AppOmni

Salesforce Security Handbook

Salesforce is a highly-dynamic SaaS CRM platform which stores extremely sensitive information, including customer data, sales records, personal, and financial details. For organizations that rely on Salesforce, it's essential that security professionals have a comprehensive understanding of the platform and its risks.

This handbook presents an in-depth examination of Salesforce from a security perspective, focusing on its use cases, user types, RBAC constructs and much more. Recent SaaS supply chain attacks exploiting poor Oauth security by hacker groups UNC6395, UNC6040, ShinyHunters have targeted Salesforce instances at hundreds of organizations. This handbook aims to arm Security Professionals with the knowledge needed to navigate Salesforce securely, by bringing awareness of potential risks and offering mitigation strategies.

Reading Time: 15 mins

Overview

Salesforce is a powerful, cloud-based Customer Relationship Management (CRM) platform. It helps organizations manage their customer relationships and interactions, streamline processes, and improve profitability. Its cloud infrastructure allows for high-speed, scalable, and innovative solutions that are readily accessible worldwide.

Contents

Use Cases

Salesforce offers a suite of services that span sales, service, marketing, analytics, and more. Typical use cases include:

1. **Sales Cloud:** A tool for sales teams to manage leads, opportunities, and customer accounts. It spans the entire sales journey from prospecting to closing a deal. By tracking customer interactions, offering real-time data insights, and forecasting sales, it enables a more proactive and efficient sales process.
2. **Service Cloud:** With features designed for customer service and support, it aids in efficient case management and issue resolution. This includes tracking customer inquiries, providing timely resolutions, and maintaining a knowledge base for recurring issues. It helps businesses improve customer satisfaction and loyalty while reducing the operational costs of customer service.
3. **Marketing Cloud:** This component allows digital marketing automation and analytics. It assists businesses in creating personalized customer journeys across multiple channels, such as email, web, social media, and more. With predictive analytics, marketers can craft campaigns that resonate with their audience and measure their effectiveness in real-time.
4. **Commerce Cloud:** Supports e-commerce by enabling businesses to create seamless shopping experiences across various channels. It not only provides tools for online marketing and customer service but also facilitates inventory management, order management, and other e-commerce functions. The aim is to deliver a unified and personalized customer experience, which boosts conversion rates and customer retention.
5. **Experience Cloud:** This platform is instrumental in creating and managing branded digital destinations for different stakeholders - customers, partners, and employees. It enables companies to build engaging, mobile ready community portals that strengthen engagement, collaboration, and productivity.

Salesforce's platform provides organizations with a comprehensive set of tools and functionalities to drive sales, deliver customer service, automate marketing efforts, enable e-commerce, and create engaging digital experiences.

However, the extensive functionality and broad scope of Salesforce can introduce significant complexity and potential security risks. It is crucial to carefully manage access controls, secure sensitive data, and proactively address potential vulnerabilities and misconfigurations.

By understanding the features, operations, and security considerations associated with Salesforce's use cases, organizations can leverage the platform effectively while ensuring the confidentiality, integrity, and availability of their data.

Salesforce Security Incidents

As SaaS adoption grows, the risk for breaches that threaten business operations and the security of highly sensitive data escalates. Below are a few notable Salesforce security incidents seen in the press:

- **UNC6395, UNC6040, and ShinyHunters Hacker Groups:** New hacker and extortion groups have targeted weak Oauth security policies at hundreds of organizations to steal information by using privileged identities to connect fake Dataloader applications or compromising connected applications like Drift by Salesloft. Global businesses such as Allianz Life, Adidas, Qantas, and Chanel have been impacted by these attacks. Read more.
- **Toyota Italy:** Accidentally leaked secrets for its Salesforce Marketing Cloud and Mapbox API's for more than 18 months. This opened the door to bad actors to gain access to customer phone numbers, email addresses making phishing attempts an easy attack vector. Read more.
- **AstraZeneca:** A highly privileged employee left credentials for an internal AstraZeneca server on the code sharing site, GitHub for over a year. These credentials accessed a test Salesforce cloud environment which held some patient data. Because patient data was exposed, AstraZeneca also faced questioning into their compliance standards. Read more.
- **State of Vermont, TCF Bank, and many more:** Leaked sensitive data to the public due to a misconfiguration in Experience Cloud. Data exposed includes personally identifiable information (PII) such as Social Security numbers, names, and addresses. In response to the risks identified, Salesforce stated that they are "not inherent to the Salesforce platform, but they can occur when customers' access control permissions are misconfigured." Read more.

Shared Responsibility Model

Salesforce Model

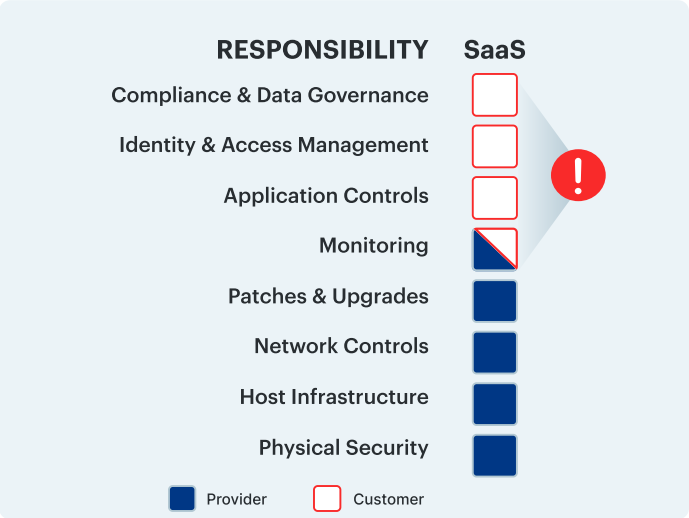
Salesforce operates on a shared responsibility model, where both the organization and Salesforce have obligations in maintaining a secure environment. Understanding these shared responsibilities is vital for security professionals when utilizing the Salesforce platform. Here are the key considerations in the shared responsibility model:

Salesforce Responsibilities

- **Infrastructure Security:** Salesforce is responsible for the physical security of its data centers and the underlying infrastructure supporting the Salesforce service. This includes implementing access controls, monitoring systems, and employing security measures to protect the hardware, software, and networking infrastructure.
- **Operational Security:** Salesforce is responsible for the operational runtime environment for its customers. This involves patching and updating underlying software and systems, managing vulnerabilities, and ensuring the logical separation of customer data within their multi-tenant architecture.
- **Network Security:** Salesforce is responsible for securing the underlying hardware, software and networking that supports the Salesforce service.
- **Data Center Security:** Salesforce is responsible for the physical security of its data centers, employing measures such as video surveillance, access controls, and environmental controls to safeguard the infrastructure and customer data.

Customer Responsibilities

- **Data Security:** Customers are responsible for the security of their own data within the Salesforce environment. This involves implementing appropriate data classification, setting access controls and permissions, and encrypting sensitive data to prevent unauthorized access or disclosure. Customers should also consider data backup and disaster recovery strategies to protect against data loss.
- **User Security:** Customers are responsible for managing their own users and their access to Salesforce. This includes provisioning and de-provisioning user accounts, enforcing strong password policies, implementing multi-factor authentication where necessary, and regularly reviewing user access rights to ensure least privilege principles are followed. Customers should also provide security awareness training to educate users about best practices and potential security risks.
- **Application Security:** Customers are responsible for the secure configuration and use of the Salesforce service. This includes securely configuring the Salesforce environment based on recommended security guidelines, regularly applying updates and patches provided by Salesforce, and conducting security testing and vulnerability assessments. Customers should also assess and review the security of any third-party applications before installing them within the Salesforce environment.



- **Incident Response and Monitoring:** Customers should implement incident response plans to effectively detect, respond to, and recover from security incidents within their Salesforce environment. This includes monitoring user activities, implementing logging and auditing mechanisms, and promptly investigating and remediating any suspicious or unauthorized activities.
- **Compliance and Data Governance:** Customers must ensure their use of Salesforce complies with applicable regulations and industry-specific requirements. This includes managing data privacy, protection, and retention in accordance with relevant data protection laws and industry standards. Customers should also conduct regular internal audits to assess compliance with their own policies and procedures.

Summary

In summary, while Salesforce provides a secure and compliant infrastructure, customers must ensure they use the service securely. The shared responsibility model underscores the importance of understanding where Salesforce's responsibilities end and where the customer's begin to maintain a secure Salesforce environment.

What Data is Stored in Salesforce

Operational Data

Salesforce allows organizations to store and manage a wide range of operational data, including sensitive information. Some examples of operational data stored in Salesforce are:

- **Personally Identifiable Information (PII):** Salesforce can store detailed customer profiles, contact details, and interactions. This includes names, addresses, phone numbers, email addresses, and social media profiles. It is essential to handle this data securely, protecting it from unauthorized access or disclosure.
- **Sales and Marketing Data:** Salesforce is often used as a customer relationship management (CRM) system, storing sales and marketing-related data. This includes leads, opportunities, deals, sales forecasts, and campaign information. Protecting this data is critical to maintaining the competitiveness and reputation of the organization.
- **Service and Support Data:** Salesforce's service cloud capabilities enable the storage of service and support data, including customer service interactions, case details, ticketing information, and resolution history. This data may contain sensitive information shared during support interactions and should be adequately protected.
- **Financial and Billing Data:** Organizations using Salesforce for financial management may store financial and billing data. This includes invoices, payment records, billing details, and financial reports. Proper security controls are necessary to safeguard this sensitive financial information.
- **Collaboration Data:** Salesforce provides collaboration features such as Chatter, allowing users to share files, collaborate on projects, and communicate within the platform. This data may include sensitive documents, discussions, and intellectual property. Ensuring appropriate access controls and encryption for shared files is crucial to prevent unauthorized access or data leakage.

Configuration Data

Salesforce stores configuration data that defines the structure and behavior of the platform and customizations made by the organization. Some examples of configuration data stored in Salesforce are:

- **Standard Objects:** Salesforce provides a set of pre-built standard objects that are commonly used for various business processes. These include objects such as Accounts, Contacts, Opportunities, Cases, and Leads.
- **Custom Objects:** Salesforce allows organizations to create custom objects tailored to their use cases and requirements. Custom objects represent unique data structures and are often used to capture specialized information that is not covered by standard objects.
- **Fields and Relationships:** Within standard and custom objects, Salesforce enables organizations to define fields to capture various data types such as text, number, date, or picklist values. Additionally, relationships between objects can be established to establish data connections and hierarchies.
- **Workflows and Process Automations:** Salesforce provides workflow and process automation capabilities to streamline business processes. Organizations can define rules, triggers, and approvals that automate tasks and enforce consistent workflows.
- **User Roles and Permissions:** Salesforce's role-based access control (RBAC) system allows organizations to define user roles and assign appropriate permissions in a highly granular manner. This ensures users have the necessary access rights and permissions to perform their job functions while preventing unauthorized user actions.
- **Integration Configurations:** Salesforce allows integration with other systems and applications. Configuration data related to these integrations include API settings, authentication credentials, and connection details.
- **Reporting and Analytics Configurations:** Salesforce offers powerful reporting and analytics capabilities, allowing organizations to generate insights from their data. Configurations related to report and dashboard access, data visibility, and data export permissions should be carefully managed to prevent unauthorized data exposure or misuse.

Summary

Securing data in Salesforce is crucial for security professionals. It is crucial for organizations to implement robust security measures. This includes continuous configuration reviews, strong access control policies, encryption of data in transit and at rest, and comprehensive data governance policies. Furthermore, any configuration changes should be carefully managed and tracked to avoid inadvertent vulnerabilities, ensuring the security and integrity of both operational and configuration data.

Roles & Responsibilities

Salesforce Operators

The operation of Salesforce within an organization typically involves several key roles, each with its own responsibilities and areas of focus. Each role can vary depending on the size of the organization but these typically include:

1. **Salesforce Administrators: A**dministrators are the stewards of an organization's Salesforce environment. They configure and manage Salesforce to meet the needs of the organization and its users. Responsibilities can include creating and managing users, defining security settings, creating workflows and automation, managing data, generating reports, and assisting users with Salesforce issues. They also serve as a liaison between users and developers to ensure that the Salesforce environment continues to evolve to meet changing business needs.

2. **Salesforce Developers:** Developers use the Salesforce platform to build custom applications, interfaces, and functionality to extend the capabilities of Salesforce beyond its out-of-the-box offerings. They use languages such as Apex (Salesforce's proprietary programming language) and Visualforce, along with tools like Lightning App Builder and Salesforce DX. They are responsible for designing, coding, testing, and implementing new Salesforce software applications to meet business objectives.

3. **Salesforce Architects:** Architects are responsible for the high-level design of an organization's Salesforce environment. This includes defining the technical vision, making strategic technology decisions, and ensuring that the environment remains scalable, reliable, secure, and meets the business's needs. Architects often work closely with admins and developers to guide the evolution of the Salesforce environment.

4. **Salesforce Consultants:** Consultants work with organizations to define their Salesforce strategy. They help to identify business requirements, recommend best practices, and guide the implementation of Salesforce solutions. They may also provide training and support to users.

Salesforce Users

Salesforce users come from various roles within an organization, each interacting with the platform in unique ways and needing different levels of access and permissions. User types include:

1. **Sales Representatives:** Users who utilize Salesforce to manage their sales pipeline, track opportunities, and collaborate with team members.

2. **Customer Service Representatives:** Users responsible for resolving customer inquiries, support tickets, and managing customer service processes within Salesforce.

3. **Executives and Managers:** Users at higher levels who leverage Salesforce for strategic decision-making, accessing reports and analytics, and monitoring business performance.

External Users

In addition to internal users, Salesforce also supports the engagement of external users, such as customers, partners, and suppliers using Experience Cloud. Here are some typical external user scenarios and associated security considerations:

- **Customer Portals:** Organizations often provide customer portals to allow customers to access self-service features, view their account information, submit support cases, or track orders. Security considerations include ensuring proper authentication and authorization mechanisms, securely handling sensitive customer data, and implementing access controls to protect customer information from unauthorized access.

- **Partner Communities:** Partner communities enable collaboration and information sharing between an organization and its partners. This may involve joint opportunity management, sharing sales and marketing collateral, or collaborating on support cases. Security considerations include managing user access rights, enforcing data-sharing rules, and ensuring secure integration between the organization's Salesforce instance and partner systems.

- **Supplier Collaboration:** Organizations may use Salesforce to collaborate with suppliers, manage procurement processes, or track supplier performance. It is critical to establish appropriate access controls to protect sensitive procurement data, ensure secure communication channels, and establish strong identity and access management practices for supplier users.

- **App Users:** In some cases, organizations build custom applications on the Salesforce platform and provide access to external users. These applications could range from customer facing portals to mobile apps. Security considerations include secure application design, robust authentication mechanisms, secure API integrations, and adherence to Salesforce security best practices for custom development.

Summary

Managing security in a Salesforce deployment involves enforcing least privilege access, adopting secure coding practices, providing user training on data handling, and conducting regular audits. By focusing on these key areas, organizations can effectively mitigate security risks associated with the various roles and their responsibilities within Salesforce.

RBAC Structure

Salesforce RBAC Structure

Role-Based Access Control (RBAC) is a method of regulating access to computer or network resources based on the roles of individual users within an organization. In Salesforce, this is handled through a combination of profiles and permission sets.

1. **Profiles:** A profile defines a user's functional access in Salesforce. This includes what they can do within the app (such as creating or editing records), what features they can use, and their permissions on standard and custom objects.
2. **Permission Sets:** While profiles define the baseline permissions for users, permission sets are used to grant additional permissions. They provide more granular access controls beyond what profiles offer. Permission sets can be assigned to any user, regardless of their profile.
3. **Roles and Role Hierarchies:** Roles in Salesforce do not grant any permissions, but they do determine the level of visibility that users have into a Salesforce org's data. The role hierarchy represents the level of data access that a user or group of users needs.

Common risks associated with RBAC in Salesforce

1. **Overly Broad Access:** If a user is assigned a profile or permission set that grants them more access than they need to perform their job functions, they could view/modify/delete data they should not have access to or potentially begin customizing the configuration of the application itself in ways beyond their job remit. This principle of least privilege violation could lead to data leakage or unauthorized data alteration.
2. **Accumulation of Access Rights:** As users move roles within an organization, they may be granted new permissions without revoking old ones, leading to an excessive accumulation of access rights. Over time, this could result in users having much more access than they require, increasing the potential damage if their account is compromised.
3. **Lack of Role Definition:** Without clearly defined roles and permissions, an organization may not have a clear understanding of who has access to what, making it harder to manage and secure sensitive data.
4. **Insufficient Auditing and Monitoring:** Without regular reviews of user permissions, unauthorized or inappropriate access could go unnoticed. Regular audits can help to identify and correct permissions that are too broad, unused, or inappropriate for a user's role.

Summary

To mitigate these risks, security professionals should adopt the following practices. Firstly, they should regularly review and update role assignments to ensure they align with employees' responsibilities.

It is essential to validate and adjust permissions based on the principle of least privilege. Implementing proper segregation of duties helps prevent conflicts of interest and enhances oversight.

Additionally, it is crucial to regularly review and audit access control configurations to ensure they are aligned with security requirements and best practices. These proactive measures contribute to a more secure RBAC implementation and minimize the risk of unauthorized access or privileges.

Customization in Salesforce

Customization Capabilities

Salesforce is renowned for its high degree of customizability, enabling it to adapt to the unique needs of each business. From simple changes to more complex customizations, Salesforce can be tailored to streamline business processes and enhance productivity. Typical customizations include:

- Adding Custom Fields to Standard Objects: Businesses often need to track additional information that is not catered to by standard objects in Salesforce. By adding custom fields, businesses can ensure that all necessary information is captured and accessible.
- Creating Custom Objects: When standard objects can't capture a unique business process or data type, creating custom objects can provide a bespoke solution.
- Building Custom Workflows and Automation: Automating routine tasks and creating custom workflows based on specific business rules helps improve efficiency and reduce human error.
- Developing Custom Applications: With Salesforce's low-code and pro-code development environments, businesses can create custom applications tailored to their unique requirements.
- Visual Customizations: Salesforce allows changes to its user interface, enabling a more engaging and user-friendly experience.

Common risks associated with Customization: • Code Security: Any custom code, whether for a new application, a Visualforce page, or an Apex class, must be written following secure coding principles to prevent vulnerabilities such as injection attacks or cross-site scripting.

- Access to Custom Objects and Fields: Just like with standard objects and fields, access to custom objects and fields needs to be tightly controlled. Role-Based Access Control (RBAC) should be used to ensure that only authorized users can view and edit this data.
- Testing and Validation: Customizations, particularly those involving code changes, should undergo thorough testing and validation before being deployed to the production environment. This can help identify and fix potential security issues.
- 3rd Party Applications: If customizations involve third-party applications or integrations, you should evaluate their security measures and data handling practices.
- Data Privacy and Compliance: Any new data fields or objects should be evaluated for privacy and compliance implications, particularly if they will store sensitive or regulated data.

Summary

While the extensive customization capabilities of Salesforce offer plenty of benefits, they also demand careful planning and execution to keep the environment secure.

Firstly, consider conducting a comprehensive assessment of your business processes to identify the specific customizations necessary, avoiding unnecessary

complexity. Whenever possible, leverage Salesforce's 'click-not-code' capabilities before resorting to custom code, as this can reduce the risk of code vulnerabilities. If coding is unavoidable, follow secure coding practices and engage in exhaustive testing.

Rigorously manage access rights to custom objects and fields, ensuring only necessary personnel have permissions. Thoroughly evaluate third-party applications for their security and data handling practices before integrating them into your system. Finally, consider data privacy and compliance implications when adding new fields or objects. Remember, customization should add value and not become a source of vulnerability.

3rd Party Apps

SaaS-to-SaaS Ecosystem

There are often a large number of third-party, or SaaS-to SaaS apps that businesses often integrate with Salesforce for extended functionalities.

While there is a wide range of third-party apps available for integration with Salesforce, it's important to note that the ecosystem encompasses both established and niche apps. The Salesforce AppExchange, Salesforce's official marketplace, hosts thousands of apps catering to diverse business needs.

While established vendors offer robust and well-vetted solutions, there are also niche apps that provide specialized functionalities.

Some of the more common 3rd party apps include:

1. **DocuSign:** Used for digital signatures and contract management. Its seamless integration with Salesforce aids in simplifying the agreement process.
2. **MailChimp:** A well-known email marketing service that helps businesses automate and manage their email campaigns.
3. **Tableau:** Owned by Salesforce, it provides advanced data visualization and business intelligence capabilities.
4. **Zapier:** Helps to automate workflows by connecting Salesforce with a multitude of other apps and services.
5. **Slack:** A popular collaboration tool that is used for real-time communication and file sharing. Salesforce's acquisition of Slack has led to even deeper integrations.
6. **Conga Composer:** Used to generate complex documents and reports from Salesforce data.
7. **SurveyMonkey:** Used to collect customer feedback and insights which can be integrated directly into Salesforce records.
8. **QuickBooks:** A popular accounting application. The QuickBooks integration allows for a streamlined financial workflow.
9. **Jira:** For project management, especially within software development teams, integrating Jira and Salesforce can improve collaboration and issue tracking.

Common risks associated with 3rd Party Apps Some of the followings risks should be considered when installing 3rd party apps into Salesforce:

- **Data Exposure:** Each new integration represents a potential exposure point for data. When you integrate a third-party application, you need to ensure that the application only has access to the necessary data and that it handles this data securely.
- **Access Control:** It's crucial to control which users can use these integrations, and what data they can access or modify through them. Principle of least privilege should be applied here to ensure a user only has enough privilege to perform their tasks, and no more.
- **Vendor Security:** Before integrating a third-party application, it is essential to review the vendor's security practices. This includes their data protection measures, compliance certifications, and how they respond to security incidents.
- **API Security:** Many integrations work through APIs, which can be a potential attack vector. It is essential to ensure these APIs are secure and used correctly.
- **Ongoing Monitoring:** Once an integration is in place, it's crucial to monitor it regularly for any unusual activity or potential security issues. Without continuous monitoring, reports only show a snapshot of time.

When considering lesser-known or niche third-party apps, organizations should exercise additional caution. While these apps may offer unique features or cater to specific industry requirements, they may not have undergone the same level of scrutiny or have a large user base compared to established vendors. It becomes essential to conduct thorough research, assess the vendor's reputation, evaluate security practices, and review customer reviews or ratings.

Summary

To mitigate risks from SaaS-to-SaaS connected apps, organizations should conduct thorough due diligence on 3rd party app vendors, review app ratings and reviews, and carefully consider the necessity and security implications before installing any app. Regular monitoring and assessment of installed apps are also essential to ensure ongoing security and compliance.

Logging Capabilities

Logs and Event Types

Salesforce provides a range of logs that can be used to monitor activity, troubleshoot issues, and identify security threats. These logs can be exported to Security Information and Event Management (SIEM) systems for analysis and correlation with other logs.

The types of logs available in Salesforce include:

1. **Event Logs:** These provide visibility into an org's operational events, which you can use for auditing, compliance, performance optimization, and troubleshooting. Event types include API calls, login events, and security incidents.
2. **Login History:** This log captures the last six months of login history for all users. It includes information such as login date, source IP, whether the login was successful, and if multi-factor authentication was used.
3. **Setup Audit Trail:** This log captures the last six months of setup changes made by admins in the org. This can help identify who made changes, what those changes were, and when they occurred.
4. **Debug Logs:** These logs store database operations, system processes, and errors that occur when executing a transaction or running unit tests. They can be used for troubleshooting and identifying issues in Apex code or Visualforce pages.
5. **Apex Logs:** These logs provide information about Apex executions. They include details on the start and end time of each transaction, the duration of each transaction, and the email addresses of users who invoked Apex.

Summary

For effective log management, it is important to regularly review and analyze logs, keep them only for as long as required for compliance or business needs, and protect them to ensure their integrity and confidentiality. Using a SIEM solution can help automate these tasks and provide more comprehensive visibility by correlating Salesforce logs with logs from other systems.

Top Security Risks

It is essential for security professionals to be aware of the potential Salesforce security risks. Here are some common security risks associated with Salesforce:

- **Insufficient User Access Control:** Salesforce offers complex security controls such as Profiles, Permission Sets, and Sharing Rules to control user access to data and functionality. Misconfigured or overly broad permissions can lead to unauthorized access to sensitive data.
- **Experience Cloud Misconfiguration:** As per the recent Krebs on Security article, a large number of Salesforce users leveraging Experience Cloud are leaking data to the public internet. Public-facing sites are prone to misconfiguration which can inadvertently leak sensitive data.
- **Inadequate Audit Trail Management:** Salesforce provides audit trails that track changes made in the system. If these logs are not regularly reviewed, you may miss malicious activities or system misconfigurations.
- **Third-Party App Risks:** Salesforce's AppExchange hosts many third-party applications that can extend the functionality of Salesforce. However, these applications may also introduce vulnerabilities if they are not properly vetted.
- **Data Leakage:** As Salesforce is a cloud-based platform, data can potentially be accessed from any device with internet connectivity. This introduces the risk of data leakage through lost or stolen devices, insecure networks, or due to insider threats.
- **API Vulnerabilities:** Salesforce provides numerous APIs for integration with other systems. These APIs, if not correctly configured and secured, can introduce vulnerabilities.
- **Phishing Attacks:** Like any other online platform, Salesforce users can be targeted by phishing attacks, leading to compromised user credentials and unauthorized system access.
- **Lack of Encryption for Sensitive Data:** Salesforce provides native functionality for data encryption. However, if this is not correctly implemented, sensitive data may be stored in an unencrypted format.
- **Insufficient User Awareness and Training:** Users without adequate cybersecurity training may inadvertently cause security incidents, for example by falling for phishing attacks or mishandling sensitive data.
- **Non-compliance with Legal and Regulatory Standards:** Depending on an org's industry and jurisdiction, it may be required to comply with certain legal and regulatory standards (such as GDPR, CCPA, HIPAA). Non-compliance due to incorrect Salesforce configuration can lead to legal penalties.

How AppOmni Helps.

AppOmni SaaS security makes it easy for security and IT teams to protect and monitor their entire SaaS environment. AppOmni was founded by a team of security veterans from top SaaS providers and cybersecurity vendors. Using their expertise, they put together the following list of best SaaS security practices and recommendations:

- **Baseline Security Policies:** Configurable out of the box baselines security policies to help map an organization to recommended best practice security configurations.
- **Compliance Policies:** Map a Salesforce instance to ISO27001, SOC2, NIST CSF, NIST 80053 and Sarbanes Oxley.
- **Sensitive Permission Monitoring:** Identify when risky permissions are incorrectly assigned to users, profiles or permissions sets.
- **Monitor users assigned to sensitive profiles and permission sets:** Ensure that any change in RBAC assignments within Salesforce does not result in users gaining access to assets beyond their job requirements.
- **Monitor creation of new profiles, permissions set:** Be alerted to new permission sets and profile creations and easily review an inventory of existing permission sets and profiles.
- **Understand the total risk linked to user access:** Salesforce's complicated RBAC structure makes it challenging to understand the sum of a user's data access and permissions. AppOmni's Access Explorer offers a simple way to see the current state of an accounts access and simply convert this access to a policy for continuous monitoring.
- **Monitor SaaS-to-SaaS connections:** AppOmni's App Ecosystem capabilities can provide visibility of fourth party SaaS applications which have been connected in to a Salesforce org, potentially exposing data.
- **Threat Detection:** Monitor for known threat actor TTPs, suspicious user logins, unauthorized apps, high volume API queries from VPNs, and other custom threat detection rules

Summary

In summary, this handbook underscores the complexities of Salesforce's security landscape and provides vital insights to navigate it effectively. Given the varied security considerations across customization, third-party apps, data storage, and user roles, it is imperative to review these factors carefully. This shows why it's necessary to collaborate with application operators, reviewing the security posture of the Salesforce application, identifying potential vulnerabilities, and formulating effective mitigation strategies.

To learn more, email us at info@appomni.com or visit appomni.com.