while organisations in the medium category have a size of 51 to 500. Statistics Finland (2022) defines that small organisations have less than 50 employees and medium organisations have less than 250 employees. Due to grouping in query, it is hard to say whether the organisation responded to have a size of 101 to 500 fits into this definition. This organisation was decided to be categorised as a medium. With this there were two organisations to be categorised as medium size. Category large organisations contain organisations which have more than 500 employees. The categorisation aimed to recognise whether the size of organisations indicates an organisation's willingness and capabilities to resource information security and weather those resources translate to better management of the Salesforce integration security.

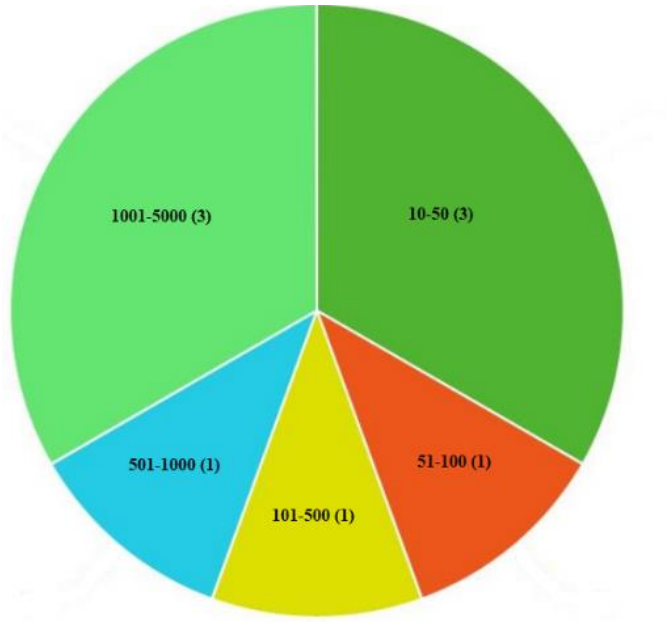

Figure 7: Size of organisations.

Looking into the Salesforce experience of each organisation, there were two organisations with less than a year of experience with Salesforce and two with one to three years of Salesforce experience. The rest of the organisations (5) have four to ten years of Salesforce experience. Organisations were categorised also with their Salesforce experience into less than a year, 1 to three years, and four to ten years of experience. Assuming there are some differences between organisations related to the Salesforce knowledge and how to ensure Salesforce integration security between organisations that have used Salesforce longer and those with less experience with the platform.

Six out of nine organisations have the same, or in a close range, amount of Salesforce users than they have employees. This indicates that most of the organisations that responded have implemented their Salesforce on all levels of their organisation. It is important to note that most the smaller organisations have all their employees as users. This indicates that even larger organisations have more resources in their use, Salesforce license expenses can raise a lot when a larger organisation has all their employees as Salesforce users.

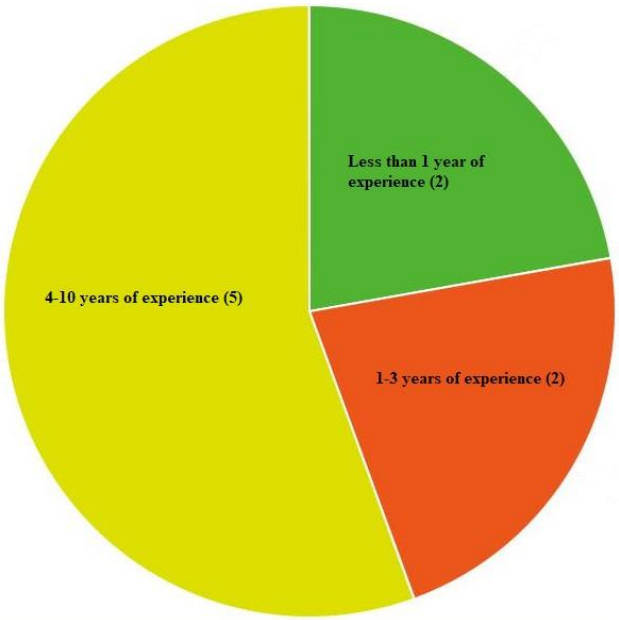

Figure 8: Years of Salesforce experience organisation have.

5.2 Results

In this section, we go through all the questions split into the four categories: Information Security Policy (ISP) and responsible person, Customs on Salesforce integrations, Integration security knowledge, Responsibilities to create secure integrations, and best practices to ensure integration security. In each section those two categorisations, size and experience were used to go through the results.

5.2.1 Information Security Policy and responsible person

Almost all organisations have some ISP. One smaller and one medium organisation did not have such a policy. Large organisations were the only group where all organisations had information on some ISP. Large organisations also more likely than not have chief information officer and other formal security manager roles (CISO, CIO, Security manager). In small and medium size organisations, a person in charge of information security seems to have multiple roles where security is one of many. Study shows that the size of the organisation clearly affected how clear and formal the security role organisation has. Smaller organisations have more generic security roles where the responsibility of security is whether one of the roles or, in some cases, it is one of the tasks the person has alongside other tasks. In larger organisations, an assigned person is in charge of security, and their primary role is to ensure information security as a whole. Job titles of such persons are often CIO or CISO. The

study shows a clear correlation between size and formality of the person in charge of security in the organisation.

All organisations with some ISP state that they are not directly covering integration security in the information security policies. It is safe to assume that organisations that have ISP but did not answer the question do not have integrations included directly or indirectly in their ISP. Larger organisations tend to have wider ISP and seem to include aspects of integration and information security better than smaller organisations. Only one small organisation covers data security and processing in their ISP. There is room for improvement in all organisation's ISP's to cover integration security better.

ISP should define different data types and provide actions to protect data. Integration point of view should be included in this part of ISP alongside GPDR and other regulations. For the development side of the ISP, development lifecycle best practices, models, and frameworks such as SDL (secure development lifecycle) should be defined in the ISP to guide secure development. (International Organization for Standardization, 2013; Information technology — Security techniques — Information security management systems — Requirements 2013). ISO 27001 (International Organization for Standardization, 2013; Information technology — Security techniques — Information security management systems — Requirements 2013) also mentions that third-party supplier policy should be either included in the ISP or as a separate document. In summary, integration development and security should be reflected in all parts of ISP alongside software development.

5.2.2 Customs on creating Salesforce integrations

Organisations approach the creation of integrations differently. Many organisations rely on partners, some have internal developers to implement integrations, and especially larger organisations use both. Pretty much all organisations think that integrations are an essential part of Salesforce. All organisations stated that integrations are a significant part of the Salesforce ecosystem. However, there was a slight indication that in the smaller organisations, which were more likely to use partners, the importance of integrations was higher than in larger ones. It would be interesting to see whether the number of other systems an organisation uses affects how important they see the role of integrations. Assuming that the more systems organisations have, the more integrations they need, making the importance of integrations even higher.

It seems that many organisations do not quite understand what the definition of a Salesforce developer is. In the survey there were assumption that question about the amount of in-house Salesforce developers would be commonly understood, but it seems that this was not the case. FMD (2022) states that a Salesforce developer has a comprehensive understanding of Salesforce, knows how to customise and manage Salesforce instances, and can create third-party integrations. Essential skills Salesforce developers have programming and problem-solving skills, mindset and willingness to work with technology (FMD 2022). With this definition, it is safe to assume that smaller organisations do not have many Salesforce developers, if none, despite some answers where smaller organisations seem to have more than five in-house Salesforce developers. There is also a possibility that some of the answers where the in-house developer amount is high are Salesforce partners. Salesforce partner is a consulting agency that Salesforce authorises to provide development and consulting for organisations using Salesforce (Skyplanner 2022). They can also be using Salesforce by themself, which could explain results where a smaller organisation has a high amount of in-house Salesforce developers. Other than that, larger organisations, organisations that have used Salesforce longer tend to have more in-house Salesforce developers. The percentage of employees as Salesforce users did not indicate whether the organisation had many Salesforce developers or not.

The study shows that more in-house developers are more likely to do integrations as in-house work. The organisation's size also made a massive difference in how they do integrations. Small organisations tend to use partners when creating integrations, while medium organisations rely more on in-house integration development. Large organisations are creating integrations by using both in-house and partner resources. It is safe to assume that larger organisations have a high number of systems and, therefore, a higher need for complex integrations, creating a need for a higher amount of Salesforce developers. Due to the lack of Salesforce developers on the market, larger organisations must use partners to get this resource. As a result, smaller organisations do not have as much in-house resources, so they must use partners.

In the study, we also found that much improvement is needed on how organisations ensure that partners follow the organisation's information security policies and practices. For example, only one out of nine organisations seem to have non-Disclosure agreements (NDA) and data processing agreements (DPA), including the following information security policies and practices. Three organisations have some form of auditing in place, where the organisation or a third party reviews the security of implementations. Most organisations that are using partners seem to assume and trust that partners Salesforce developers are ensuring integration security as default. In section 6.1, there was stated about the organisation's responsibility to their customers and how GDPR and other national

and international regulations need to be considered when information is transferred from one environment to the other. Therefore, the organisation must be aware of precautions and design patterns Salesforce developers have used to create integrations.

5.2.3 Integration security knowledge

There is two tables, table 1 and table 2 created from the responses to the *Salesforce survey for organisations*. These tables present average scores of responses. There are table for size of organisation categorisation and for Salesforce experience in years categorisation. Both tables are divided by the grouping of each categorisation. Average scores are using scale 1 to 6 where 1 is "*strongly disagree*" and 6 is "*strongly agree*".

Organisations have different levels of knowledge of what comes about integration security. There is also a significant difference seen between organisations that are large in size than in smaller organisations. It also seems that there is a strong correlation between integration security knowledge and recognising different vulnerabilities integrations create. Also, the number of in-house Salesforce developers affects the organisation's integration knowledge level. Organisations of all sizes have a better understanding of how to implement information security on integration creation than they have of threats that integrations create. In chapter 4.3 Security of integrations, we went through common vulnerabilities integrations have. These should be well understood in all organisations because all the integration implementations should ensure that these threats are covered. This should be something for the organisations to include in their ISP so that it is easier to point out to developers what kind of threats need to consider.

Smaller organisation's level of knowledge about integration security threats and knowledge on how to create secure integrations is not at in good level. There seem to be three reasons for this finding, which all tight to a lack of resources. First, smaller organisations do not have as many in-house Salesforce developers and security professionals as bigger ones. Another reason is that smaller organisations do not have ISP, or there are significant shortcomings in their ISP. Even though the situation is much better in large organisations, there seem to be improvements also needed there.

There seems to be an interesting conflict between security knowledge and the importance of integration security. All organisations state that it is important to consider information security while creating integrations. It would be interesting to see whether the importance of integration security is also recognised at the organisation's management level due to the lack of resources. Assuming that

with the increasing resources invested in integration security, all organisations would have a better understanding of integration threats and integration implementation from a security perspective.

Size of organisation	Amount of responses	Integrations are an essential part of Salesforce.	Our organisation knows different kinds of Information Security threats related to Salesforce integrations.	In our organization, we know how to ensure Information Security when creating integrations.	When creating integrations Information Security is something that needs to be considered.
10-50	3.00	5.67	2.67	3.67	6.00
51-500	2.00	6.00	4.00	4.00	6.00
501-5000	4.00	5.50	4.25	4.50	6.00

Table 1: Responses related to integration security knowledge using size of organisation categorisation. Average scores between 1 and 6 (1 = Strongly disagree, 2 = Disagree, 3 = Some what disagree, 4 = Some what agree, 5 = Agree, 6 = Strongly agree).

Years of Salesforce experience	Amount of responses	Integrations are an essential part of Salesforce.	Our organisation knows different kinds of Information Security threats related to Salesforce integrations.	In our organization, we know how to ensure Information Security when creating integrations.	When creating integrations Information Security is something that needs to be considered.
< 1 years of experience	2.00	5.00	3.00	4.00	6.00
1-3 years of experience	2.00	5.00	4.50	4.00	6.00
4-10 years of experience	5.00	5.75	4.50	5.25	6.00

Table 2: Responses related to integration security knowledge using years of Salesforce experience categorisation. Average scores between 1 and 6 (1 = Strongly disagree, 2 = Disagree, 3 = Some what disagree, 4 = Some what agree, 5 = Agree, 6 = Strongly agree).

5.2.4 Responsibilities to create secure integrations

Responsibilities to create secure integrations like brought up have scores from 1 to 4. 1 means "*main responsibility*", 2 *"some responsibility"*, 3 "*little responsibility*", and 4 *"no responsibility"*. Table 3 and table 4 shows how the responses were split with each categorisations and groups. This chapter goes through all those responses and findings that they provide.

When taking a look on how organisation's see responsibilities there is clear indication that organisation's think that they themselves have the highest responsibility. By taking a look on averages how organisations rated each stakeholders we see that Corporate Information Security (CIS) was ranked having most responsible. Organisation using Salesforce and partner, or system integrator were tied to the second place. These all were ranked to have main responsibility on creating secure integrations. Fourth were Salesforce having overall ranking as main responsible at a slight margin. Developer was fifth and at the last place were third-party software provider. Developer and third-party software provider was seen to have some responsibility. It is important to point out that when considering on a overall average all stakeholders had greater score than 2.5 on a scale 1 to 4, where 1 ment "Main responsibility" and 4 "No responsibility". Therefore, it is safe to say that all the

stakeholders highlighted were seen to have at least some responsibility what comes to creating secure integrations.

When take a look to the results from the organisation size point of view we can see that small organisations think that biggest responsibility lies on themself, including responsibility of CIS. After that comes Salesforce and partner or system integrator. Out of these six, developers and third-party software provider are ranked as least responsible. It seems that small organisations responses are inline with the average scores.

At the medium size organisations developers and organisation, themself are seen to have main responsibility. Then comes CIS and Partner or system integrator. Tied to the least responsible spot are third-party software provider and Salesforce. It is interesting to see that there is clear difference between small and medium size organisations. Medium size organisation tie responsibility between developers and partners or system integrators who are in charge of creating these integrations, and with organisation and its security representatives.

Large organisations have a bit higher average score than rest of the categories. They saw that CIS have the most responsibility and partner or system integrator are coming closely behind them, as both having main responsible. Salesforce's responsibility was seen as a third highest having some responsible. Organisation using Salesforce, third-party software provider, and developer are even with a lowest responsible compared to others by having some responsibility. Interestingly some large organisations saw that organisation using Salesforce have little responsibility, and one organisation thought that third-party software provider have no responsible on what comes about creating secure integrations.

When looking the results from the perspective of Salesforce experience categorisation, organisations that less experience with Salesforce see that main responsibility lies on Salesforce and CIS. Organisations with more experience agree that main responsibility lies on CIS, but rate Salesforce to have some responsibility. When organisation get more Salesforce experience, they also tend to put main responsible towards organisation using Salesforce and partner or system integrator. There was also clear difference on developers' responsibility when looking from experience perspective. Organisations that have little Salesforce experience rated developers to have some or little responsibility, whereas more Salesforce experienced organisations were unanimously agreeing that developers have some responsibility.

Size of organisation	Amount of responses	Developer	Organisation using Salesforce	Third-party software provider	Salesforce	Corporate Information Security	Partner / System Integrator
10-50	3.00	2.00	1.00	2.00	1.33	1.00	1.67
51-500	2.00	1.50	1.50	2.50	2.50	2.00	2.00
501-5000	4.00	2.25	2.25	2.25	2.00	1.25	1.50

Table 3: Responses related to responsibilities using size of organisation categorisation. Average scores between 1 and 4 (1 = Main responsibility, 2 = Some responsibility, 3 = Little responsibility, 4 = No responsibility).

Years of Salesforce experience	Amount of responses	Developer	Organisation using Salesforce	Third-party software provider	Salesforce	Corporate Information Security	Partner / System Integrator
< 1 years of experience	2.00	2.50	2.00	2.00	1.50	1.00	2.00
1-3 years of experience	2.00	2.00	1.00	2.00	2.00	1.50	1.50
4-10 years of experience	5.00	1.80	1.80	2.40	2.00	1.40	1.60

Table 4: Responses related to responsibilities using years of Salesforce experience categorisation. Average scores between 1 and 4 (1 = Main responsibility, 2 = Some responsibility, 3 = Little responsibility, 4 = No responsibility).

5.2.5 best practices to ensure integration security

Most of the organisations brought up that searching best practices and monitoring integrations are two of the most valuable way to ensure integration security. Interestingly when looking the results from the size point of view, organisations seem to agree with each other's. Especially small and medium size organisations had almost same top three.

Small organisations top three was extensive testing, searching best practices and monitoring integrations with one exception where on a spot of extensive testing was auditing security of third-party software. Medium size organisations had completely the same responses. Their top three was creating own set of validations, searching best practices, and monitoring integrations. Large organisations brought up different combinations on following choices: asking about the security from a third-party software provider, searching best practices, auditing security of third-party software, monitoring integrations and extensive testing. One large organisation also chose using solutions found from AppExchange.

5.3 Summary

As we can see in the results there is seen some differences between organisations. There is also a lot of similarities. Especially the size of organisations indicates many of characteristics organisations have. In the results we saw that large organisations have established more standardised security roles and have wider ISP. Small organisations also usually have ISP established but it seems that smaller organisations ISP covers more topics that different regulations and laws obligate them to cover. Title of the person responsible about security and their role at the Salesforce implementations is more official at larger organisations. At medium size organisations, and especially at small organisations, security seems to be part of person role. Person in charge of security at small and medium size

organisations is heavily involved other activities such as creating, designing and monitoring integrations, or having project management type of role. This indicates that there might be lack of knowledge and resources related to security and ensuring that security is considered. However, it is good that organisations are at least trying to have security considerations implemented and in most of the organisation who responded to the survey had some sort of person in charge of security.

When looking the results, we saw that organisation's at all sizes need some level of updating what comes about their ISP. Especially the organisation's that does not have enough knowledge about integration security could have benefit on using outsourced security specialists involvement in the creation of ISP. Results show that most of the organisations, and especially small one's lack of knowledge about information security threats related to integrations. Organisation's also lack knowledge about creation of safe integrations. With well documented ISP many of these knowledge absences could be tackled. When taking a look at literature we see that more depth the ISP has the easier it is to lead the development. With integration security covered at the ISP it would be easier organisations who are using partners to demand and control weather developers are considering security enough while creating integrations.

Some large organisations have strong and clear agreements including security. This type of agreements or at least mentioning security in the agreements would most likely encourage Salesforce developers and partners take security more seriously. Tähtinen (2005, p. p. 39-40, 42-43) brought up that when organisation is choosing right partner to implement integration it is important to make sure that overall architecture, including security aspect of the integration, is something partner can achieve. Also, the documentation before and after implementing integration solution should be present. These documentations should also include security aspect of the implementation. (Tähtinen 2005, p. 39-40, 42-43, 110-113).

There is seems to be some mismatch on where the responsibilities lies on. Small organisations have relied or are relaying on their partners to make sure that security is properly considered. However, they also see security to be organisations main responsibility and not as much developers or partners responisibility. If organisation think that they should be mainly in responsible about security of integrations, there needs to be proper resourcing and training for those who are organisations responsible person on security matters. At larger organisations there seem not to be as much mismatch. Larger organisations tend to relay more in their in-house resources and personals, and what is good to see that those personals seem to be proper security professionals. Auditing is something what should be leveraged more, especially by the smaller organisations where there is some lack on security knowledge. Auditing those third-party software's where integrations are

connecting is something that large organisations see as a best practice to ensure security of integrations. In the organisations where there is no enough knowledge about integration security itself it could be beneficial to audit and test also the integrations.

Overall, it seems that there is some improvement to be done at all organisations. However, it is important to note that all the responding organisations saw integration security be important and seem to have thought on some level what actions can they do to ensure security of integrations, and to make sure that their information is properly processed and managed. When we look at a size of responding organisations we see that larger organisations are more willing to respond this kind of security related surveys. This is inline with the findings that small organisations do not resource security as much as large organisations. It is safe to assume that all the survey responders agree that there is still big mismatch between security budgets and importance of security. Organisations security responsible persons tend to have a hard time to convince organisations decisionmakers to increase security budgets. However, while cyber-attacks are becoming more common, organisations seem to invest more to the security. There is increase of CIO, CISO, and other security roles established in the organisations all around the world. (Ursillo & Arnold 2019; BT group 2021).

6 How Salesforce developers ensure security of integrations?

In this chapter, we go through the result from *Salesforce survey for developers* and *Salesforce survey for Mulesoft developers*. This chapter focuses mainly on *Salesforce survey for developers* but highlights findings from *Salesforce survey for Mulesoft developers*. The idea is to examine the combined results of the two surveys and then examine whether Mulesoft developers have more security tools at their disposal by using the Mulesoft integration platform.

6.1 Analysis and profiling of Salesforce developers who responded to the survey

There were 22 responses from *Salesforce survey for developers* and 5 responses from *Salesforce survey for developers*. So, in total, there were responses from 27 individuals who were creating Salesforce integrations. Out of these 27 responses, 23 employer is the organisation that is a Salesforce partner, four can be described as in-house developers (Salesforce professionals working in an organisation that is using Salesforce), and one response is where the employer is an integration provider. The respondents had many job titles: 13 Salesforce developers, 5 Salesforce consultants, 4 Mulesoft developers, 2 Directors, 1 Salesforce architect, 1 Mulesoft integration architect, one integration specialist, and 1 integration consultant.

Responses were analysed by two different categorisations: information technology (IT) experience and the overall number of integrations a person has created. By information technology experience, four groups are 1 to 3 years, 4 to 10 years, 10 to 20 years and more than 20 years of experience. Interestingly all the groups contained a similar amount of responses.

Seven responses describe having 1 to 3 years of IT experience. 6 out of 7 respondents have worked only with Salesforce, and one has worked less than a year with Salesforce. In this group, Salesforce developers were the most dominant job title, with 71 % being Salesforce developers. 6 respondents are grouped to have 4 to 10 years of IT experience. Like the previous group, most respondents were Salesforce developers (67%). In this group, there seem to be only two respondents that have only worked with the Salesforce platform. The rest of the respondents had either less than a year or 1 to 3 years of Salesforce experience. 10 to 20 years of IT experience is the most significant group having 9 responses. This group has more mixed job titles among them, with 44% Salesforce developers, 22% Salesforce consultants, and 34% other job titles. One or zero respondents have worked their entire IT career on Salesforce. One of the respondents has worked on Salesforce for more than 10 years, 44% for 4 to 10 years and the rest have worked less than 3 years. The last group

is more than 20 years of experience. In this group, 6 respondents have worked either 4 to 10 years (50%) on Salesforce or 1 to 3 years.

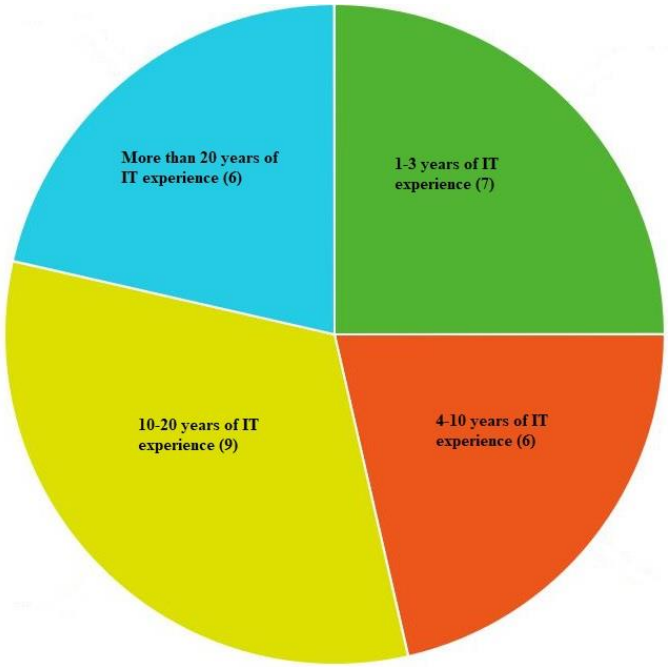

Figure 9: Years of information technology experience.

The second categorisation is the number of integrations a person has made. This includes all the integrations the person has made in their career. The first group is those who have created less than 5 integrations. This group consists of 9 responses. It is safe to assume that almost all of these integrations are created in Salesforce. The second group consist of respondents that have created 6 to 10 integrations 7 respondents in this group. Among them, there are only two whom we can assume to have created all these integrations on Salesforce. The rest of the respondents in this group have created less than 5 Salesforce integrations. The third group are those who have created 11 to 50 integrations. There is only one response where the amount of integrations is 31 to 50 and four 11-30, so combining these two into one group was clear. 60% of the respondents have created all their integrations in Salesforce. The last group contained those who had created more than 50 integrations. All of these have created only a tiny portion of the integrations as Salesforce-related integrations. However, it is essential to note that people in this group have created more Salesforce integrations than people in the other groups. Most of this group's respondents (71%) have created almost all Salesforce-related integrations using some integration platform.

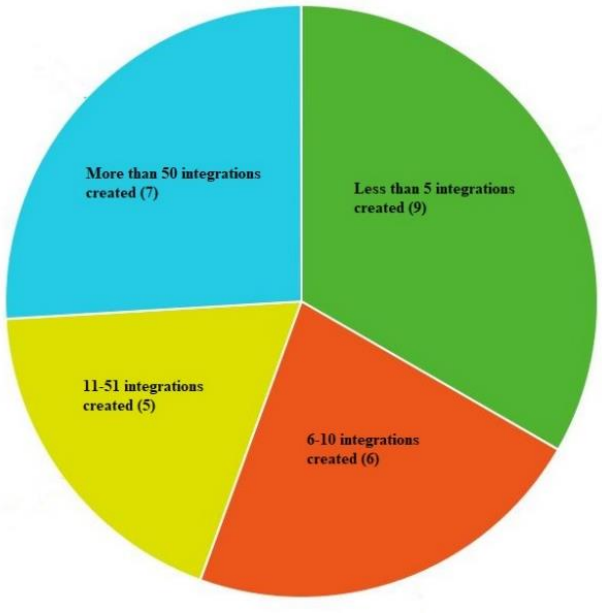

Figure 10: Number of integrations a person has made.

While going through the results and responses from Mulesoft developers are creating one individual group, which will be compared to other results. This will highlight whether there are differences in weather integrations are created with the integration platform or not.

There is a clear correlation between the IT experience and the number of integrations made. However, interestingly there was not as much correlation between Salesforce experience and Salesforce integrations people have made. This shows that those who create Salesforce integrations are not often the most experienced Salesforce professionals. However, those who create a lot of (more than 10) Salesforce integrations have, with few exceptions, at least 4 to 10 years of IT experience. Another thing to highlight is that those who have created more than 10 Salesforce integrations have created at least 11 to 30 integrations.

6.2 Results

In this chapter, we go through all the questions split into three categories: Integration security knowledge, Responsibilities to create secure integrations, and best practices to ensure integration security. In each section, both categories' information technology experience and the overall amount of integrations are used to go through the results. This section also highlights lessons learned from *Salesforce survey for Mulesoft developers*.

6.2.1 Integration security knowledge

Table 5 display how responses from *Salesforce survey for developers* average scores were divided between different groups. Table 6 shows similar like table 5, but using a number of integrations created categorisation. Average scores were calculated from all the responses to individual questions by each group. Average scores are using scale 1 to 4 where 1 is "*strongly disagree*" and 4 is "*strongly agree*".

All groups in both categorisations agree that integrations are essential to Salesforce. This result aligns with the assumption that Salesforce integrations are present in most Salesforce instances. The results also highlight the importance of this research. For example, it is safe to assume that other CRM platforms than Salesforce also have many integrations created between them and third-party applications.

Like excepted, experience and amount of integrations individual have created correlate with the security knowledge. Those who have 1 to 3 years of experience somewhat disagreed that they are aware of security threats related to Salesforce integrations. They also somewhat disagreed on whether they knew how to create secure integrations. Interestingly, one respondent thought he completely understands different security threats and knows how to create secure integrations. This participant was the only one in the group working for the organisation using Salesforce.

The second group, those with an average of 4 to 10 years of experience, saw they somewhat disagreed on knowing different security threats integrations have. Although this, they were rated on the high end of the scale, whereas the group containing 1 to 3 years of experience was at the low end, almost disagreeing. 4 to 10 years of experience group thought that even though they did not understand all the different threats, they felt capable of creating secure integrations.

10 to 20 years of experience was interestingly most awakened on integration security matters. By looking into their averages, they thought they somewhat agreed by knowing the different threats integrations face. They also agreed that they know how to create secure integrations. This group contained the highest percentage of respondents that are using integration platforms. In addition, 55% have created at least 76% and 10%, approximately a fourth of the integrations using some integration platforms. This alone highlights a correlation between integration security knowledge and using integration platforms to create integrations. With more than 20 years of experience group somewhat agreed that they understand different security threats related to integrations and had a similar average on creating secure integrations.

Against presumptions, the most amount of experience did not completely correlate to the security knowledge. The group that seems to have the highest level of integration security knowledge is, in fact, the group where participants have 10 to 20 years of experience. This group had the same knowledge about integration security threats and creating secure integrations as Mulesoft developers.

All groups agreed that information security needs to be considered while creating integrations. However, only the group containing participants with 1 to 3 years of experience barely agreed with the statement. Other groups, including Mulesoft developers, were closer to strongly agreeing than somewhat agreeing.

When looking at integration security knowledge with the amount of created integrations point of view, the results show a similar correlation to years of experience. Those who have created less than 5 integrations are somewhat disagreeing that they know different integration security threats and how to create secure integrations. Groups where participants are created 6 to 10 or 11 to 50 integrations somewhat agree on both statements. Those who have created more than 50 integrations and Mulesoft developers somewhat agree on knowing different integration security threats and how to create secure integrations.

Years of experience	Amount of responses	Integrations are an essential part of Salesforce	I am aware of different kinds of Information Security threats related to Salesforce integrations	I am aware of what information security considerations need to be taken into account when creating integrations.	When creating integrations Information Security is something that needs to be considered.
1-3 years of experience	7.00	5.43	3.00	3.57	5.00
4-10 years of experience	6.00	5.17	3.67	4.67	5.83
10-20 years of experience	9.00	5.67	4.67	5.44	5.89
20+ years of experience	6.00	5.50	5.44	4.17	5.67

Table 5: Responses related to integration security knowledge using years of experience categorisation. Average scores between 1 and 6 (1 = Strongly disagree, 2 = Disagree, 3 = Some what disagree, 4 = Some what agree, 5 = Agree, 6 = Strongly agree).

Amount of integrations created	Amount of responses	Integrations are an essential part of Salesforce	I am aware of different kinds of Information Security threats related to Salesforce integrations	I am aware of what information security considerations need to be taken into account when creating integrations.	When creating integrations Information Security is something that needs to be considered.
< 5	9.00	5.44	3.22	3.89	5.78
6-10	7.00	5.43	4.14	4.43	5.29
11-50	5.00	5.20	4.00	4.00	5.80
50+	7.00	5.71	4.43	5.29	5.86

Table 6: Responses related to integration security knowledge using amount of integrations created categorisation. Average scores between 1 and 6 (1 = Strongly disagree, 2 = Disagree, 3 = Some what disagree, 4 = Some what agree, 5 = Agree, 6 = Strongly agree).

6.2.2 Responsibilities to create secure integrations

In this chapter we go trough how developers see the responsibilities of different stakeholders. Sample and how the questions were averaged by the groups and categorisations is shown in a table 7 and table 8.

There were some exciting results when looking at how developers see different stakeholders' responsibilities on integration security. With less experience, the individual is more likely to see that most of the different stakeholders are mainly responsible. For example, a group containing 1 to 3 years of experience thought that five out of six different stakeholders have main responsibility. In other groups, the number of stakeholders having main responsibility was four, and with Mulesoft developers, it was two.

All groups agreed that developers have the main responsibility for what comes with creating secure integrations. Fewer integrations individual has made it more likely they think that the main responsibility lies on organisations. With years of experience, those who have 1 to 3, 10 to 20, and more than 20 years of experience think that organisation has the main responsibility. Other groups, including Mulesoft developers, think that the organisation has some responsibility.

Third-party software providers' responsibility was seen as the main responsibility of only those who have created 10 or fewer integrations or 10 or fewer years of experience. Others saw that third-party software provider has some responsibility. Interestingly while other groups thought that Salesforce had some responsibility, only in the group where individuals have 1 to 3 years of experience Salesforce was seen to have the main responsibility. In this group, 86% of respondents thought that Salesforce had the main responsibility. This indicates that those with less experience think that the platform provider, in this case, Salesforce, is responsible for ensuring the security of integrations. Those who have created 10 or fewer integrations agreed that the main responsibility lies in Salesforce, even though the result was not as straightforward as within 1 to 3 years of experience group. The rest of the groups in both categorisations thought that Salesforce had some responsibility.

Corporate information security (CIS) was seen to have the main responsibility. Only Mulesoft developers thought that this was not the case, and they saw CIS as having some responsibility. Lastly, when analysing results on how responsible partner or system integration was seen to be, there was a clear indication that it is seen to have main responsible. Interestingly, only one group thought that partner or system integrator does not have the main responsibility. This group contained those who have 1 to 3 years of experience. They thought that partners or system integrators had some responsibility. These are interesting results because all but one respondent in this group worked for a

Salesforce partner. The one in this group working for an organisation using Salesforce disagreed with the rest of the group, thinking that the partner or system integrator has the main responsibility.

When looking at the average scores of each group in experience categorisation, all groups except 1 to 3 years of experience think that developers are the most responsible stakeholder out of everyone else. A group of respondents with 1 to 3 years of experience think that Salesforce is the most responsible stakeholder. There is a clear correlation between experience and the amount of integrations individual has created and how they see the responsibility of third-party software provider and Salesforce. With more experience and integrations, you have created less responsibility and shift towards third-party software providers and Salesforce.

Years of experience	Amount of responses	Developer	Organisation using Salesforce	Third-party software provider	Salesforce	Corporate Information Security	Partner / System Integrator
1-3 years of experience	7.00	1.71	1.86	1.43	1.14	1.71	2.00
4-10 years of experience	6.00	1.33	2.00	1.50	2.17	1.67	1.67
10-20 years of experience	9.00	1.44	1.44	2.00	2.00	1.78	1.67
20+ years of experience	6.00	1.33	1.83	2.33	2.33	1.67	1.50

Table 7: Responses related to responsibilities using years of experience categorisation. Average scores between 1 and 4 (1 = Main responsibility, 2 = Some responsibility, 3 = Little responsibility, 4 = No responsibility).

Amount of integrations created	Amount of responses	Developer	Organisation using Salesforce	Third-party software provider	Salesforce	Corporate Information Security	Partner / System Integrator
< 5	9.00	1.67	1.67	1.44	1.56	1.67	1.89
6-10	7.00	1.43	1.57	1.57	1.71	1.57	1.86
11-50	5.00	1.20	2.00	2.60	2.60	2.00	1.60
50+	7.00	1.43	1.86	2.00	2.00	1.71	1.57

Table 8: Responses related to responsibilities using amount of integrations created categorisation. Average scores between 1 and 4 (1 = Main responsibility, 2 = Some responsibility, 3 = Little responsibility, 4 = No responsibility).

6.2.3 Best practices to ensure integration security

Table 9 shows how the best practice answers were split. There were 11 different answers chosen between all different groups and categorisations. *Auditing third-party software security*, *extensive testing*, *monitoring integrations*, *and searching best practices* made a clear top four on the list with both categorisations. With the different categorisations, there were almost no differences between the two. When looking at different groups, there were some interesting differences between the groups. Most interesting is that 43% of those belonging to the group where individuals have 1 to 3 years of experience, and 44% of those who have created less than five integrations, thought that encouraging organisations using Salesforce to take care of the security was one of the three choices.

Those with more than 20 years of experience seem to rely less on auditing the security of third-party software than other groups. However, they rely more on monitoring integrations and creating their own set of validations than other groups.

Group 1 to 3 years of experience most selected choice was *auditing security of third-party software*, and *extensive testing*, *encourage organisation using Salesforce to take care of it*, and *searching best practices* were tied to second place. 4 to 10 years of experience group had *auditing security of third-party software* and *extensive testing* tied on a first place, and *monitoring integrations* on a third place. 10 to 20 years of experience group had *auditing security of third-party software* and *searching for best practices* in the first place, and *monitoring integrations* in a third place. More than 20 years of experience group had *monitoring integrations* first, *extensive testing* second, and *creating its own set of validations* and *searching best practices* on third place. With Mulesoft developers *auditing security of third-party software* and *extensive testing* got first place, and *monitoring integrations* and *following Mulesoft's designing and building patterns* were in third place.

Results show that developers are pretty much in the same place on what comes to ensuring the security of integrations. We saw few differences in the responses, but overall, the responses were in line between different groups and categorisations.

	years of experience					Amount of integrations created					
	1 to 3	4 to 10	10 to 20	20+	All	< 5	6 to 10	11 to 50	50+	Overall	Mulesoft
Auditing security of third-party software	6	5	4	1	16	5	4	3	3	15	3
Extensive testing	3	5	2	3	13	5	2	4	5	16	3
Monitoring integrations	2	3	3	4	12	5	5	3	3	16	2
Making sure configuration properties sensitive data are secure and encrypted	1	0	0	0	1	1	0	0	0	1	0
Using solutions found from AppExchange	2	1	2	1	6	3	3	1	1	8	1
Encourage organisation using Salesforce to take care of it	3	1	1	0	5	4	2	0	0	6	0
Creating own set of validations	1	1	0	2	4	0	2	0	2	4	1
Asking about the security from a third-party software provider	1	1	0	1	3	0	2	0	1	3	1
Searching best practices	3	1	4	2	10	4	2	3	4	13	1
Good surrounding architecture which looks at things end-to-end, and not just individual responsability	0	0	1	0	1	0	0	0	1	1	1
Following MuleSoft's designing and building patterns	0	0	1	1	2	0	0	1	1	2	2

Table 9: How best practices are split.

6.2.4 Lessons learned from Mulesoft developers

When looking into the results, responses from the *Salesforce survey for Mulesoft developers* are primarily in line with those from the *Salesforce survey for developers*. Overall, all the Mulesoft developers, except one that responded to the survey, have a lot of IT experience and have created more than 30 integrations during their careers. 60% of Mulesoft developers responding to the survey have 4 to 10 years of Mulesoft experience, and the rest of them have less than 1 year of experience with the platform. Four out of five Mulesoft developers have worked with Salesforce for less than four years. The explanation for the fact that Mulesoft developers have worked quite a small portion of their career with the Salesforce platform is that Mulesoft was bought by Salesforce in March 2018

(Miller 2018). Since then, Mulesoft's role in Salesforce integrations has grown rapidly and is estimated to be an even more essential part of Salesforce integrations in the future (Knapp 2018).

Mulesoft developers seem more familiar with the security aspects of integrations than those with more than 10 years of experience. When looking at the number of integrations, results show that Mulesoft developers align with those who have created more than 50 integrations. With this information, it is safe to state that the results of this research Mulesoft platform provides a good knowledge base on security matters and ensures that Mulesoft developers know how to create secure integrations. Mulesoft developers also somewhat agree that integration security is guaranteed when following Mulesoft designing patterns. Mulesoft developers also brought up that *following MuleSoft's designing and building patterns* is one of the best practices they use to ensure the security of integrations. This outlines findings in the literature that was brought up in chapter 4.5.1. Mulesoft has excellent tools and features that help to ensure integration security.

Interestingly Mulesoft developers disagreed on the responsibility of Mulesoft. There were two responses where Mulesoft was seen to have little responsibility and two where it was seen to have main responsibility when creating integration security. It would be interesting to study this further to see whether the same result could be obtained with the larger sample.

6.3 Summary

Overall, when looking into the results, information technology experience and the number of integrations individuals have created give quite similar results. There is a clear correlation between experience and security knowledge. Where the responsibility lies when taking a look at the responsibility of different stakeholders seems to be similar with different groups. However, there were some interesting differences. First, it is important to bring up that even though there were some differences, all responses were inside of a small margin. This shows that formatting the question about the responsibilities could have been done better. The problem with the responsibility question was that either scale was too narrow, or respondents should be made to choose to rate responsibility on a scale where only one stakeholder could be assigned to one responsibility category. The way the question was formatted made analysis hard because respondents could choose all stakeholders to have the main responsibility. This also applies to *Salesforce survey for organisations*.

There is seen some lack of security knowledge among those with less than four years of experience. People in this group also think that other stakeholders are more responsible for the security of integrations than them. This changes when we take a look at developers that have more than 3 years of experience. This should be addressed in all organisations because individuals who

belong to this group are, in some cases, creating a lot of integrations. 43% of the people in this group have already, early in their career, created more than 5 integrations.

When individuals have more than 10 years of experience, their security knowledge seems to take the biggest leap among the different groups. Also, when a person has created more than 5 integrations, their security knowledge increases. This is good news because it indicates that with more experience in integrations, more security knowledge individuals have. However, especially Salesforce partners should educate new comers more on security-related matters. Creating secure integrations early on in the career is not only in a customer's best interest but also helps the new developers to create security habits. If security is not considered early on, there is a change that developer creates habits that are hard to change later on in their career. These habits can make one not concerned with security at all, creating significant security risks for the customer's systems. (Ransome, Schoenfield & Schmidt 2014, p. 3-6, p. 314-320).

Results show that making sure that third-party software itself is one of the most important practices to ensure integration security. This implies that auditing, testing or at least asking the third-party software provider about their software's security should be seen as a high priority. While developing integrations, developers tend to search for best security practices online. This is a good habit to have because someone has probably solved and thought about the same problem earlier. This means that somewhere in the depths of internet, there is a proven solution. Developers only need to find it. Testing the integration and also monitoring it is also a great habit of making sure that everything runs as it should. Monitoring is also something where integration platforms, such as Mulesoft, can add much value. Many integration platforms have built-in monitoring tools, and developers should leverage these capabilities. (Knapp 2018; Seth 2018). Developers that are not working with any integration platform should think about how they can monitor the integrations they create. Maybe create custom solutions, find pre-build solutions from AppExchange or leverage functionalities that Salesforce offers.

Developers should be careful about excepting organisations to take care of the security. As we can see in the results of *the Salesforce survey for organisations* there are some organisations that are capable of taking care of security by themselves. However, there are much more organisations that are not equipped to do so or lack security knowledge or integration development knowledge. One open answer of the *Salesforce survey for developers* brings up that social engineering is one of the most dominant attack vectors, which is true. Especially educating Salesforce users on security precautions should be the organisation's responsibility. Besides social engineering, there are also other attack vectors and covering them should be the responsible of those who develop integrations (Ransome, Schoenfield & Schmidt 2014, p. 10-11, p. 66-73, p. 264-269).

One way to increase developers' security knowledge is to implement the SDL concept at the organisation level. The weather this means customer organisation or Salesforce partner organisation with SDL principles, it would be more clear for developers to recognise different stages of integration development and what is their responsible at each stage. Chapter 4.3 highlighted the benefits and features SDL bring. In Chapter 7 we show an example by using SDL to show how security responsibilities can be simplified and documented.

7 Discussion

In this chapter, we wrap up the research and all the results. This chapter also highlights how literature and survey respondents see responsibilities in creating secure Salesforce integrations. Chapter 7.2 brings up best practices for the organisations and chapter 7.3 for the developers to ensure Salesforce integration security.

7.1 Responsibilities to ensure integration security

When creating integrations, there are laws, regulations and standards that organisations need to follow. Organisations are responsible is to follow these precautions. Organisations are also the one that is accountable to their customers and clients if the information is leaked or integrations are not created by following laws and regulations. With NDAs and other agreements, organisations can shift responsible towards partners and developers, but in case of a breach, the public opinion will most likely be that organisation is responsible. This implies that organisations need to take ownership of the integrations and ensure that everyone creating integrations to the Salesforce instance is following security best practices. The study conducted for this research shows that organisations see themself, including Corporate Information Security and security personnel, to have the highest responsibility for making integrations secure. Interestingly developers saw that developers are the stakeholder most responsible for making integrations secure.

Interestingly hypothesis of this research was not correct. This study shows that, unlike this research's hypothesis, organisations and developers see themself to be the most responsible stakeholder in making integrations secure. This is a good result because it implies that both sides of the coin are taking ownership of the security. Ilmarinen and Koskela (2015, p. 155-159) argued that security is everyone's responsibility. It does not matter whether you are an organisation's security personnel, developer or user you need to make sure that you are not the weakest link in what comes about security.

One thing this research did not cover is how third-party software providers see their responsibility. Both organisations and developers thought that third-party software providers had at least some responsibility. It would be interesting to compare third-party software providers' thoughts on where they see the responsibility lies and how much different stakeholders have responsibility for making integrations secure.

7.2 Best practices for the organisations

Organisations, most importantly, need to ensure that they have an information security policy (ISP) which includes integration security and that ISP is followed by everyone. One way to approach this is to include the CRM security management system (CRM-SMS) in the ISP or have it as a separated document (Seify 2006, p. 440-445). Seify (2006, p. 440-445) bring up that CRM-SMS contains five risk management paradigms which are *"determining organisational CRM security objectives, strategies, and policies"*, *"identifying and analysing the security threats to, and vulnerabilities of the assets of CRM systems within the organisation"*, *"implementing CRM security plan"*, *"developing and implementing CRM security awareness and training program"*, and *"following up the CRM security plan"*. With CRM-SMS, organisations will have a clear idea of their Salesforce infrastructure security and the security level it has. CRM-SMS also includes risk management with the following eight steps "*gathering Information, analysing Gap, identifying the security requirements, making decision for the baseline or detailed risk assessment, assessing the baseline, assessing the detailed risk, selecting the controls and finally reviewing and reforming CRM security policy and strategy"* (Seify 2006, p. 440-445). CRM-SMS should be in line with ISP, and when done properly, it will also include an integrated security management aspect in the Salesforce context.

Among already brought up, organisations value ensuring that third-party software is secure and integrations are monitored and tested extensively. This research brought up that Mulesoft has built in monitoring tools. There are also different ways to monitor incoming and outcoming information flow within Salesforce. This can be as simple as monitoring changes within records by using standard Salesforce features highlighted in chapter 3.3. To extend the organisation's knowledge about integrations they have and how they process data, there should be comprehensive documentation about the integrations. This documentation should also include the results of security testing.

Organisations should also increase their Salesforce security knowledge. There are great trails, webinars, and blogs from Salesforce, which should be mandatory for all security experts and Salesforce admins in the organisation (Salesforce Trust 2022).

Best practices for organisations are implementing security knowledge on all levels and having comprehensive policies and documentation that those who create Salesforce integrations need to follow. Especially small organisations and organisations that do not have security personnel could benefit from having information security consulting to create these policies and documentation and offer employees information security training.

7.3 Best practices for the developers

Developers are in charge of creating integrations. Because developers have the knowledge and skills to create integrations, it should also be their responsibility to create integrations by following security standards and best practices. Part of being a developer is to make sure that knowledge is not outdated. Developers should follow security, especially Salesforce integration security-related publications and guidelines, to keep up with the security standards. Salesforce provides excellent tools and features which can add to the security of integrations. All developers that create Salesforce integrations should know how to implement these tools and features on the organisation's Salesforce instance. How to manage the integration of users and profiles? How to monitor integrations? What is the level of access each integration needs, and how it controls that integration can access only the data it needs to be able to? These some of the are questions developers need to have answers to. It is essential to understand that developers need to take main responsibility for the Salesforce integrations even though there are no agreements or discussions about security from the organisation's side. Organisations and Salesforce partners need to ensure that there is proper support for the developers to create security within their integrations.

One way for developers to ensure security is considered is to follow secure development lifecycle (SDL) practices. SDL provides comprehensive security practices, which can be used as a *checklist* to ensure all security precautions are considered. In chapter 4.3.1, this research brought up all the key features of SDL and how it could be implemented. Especially Salesforce partners should use SDL to implement security on all the development and as a guide to training new developers. This study showed that those who do not have as much experience in information technology or with integration development do not have enough knowledge about integration security.

Best practices for the developers include security knowledge about common threats on Salesforce integrations, design patterns to ensure secure development, and ensuring that every Salesforce integration is monitored and tested. The biggest challenge for the developers is that they usually work under a deadline, and there is not enough time for security and extensive testing. This is something that needs to change in order to enable developers to create more secure integrations.

7.4 Conclusion

The world is becoming more digital each day. Since customers and competitors are online, organisations are forced to take digital leaps to stay relevant. This makes many organisations search best-suited customer relationship management system to add to their information technology infrastructure. As highlighted in this research Salesforce is one of those platforms. Salesforce's

capabilities to provide security features and high customizability, on top of CRM functionalities, are why many organisations choose Salesforce.

This research went through features that create Salesforce's security. Cloud computing infrastructure with all the typical security features and the Salesforce platform's security controls provide a great layer of security for organisations using Salesforce. However, integrations can create different vulnerabilities for the organisations. At Salesforce, integrations are commonly either processing and providing information for the third-party software or taking data to form third-party sources and storing it into Salesforce. If the third-party software, or integration is exploited, the malicious actor can violate the confidentiality and integrity of the information stored in Salesforce.

This research shows that enabling standard Salesforce functionalities will add security of Salesforce instance. Auditing capabilities ensure that Salesforce instance is monitored and all actions and changes in Salesforce are logged. Organisations and developers need to create an architecture where integrations have access to only the necessary data. Also, following best practices such as creating integration dedicated user profiles for the integrations to use and implementing authentication and login policies to those user profiles is much needed. As in Mulesoft, implementing monitoring capabilities to see what each integration is doing should be something that all Salesforce instances and developers aim to achieve. On top of standard functionalities, different AppExchange products should be leveraged to provide extra layers of security within Salesforce.

This research included a study where organisations using Salesforce, Salesforce developers and Mulesoft developers were asked about integration security and responsibilities related to the integration security. The studies show that all parties are taking ownership of ensuring security. Organisations state that it is mainly their responsibility, and developers see it as theirs. By looking at results conducted with the studies, we can see that small organisations' Salesforce integrations made by inexperienced developers are the most vulnerable. Another key finding was that organisations do not have integrations included in their ISP. This should be addressed and fixed in all organisations. Those organisations that do not have ISP at all should create one. Also, obligating developers to be familiar with the organisation's ISP and follow regulations and standards brought up in the ISP.

The major drawback of this research was the sample size. Especially the small sample of organisations means that results cannot be generalised. There were also design flaws in the survey. Questions about responsibilities should have been created so that differences between stakeholders would have come out more clearly. Also, the lack of research on integration security created some challenges for this research. Without a doubt there is need for further research. Future research could

be done by investigating whether findings in this research can be verified with a larger sample. Also, there seems to be a need for studies exploring actions different stakeholders do while creating integrations.

References

Arora, A. & Gupta, A. (2013). Force.com tips and tricks. Packt Publishing.

Bass, J. M.; Beecham, S. & Noll, J. (2018). Experience of Industry Case Studies: A Comparison of Multi-Case and Embedded Case Study Methods. 2018 IEEE/ACM 6th International Workshop on Conducting Empirical Studies in Industry (CESI), pp. 13-20. ISBN: 978-1-4503-5736-4

Barona, R. & Anita, E. A. M. (2017). A survey on data breach challenges in cloud computing security: Issues and threats. 2017 International Conference on Circuit, Power, and Computing Technologies (ICCPCT), pp. 1-8, doi: 10.1109/ICCPCT.2017.8074287.

BSI (24.09.2022). ISO/IEC 27018 Safeguarding Personal Information in the Cloud. BSI Group. Whitepaper:https://www.bsigroup.com/Documents/iso-iec-27018/ISOIEC-27018-Safeguarding-information-in-the-cloud-whitepaperDec2015.pdf – Sited 24.09.2022

BSIMM (24.08.2022). BSIMM12 2021 Insights & trends report. https://www.bsimm.com/content/dam/bsimm/reports/bsimm12.pdf

BT group (2021). CISOs under the spotlight. BT group. Whitepaper. https://www.globalservices.bt.com/en/forms/cisos-under-the-spotlight-whitepaper - Sited 23.09.2022

Coltman, T. R. (2006). "Where Are the Benefits in CRM Technology Investment?" Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06), 2006, pp. 111c-111c, doi: 10.1109/HICSS.2006.535.

Fawcett, Andrew (2014). Force.com Enterprise Architecture. Packt Publishing. ISBN:

1-78217-299-8

FMD group (16.09.2022). What is a Salesforce Developer? FMD group. Blog - Sited 16.09.2022.

Gupta, R.; Verma, S. & Janjua, K. (2018). "Custom Application Development in Cloud Environment: Using Salesforce," 2018 4th International Conference on Computing Sciences (ICCS), 2018, pp. 23-27, doi: 10.1109/ICCS.2018.00010.

Ilmarinen, V. & Koskela, K. (2015). Digitalisaatio: Yritysjohdon käsikirja (1. edition.). Talentum.

International Organization for Standardization. (2013). Information technology — Security techniques — Information security management systems — Requirements (ISO/IEC 27001:2013) https://www.iso.org/standard/54534.html

International Organization for Standardization. (2014). Asset management — Overview, principles, and terminology (ISO Standard No. 55000:2014).

https://www.iso.org/standard/55088.html

International Organization for Standardization. (2014). Asset management — Management systems — Requirements (ISO Standard No. 55001:2014).

https://www.iso.org/standard/55089.html

International Organization for Standardization. (2015). Quality management systems — Requirements (ISO Standard No. 90001:2015).

https://www.iso.org/standard/62085.html

International Organization for Standardization. (2016). Petroleum, petrochemical, and natural gas industries — Collection and exchange of reliability and maintenance data for equipment (ISO Standard No. 14224:2016). https://www.iso.org/standard/64076.html

International Organization for Standardization. (2018). Asset management — Management systems — Guidelines for the application of ISO 55001 (ISO Standard No. 55002:2018). https://www.iso.org/standard/70402.html

International Organization for Standardization. (2018). Industrial automation systems and integration — Integration of life-cycle data for process plants including oil and gas production facilities — Part 13: Integrated asset planning life-cycle (ISO Standard No. 15926-13:2018). https://www.iso.org/standard/70694.html

Jiang, Y. (2009). "Integration of CRM and ERP in E-Commerce Environment," 2009 International Conference on Management and Service Science, 2009, pp. 1-4, doi: 10.1109/ICMSS.2009.5303269.

Kashivskyy, Adrian (2015). Imperative vs. Declarative Programming - Pros and Cons. Netguru. Online article: https://www.netguru.com/blog/imperative-vs-declarative - Sited 13.07.2022.

Knapp, Kristin (2018). Mulesoft. TechTarget. Online article: https://www.techtarget.com/searchcloudcomputing/definition/Mulesoft - Sited 21.07.2022

Kovacs, Eduard (2021). Companies Still Exposing Sensitive Data via Known Salesforce Misconfiguration. Securityweek. Article: https://www.securityweek.com/companies-still-exposing-sensitive-data-known-salesforce-misconfiguration?&web_view=true

Lakaniemi, Ilkka (2014). Digitalisaatio keskisuurissa yrityksissä. Liikenne- ja Viestintäministeriön julkaisuja 14/2014. Liikenne- ja Viestintäministeriö. ISBN: 978-952-243-399-2

Li, Jin; Chen, Jinfu; Huang, Minhuan; Zhoum, Minmin; Xie, Wanggen; Zeng, Zhifeng; Chen, Shujie & Zhang, Zufa (2018). "An integration testing framework and evaluation metric for vulnerability mining methods," in China Communications, vol. 15, no. 2, pp. 190-208, Feb. 2018, doi: 10.1109/CC.2018.8300281.

Liu, X. & Pang, J. (2009). "Application of the Integration for ERP and CRM Based on EJB-JMS and XML," 2009 International Symposium on Computer Network and Multimedia Technology, 2009, pp. 1-4, doi: 10.1109/CNMT.2009.5374617.

Loshin, Paul (2022). object. TechTarget. Online article: https://www.techtarget.com/searchapparchitecture/definition/object - Sited 12.07.2022.

Mainka, C.; Mladenov, V. & Schwenk, J. (2016). "Do Not Trust Me: Using Malicious IdPs for Analyzing and Attacking Single Sign-on," 2016 IEEE European Symposium on Security and Privacy (EuroS&P), 2016, pp. 321-336, doi: 10.1109/EuroSP.2016.33.

Manchar, A. & Chouhan, A. (2017). "Salesforce CRM: A new way of managing customer relationship in cloud environment," 2017 Second International Conference on Electrical, Computer and Communication Technologies (ICECCT), 2017, pp. 1-4, doi: 10.1109/ICECCT.2017.8117887.

Metazoa (14.07.2022). Org Security Center. https://www.metazoa.com/org-security-center/

Microsoft (24.08.2022). What are the Microsoft SDL practices? https://www.microsoft.com/en-us/securityengineering/sdl/practices

Miller, Ron (2018). Salesforce is buying Mulesoft at enterprise value of $6.5 billion. Tech Crunch. Online article: https://techcrunch.com/2018/03/20/salesforce-is-buying-Mulesoft-at-enterprise-value-of-6-5-billion/ - Sited 25.09.2022

Mulesoft (21.07.2022). Mulesoft Anypoint Platform. https://www.Mulesoft.com/

Mydyti, H.; Ajdari, J. and Zenuni, X. (2020). "Cloud-based Services Approach as Accelerator in Empowering Digital Transformation," 2020 43rd International Convention on Information, Communication and Electronic Technology (MIPRO), 2020, pp. 1390-1396, doi: 10.23919/MIPRO48935.2020.9245192.

Nachimuthu, N. (2021). Hands-On Mulesoft Anypoint Platform Volume 1: Designing and Implementing RAML APIs with Mulesoft Anypoint Platform (English Edition). BPB Publications, 2021. ISBN: 9389898234

Naeem, Tehreem (2019). Create a Unified View of Your Customer Data with Salesforce Integration Tools. Astera. Online article: https://www.astera.com/type/blog/salesforce-integration-tools/ - Sited 21.07.2022

NIST (24.08.2022). Secure Software Development Framework SSDF. https://csrc.nist.gov/Projects/ssdf

OWASP (24.08.2022). OWASP SAMM. https://owaspsamm.org/

OwnBackup. Data security. https://www.ownbackup.com/products-data-security/

Paige, Kevin (2018). It's time for a new security model. Mulesoft Blog. Online article: https://blogs.Mulesoft.com/api-integration/security/its-time-for-a-new-security-model/ - Sited 21.07.2022

Patel, J. & Chouhan, A. (2016). "An approach to introduce basics of Salesforce.com: A cloud service provider," 2016 International Conference on Communication and Electronics Systems (ICCES), 2016, pp. 1-8, doi: 10.1109/CESYS.2016.7889991.

Patel, J. & Chouhan, A. (2017). "An integration of salesforce.com with Twitter: A case of AppExchange," 2017 Second International Conference on Electrical, Computer and Communication Technologies (ICECCT), 2017, pp. 1-6, doi: 10.1109/ICECCT.2017.8117882.

Ransome, J. F., Misra, A., Schoenfield, B. & Schmidt, H. A. (2014). Core software security: Security at the source. CRC Press, Taylor & Francis Group.

Renwick, Priscila (2022). Ultimate Introduction to Salesforce Integration. SalesforceBen. Online article: https://www.salesforceben.com/salesforce-integration/ - Sited 21.07.2022

Rittinghouse, J. W. & Ransome, J. F. (2009). Cloud Computing. CRC Press.

Rodgers, Georgina (2021). The top Salesforce integration tools. Rapidi. Online article: https://www.rapidionline.com/blog/top-salesforce-integration-tools - Sited 21.07.2022

Rot, A. and Sobinska, M. (2020). "Challenges for Knowledge Management in Digital Business Models," 2020 10th International Conference on Advanced Computer Information Technologies (ACIT), 2020, pp. 555-558, doi: 10.1109/ACIT49673.2020.9208867.

Salesforce Trust (24.09.2022). Security for Administrators. Salesforce Trust, Salesforce. Online link: https://security.salesforce.com/security-for-administrators - Sited 24.09.2022

Saxena, A.; Sengupta, S.; Duraisamy, P.; Kaulgud, V. & Chakraborty, A. (2013). "Detecting SOQL-injection vulnerabilities in SalesForce applications," 2013 International Conference on Advances in Computing, Communications, and Informatics (ICACCI), 2013, pp. 489-493, doi: 10.1109/ICACCI.2013.6637220.

Seify, M. (2006). "New Method for Risk Management in CRM Security Management," Third International Conference on Information Technology: New Generations (ITNG'06), 2006, pp. 440-445, doi: 10.1109/ITNG.2006.99.

Seth, M. (2018). "Mulesoft – Salesforce Integration Using Batch Processing," 2018 5th International Conference on Computational Science/ Intelligence and Applied Informatics (CSII), 2018, pp. 7-14, doi: 10.1109/CSII.2018.00009.

Singh, A.; Sharma, S.; Kumar, S. R. & Yadav, S. A. (2016). Overview of PaaS and SaaS and its application in cloud computing. 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH), 2016, pp. 172–176.

Skyplanner (16.09.2022). What is a Salesforce Consulting Partner and How Can It Help You? Skyplanner. Blog - Sited 16.09.2022.

Soni, K. & Vala, B. (2017). "Roadmap to salesforce security governance & salesforce access management," 2017 Second International Conference on Electrical, Computer and Communication Technologies (ICECCT), 2017, pp. 1-4, doi: 10.1109/ICECCT.2017.8117831.

Statistics Finland (16.09.2022). Small and medium size enterprises. https://www.stat.fi/meta/kas/pienet_ja_keski_en.html

Tähtinen, Sami (2005). Järjestelmäintegraatio: Tarve, vaihtoehdot, toteutus. Talentum.

Ursillo, Steve JR. & Arnold, Christopher (2019). Cybersecurity is critical for all organisations - Large and Small. International federation of accountants, IFAC. Online article: https://www.ifac.org/knowledge-gateway/preparing-future-ready-professionals/discussion/cybersecurity-critical-all-organizations-large-and-small - Sited 23.09.2022

Violino, Bob (23.10.2022) 7 deadly sins of Salesforce security. CSO . Blog – Sited 23.10.2022

Vuong, J. & Braun, S. (2015). "Towards Efficient and Secure Data Storage in Multi-tenant Cloud-Based CRM Solutions," 2015 IEEE/ACM 8th International Conference on Utility and Cloud Computing (UCC), 2015, pp. 612-617, doi: 10.1109/UCC.2015.107.

Williams, D. (2014). Connected CRM: Implementing a big-data-driven, customer-centric business strategy. John Wiley & Sons, Inc.

WithSecure (14.07.2022). WithSecure Cloud Protection for Salesforce. https://www.withsecure.com/content/dam/with-secure/en/resources/withsecure-cloud-protection-salesforce-solution-overview-en.pdf.coredownload.pdf

Xiaoliang, Z.; Jinshui, W. & Kehe, W. (2014). "The study of bidding service cloud platform in power business expanding based on SaaS," 2014 IEEE 5th International Conference on Software Engineering and Service Science, 2014, pp. 492-495, doi: 10.1109/ICSESS.2014.6933613.

APPENDIX A – Salesforce survey for developers

Salesforce survey for developers

Empirical research for MSc thesis determine which actions Salesforce Developers are doing to ensure integrations are created safely regarding security. The survey response time is **16.08.2022 - 13.09.2022**.

Regarding integrations, integration means any connection that transfers data between Salesforce and third-party software. In the Salesforce context, this can mean, for example, DML operations (insert, update, upsert, delete) made from third-party software into the Salesforce or queries that provide information stored in Salesforce to the third-party software.
Third-party software means a computer program created or developed by a different organization than Salesforce and owned by others than Salesforce.

*Required

Scope of the study

I expect that the respondent has worked with or created at least one integration from Salesforce to third-party software. I also assume that the respondent is familiar with Salesforce and has worked with the platform.

This survey aims to provide base material for my MSc thesis about Salesforce integrations security. My MSc thesis will find out how integrations are managed and what actions developers and organisations are doing to achieve the security of the Salesforce instance. In my MSc thesis, I delimit Salesforce security as a whole to regard only integration and the threat they conduct to the overall security.

Terms and conditions

All the answers are anonymous, and they are handled anonymously. Therefore, I am not retaining or collecting any data that can identify individuals in this survey. All the answers are stored in Google Drive, which is used account provided by the University of Jyväskylä, and they will be deleted six (6) months after this survey is closed. Only the author of this MSc thesis (Musa Jallow) can see the answers as complete.

1. I agree to the terms and conditions *

Mark only one oval.

◯ Yes

General Information

2. Type of your employer *

Mark only one oval.

- ◯ Salesforce partner
- ◯ Organisation using Salesforce
- ◯ Salesforce
- ◯ Freelancer
- ◯ Other: _____

3. Job title *

Mark only one oval.

- ◯ Salesforce Developer
- ◯ Salesforce Consultant
- ◯ Admin User
- ◯ Project Manager
- ◯ Director
- ◯ Other: _____

4. Salesforce experience *

Mark only one oval.

- ◯ < 1 year
- ◯ 1-3 years
- ◯ 4-10 years
- ◯ 10+ years

5. Information technology experience *

Mark only one oval.

- ◯ < 1 year
- ◯ 1-3 years
- ◯ 4-10 years
- ◯ 10-20 years
- ◯ 20+ years

6. How many integrations have you created between Salesforce instance and third-party software? *

Mark only one oval.

- ◯ < 5
- ◯ 6-10
- ◯ 11-30
- ◯ 31-50
- ◯ 50+

7. What percentage of Salesforce-related integrations have you made using some integration platform (HiQ Frends, Dell Boom etc.)? *

Mark only one oval.

- ◯ 0 %
- ◯ 1-10 %
- ◯ 11-25 %
- ◯ 26-50%
- ◯ 51-75%
- ◯ 76-100%

8. How many integrations have you created, including no Salesforce-related ones (if any)?

Mark only one oval.

- ◯ < 5
- ◯ 6-10
- ◯ 11-30
- ◯ 31-50
- ◯ 50+

Salesforce Integrations

Statements that are answered on a scale 1-6 (1 = Strongly disagree, 2 = Disagree, 3 = Some what disagree, 4 = Some what agree, 5 = Agree, 6 = Strongly agree)

9. Integrations are an essential part of Salesforce. *

Mark only one oval.

	1	2	3	4	5	6	
Strongly disagree	◯	◯	◯	◯	◯	◯	Strongly agree

10. I am aware of different kinds of Information Security threats related to Salesforce integrations. *

Mark only one oval.

	1	2	3	4	5	6	
Strongly disagree	◯	◯	◯	◯	◯	◯	Strongly agree

11. I am aware of what information security considerations need to be taken into account when creating integrations. *

Mark only one oval.

	1	2	3	4	5	6	
Strongly disagree	◯	◯	◯	◯	◯	◯	Strongly agree

12. When creating integrations Information Security is something that needs to be considered. *

Mark only one oval.

	1	2	3	4	5	6	
Strongly disagree	◯	◯	◯	◯	◯	◯	Strongly agree

13. When creating integrations, there are different stakeholders involved in the process. Rate each stakeholder's role when making integration secure. (1 = Main responsibility, 2 = Some responsibility, 3 = Little responsibility, 4 = No responsibility) *

Mark only one oval per row.

	1 Main responsibility	2 Some Responsibility	3 Little responsibility	4 No responsibility
Developer	◯	◯	◯	◯
Organisation using Salesforce	◯	◯	◯	◯
Third-party software provider	◯	◯	◯	◯
Salesforce	◯	◯	◯	◯
Corporate Information Security	◯	◯	◯	◯
Partner / System Integrator	◯	◯	◯	◯

14. Choose 3 most valuable ways to ensure Information Security when creating integrations *

Tick all that apply.

- [ ] Using solutions found from AppExchange
- [ ] Creating own set of validations
- [ ] Creating support ticket to Salesforce
- [ ] Asking about the security from a third-party software provider
- [ ] Auditing security of third-party software
- [ ] Extensive testing
- [ ] Searching best practices
- [ ] Encourage organisation using Salesforce to take care of it
- [ ] Monitoring integrations
- [ ] Other: _____

15. Is there something else you would like to bring up?

APPENDIX B – Salesforce survey for MuleSoft developers

Salesforce survey for MuleSoft developers

Empirical research for MSc thesis to determine which actions MuleSoft Developers are doing to ensure integrations are created safely regarding security. The survey response time is **16.08.2022 - 13.09.2022.**

Regarding integrations, integration means any connection that transfers data between Salesforce and third-party software. In the Salesforce context, this can mean, for example, DML operations (insert, update, upsert, delete) made from third-party software into the Salesforce or queries that provide information stored in Salesforce to the third-party software.
Third-party software means a computer program created or developed by a different organization than Salesforce and owned by others than Salesforce.

*Required

Scope of the study

I expect that respondents have worked with or created at least one integration from Salesforce to third-party software by using MuleSoft. I also assume that respondents are familiar with Salesforce and have worked with the platform.

The aim of this survey is to provide base material for my MSc thesis about Salesforce integrations security. My MSc thesis will find out how integrations are managed and what actions developers and organisations are doing to achieve the security of the Salesforce instance. In my MSc thesis, I delimit Salesforce security as a whole to regard only integration and the threat they conduct to the overall security.

Terms and conditions

All the answers are anonymous, and they are handled anonymously. Therefore, I am not retaining or collecting any data that can identify individuals in this survey. All the answers are stored in Google Drive, which is used account provided by the University of Jyväskylä, and they will be deleted six (6) months after this survey is closed. Only the author of this MSc thesis (Musa Jallow) can see the answers as complete.

1. I agree to the terms and conditions *

Mark only one oval.

◯ Yes

General Information

2. Type of your employer *

Mark only one oval.

- ◯ Salesforce partner
- ◯ Organisation using Salesforce
- ◯ Salesforce
- ◯ Freelancer
- ◯ Other: _____

3. Job title *

Mark only one oval.

- ◯ Salesforce Developer
- ◯ Salesforce Consultant
- ◯ MuleSoft Developer
- ◯ Other: _____

4. Salesforce experience *

Mark only one oval.

- ◯ < 1 year
- ◯ 1-3 years
- ◯ 4-10 years
- ◯ 10+ years

5. MuleSoft experience *

Mark only one oval.

- ◯ < 1 year
- ◯ 1-3 years
- ◯ 4-10 years
- ◯ 10+ years

6. Information technology experience *

Mark only one oval.

- ◯ < 1 year
- ◯ 1-3 years
- ◯ 4-10 years
- ◯ 10-20 years
- ◯ 20+ years

7. How many integrations have you created between Salesforce instance and third-party software with MuleSoft? *

Mark only one oval.

- ◯ < 5
- ◯ 6-10
- ◯ 11-30
- ◯ 31-50
- ◯ 50+

8. How many integrations have you created, including no Salesforce and MuleSoft-related integrations(if any)?

Mark only one oval.

- < 5
- 6-10
- 11-30
- 31-50
- 50+

Salesforce Integrations

Väittämiä joihin vastataan asteikolla 1-6 (1 = Strongly disagree, 2 = Disagree, 3 = Some what disagree, 4 = Some what agree, 5 = Agree, 6 = Strongly agree)

9. Integrations are an essential part of Salesforce. *

Mark only one oval.

	1	2	3	4	5	6	
Strongly disagree							Strongly agree

10. I am aware of different kinds of Information Security threats related to Salesforce integrations. *

Mark only one oval.

	1	2	3	4	5	6	
Strongly disagree							Strongly agree

11. I am aware of what information security considerations need to be taken into account when creating integrations. *

Mark only one oval.

	1	2	3	4	5	6	
Strongly disagree	◯	◯	◯	◯	◯	◯	Strongly agree

12. When creating integrations Information Security is something that needs to be considered. *

Mark only one oval.

	1	2	3	4	5	6	
Strongly disagree	◯	◯	◯	◯	◯	◯	Strongly agree

13. When following MuleSoft designing patterns, integration security is guaranteed. *

Mark only one oval.

	1	2	3	4	5	6	
Strongly disagree	◯	◯	◯	◯	◯	◯	Strongly agree

14. When creating integrations, there are different stakeholders involved in the process. Rate each stakeholder's role when making integration secure. (1 = Main responsibility, 2 = Some responsibility, 3 = Little responsibility, 4 = No responsibility) *

Mark only one oval per row.

	1 Main responsibility	2 Some Responsibility	3 Little responsibility	4 No responsibility
Developer	◯	◯	◯	◯
Organisation using Salesforce	◯	◯	◯	◯
Third-party software provider	◯	◯	◯	◯
Salesforce	◯	◯	◯	◯
MuleSoft	◯	◯	◯	◯
Corporate Information Security	◯	◯	◯	◯
Partner / System Integrator	◯	◯	◯	◯

15. Choose 3 most valuable ways to ensure Information Security when creating integrations *

Tick all that apply.

- [ ] Using solutions found from AppExchange
- [ ] Creating own set of validations
- [ ] Creating support ticket to Salesforce
- [ ] Asking about the security from a third-party software provider
- [ ] Auditing security of third-party software
- [ ] Extensive testing
- [ ] Searching best practices
- [ ] Encourage organisation using Salesforce to take care of it
- [ ] Following MuleSoft's designing and building patterns
- [ ] Monitoring integrations
- [ ] Other: _____

16. What are MuleSofts best benefits related to Information security?

_____

_____

_____

_____

_____

17. Is there something else you would like to bring up?

_____

_____

_____

_____

_____

APPENDIX C – Salesforce survey for organizations

Salesforce survey for organizations

Empirical research for MSc thesis to find out which actions organizations using Salesforce are doing to ensure integrations are created safely regarding security. The survey response time is **16.08.2022 - 13.09.2022**.

Regarding integrations, integration means any connection that transfers data between Salesforce and third-party software. In the Salesforce context, this can mean, for example, DML operations (insert, update, upsert, delete) made from third-party software into the Salesforce or queries that provide information stored in Salesforce to the third-party software.
Third-party software means a computer program created or developed by a different organization than Salesforce and owned by others than Salesforce.

*Required

Scope of the study

I expect that the respondent is familiar with the organisation's Salesforce instance, and knows about the organisation's information security and policies related to security. I also assume that the respondent organisation has at least one integration between their Salesforce and third-party software. I hope that there will be only one answer per organisation.
This survey aims to provide base material for my MSc thesis about Salesforce integrations security. My MSc thesis will find out how integrations are managed and what actions developers and organisations are doing to achieve the security of the Salesforce instance. In my MSc thesis, I delimit Salesforce security as a whole to regard only integration and the threat they conduct to the overall security.

Who from the organisation should respond to this survey?

Due to various organisations, there is no particular person or role who should respond to this survey. For the organisations with Information Security Policies implemented, the best person to respond is one who understands those policies well. Other than that, the respondent could be in charge of the organisation's information-/digital systems. For the respondent, there is no need to have more profound knowledge about Salesforce. However, they should have an understanding of integrations there is created between Salesforce and the third-party software.
NOTE! Responding to this survey can be a joint effort.

Terms and conditions

All the answers are anonymous, and they are handled anonymously. Therefore, I am not retaining or collecting any data that can identify individuals in this survey. All the answers are stored in Google Drive, which is used account provided by the University of Jyväskylä, and they will be deleted six (6) months after this survey is closed. Only the author of this MSc thesis (Musa Jallow) can see the answers as complete.

1. I agree to the terms and conditions *

Mark only one oval.

- ◯ Yes

Organization Information

2. Size of organization *

Mark only one oval.

- ◯ <10 employees
- ◯ 10-50 employees
- ◯ 51-100 employees
- ◯ 101-500 employees
- ◯ 501-1000 employees
- ◯ 1000-5000 employees
- ◯ 5000+ employees

3. Years organisation have used Salesforce *

Mark only one oval.

- ◯ < 1 year
- ◯ 1-3 years
- ◯ 4-10 years
- ◯ 10+ years

4. How many Salesforce users does the organization have *

Mark only one oval.

- < 10 users
- 10-50 users
- 51-100 users
- 101-500 users
- 501-1000 users
- 1000-5000 users
- 5000+ users

5. Does organization have in-house Salesforce developers? If so how many?

Mark only one oval.

- 1
- 2
- 3
- 4
- 5-10
- 10+

Security Policies and customs

6. Does organisation have some Information Security Policy? *

Mark only one oval.

- Yes
- No

7. Suppose you answered Yes to the previous question. What does organisation's Information Security Policy say about Integrations (directly or indirectly)?

8. Does the organisation have someone in charge of Information Security? *

Mark only one oval.

- Yes
- No

9. Suppose you answered Yes to the previous question. What is the person's role in ensuring that Salesforce integrations are secure?

10. Suppose you answered No to the previous two questions. Are there any guidelines, standards, or customs to ensure the security of Salesforce integrations?

11. How does the organisation do Salesforce integrations? *

Mark only one oval.

- ◯ Integrations are done in-house
- ◯ Integrations are done by partner
- ◯ Integrations are done in-house and by using partner

12. If a partner is doing at least some of the integrations, how is the organisation ensuring that Information Security practices are in place?

_____

_____

_____

_____

_____

Salesforce Integrations

Statements that are answered on a scale 1-6 (1 = Strongly disagree, 2 = Disagree, 3 = Some what disagree, 4 = Some what agree, 5 = Agree, 6 = Strongly agree)

13. Integrations are an essential part of Salesforce. *

Mark only one oval.

	1	2	3	4	5	6	
Strongly disagree	◯	◯	◯	◯	◯	◯	Strongly agree

14. Our organisation knows different kinds of Information Security threats related to Salesforce integrations. *

Mark only one oval.

	1	2	3	4	5	6	
Strongly disagree	◯	◯	◯	◯	◯	◯	Strongly agree

15. In our organization, we know how to ensure Information Security when creating integrations. *

Mark only one oval.

	1	2	3	4	5	6	
Strongly disagree	◯	◯	◯	◯	◯	◯	Strongly agree

16. When creating integrations Information Security is something that needs to be considered. *

Mark only one oval.

	1	2	3	4	5	6	
Strongly disagree	◯	◯	◯	◯	◯	◯	Strongly agree

17. When creating integrations, there are different stakeholders involved in the process. Rate each stakeholder's role when making integration secure. (1 = Main responsibility, 2 = Some responsibility, 3 = Little responsibility, 4 = No responsibility) *

Mark only one oval per row.

	1 Main responsibility	2 Some Responsibility	3 Little responsibility	4 No responsibility
Developer	◯	◯	◯	◯
Organisation using Salesforce	◯	◯	◯	◯
Third-party software provider	◯	◯	◯	◯
Salesforce	◯	◯	◯	◯
Corporate Information Security	◯	◯	◯	◯
Partner / System Integrator	◯	◯	◯	◯

18. Choose 3 most valuable ways to ensure Information Security when creating integrations *

Tick all that apply.

- [ ] Using solutions found from AppExchange
- [ ] Creating own set of validations
- [ ] Creating support ticket to Salesforce
- [ ] Asking about the security from a third-party software provider
- [ ] Auditing security of third-party software
- [ ] Extensive testing
- [ ] Searching best practices
- [ ] Encourage organisation using Salesforce to take care of it
- [ ] Monitoring integrations
- [ ] Other: _____

19. Is there something else you would like to bring up?