

Copyright © 2024 Advension™. All rights reserved.

Foreword

We're navigating through uncertain times, rising inflation, political tensions, volatile stock markets, unpredictable weather events, and enduring challenges like pandemics and food and water shortages.

These global issues are creating widespread instability, socio-political dynamics of inequality, and deepening divisions, all of which are contributing to a surge in cybersecurity breaches.

While numerous attacks have targeted corporate IT systems and networks across industries like financial services, manufacturing, and supply chain, Salesforce has not been exempt.

As the leading CRM platform for over a decade, Salesforce is entrusted by some of the world's largest companies to manage highly sensitive data, including customer profiles, financial records, medical information, and more. Its broad adoption across departments like Marketing, Sales, and Finance, combined with its versatile cloud-based architecture, makes it a powerful tool, yet also a prime target for cyberattacks.

Addressing these challenges effectively is crucial to safeguarding your Salesforce setup from vulnerabilities that could be exploited, leading to significant financial losses and damaging your company's reputation and credibility.

This paper aims to raise awareness and provide essential insights and best practices for implementing the security measures needed to protect your Salesforce environment effectively.



ALEXANDER STOJANOVIC
CEO | CISO
@Advension

Copyright © 2024 Advension™. All rights reserved.

Executive Summary

The primary purpose of this paper is to assist CISOs, CIOs, CTOs, and IT leaders, as well as any cybersecurity professional by offering essential cybersecurity insights, technical guidance, and best practices for securing their Salesforce Cloud enterprise landscape. Many organisations face challenges in consistently applying security principles across all cloud solutions, inadvertently creating vulnerabilities that attackers can exploit.
This often occurs due to various factors, such as prioritising business objectives like reducing time-to-market over implementing robust security measures, or simply a lack of skilled resources.

Security is frequently viewed as a burden—something that consumes resources, raises costs, and delays product launches.

This issue is further compounded by the fact that cybersecurity is often placed under IT departments, which are primarily focused on internal challenges. However, the true value of strong cybersecurity extends beyond internal concerns—it's crucial for building customer trust and enhancing the overall valuation of the company.

In today's digital age, trust is paramount, and it is built on a foundation of strong cyber defence and adherence to essential security principles.

Given the critical importance of cyber security, leaders in this field deserve a seat at the C-level table, working closely with revenue management and, marketing and sales teams to ensure that security is integrated into the broader business strategy.

Key Findings

While Salesforce provides a wide array of features, tools, and configurations to enhance its security, it doesn't operate in isolation. It is always part of a larger IT ecosystem that must adhere to cross-platform information security standards.

Based on our analysing of 30+ state of security reports, statistical data, and drawing on our extensive experience in the field, we have identified four essential areas that need to be addressed.
Two of these areas are directly related to Salesforce and its capabilities, while the other two extend beyond the Salesforce domain.

The following four aspects of Salesforce cybersecurity defence are explored in greater detail throughout this paper:

- Platform Security
- Application / Code Security
- *Development and Deployment Processes*
- *Impact of Organisational Culture on Security*

> ***"In trust we trust.***
> ***Trust is our #1 value. We build trust with stakeholders by leading with ethics and through the integrity of our technology. We are dedicated to transparency, deep listening, and delivering on our commitments."***
>
> SALESFORCE.COM

Copyright © 2024 Advension™. All rights reserved.

Table of Contents

04 Introduction
Overall introduction to this white paper, the key challenges and high-level stats.
#SalesforceSecurity | 3 min read

06 Global Key Challenges
General world-wide cybersecurity challenges across different walks of life.
#GlobalSecurityChallenges | 10 min read

07. Major Geopolitical Concerns
08. Increased Attack Complexity
09. Complex Organisational Structures
10. Stress and Anxiety in Cybersecurity..
11. Talent and Skills Gap
12. Inadequate Cyber Defence

13 Threats, Principles, Defence..
Brief overview on the key top security threats, guiding principles, and defence surface.
#ThreatsAndSecurityPrinciples | 10 min read

14. Top Security Threats
15. Cyber-Security Principles
16. Defence Surface

17 Salesforce Security Assess..
Overview of key areas and reasons for conducting frequent Security Assessments.
#SalesforceSecurityAssessment | 10 min read

18. Securing Salesforce: Why Security..
19. Critical Areas for Assessment

22 Salesforce Platform and Sys..
Overview of the most critical configurations needed to secure Salesforce.
#SalesforcePlatformSecurity | 10 min read

23. Essential Security Configurations..
24. Key Areas to Address

28 Salesforce Application and..
Overview of the most critical code hardening and logic specific measures for cyber defence.
#SalesforceCodeSecurity | 10 min read

29. Best Practices for Securing Apex, Visu..
30. Essential Code Security Measures

33 Development and Deploy..
Overview of the most essential development and deployment practices to reduce cyber threats.
#SalesforceSSDLC | 10 min read

34. The Importance of Secure Code and ..
35. Key Development and Deployment Str..

37 Culture and Organisational..
Understanding the human error and people as the key line of a successful cyber defence.
#CultureSecurity #HumanFirewall | 10 min read

38. Building a Strong Security Culture..
39. Addressing the Human Side of Cyber..

42 Summary
An extensive conclusion of the overall report, and next step.
5 min read

43 Acknowledgement
Official thanks to the key collaborators that helped shaping the content of this report.
3 min read

44 Appendix
Bonus resources and knowledge sources to guide the Salesforce defence path.
2 min read

45 References
All key references that have been cited throughout the report.
2 min read

Copyright © 2024 Advension™. All rights reserved.

Introduction

In the modern digital landscape, Salesforce has established itself as a leading platform, acquiring over 20% market share and serving over 150,000 customers globally.
This extensive user base includes government agencies, financial services, manufacturing, and over 90% of the Fortune 500 companies, handling trillions of customer data points and billions of data transactions per day.

The platform's widespread adoption and the critical nature of the data it handles make Salesforce an attractive target for cyber threats, with hacker groups and individuals increasingly focusing their efforts on exploiting potential vulnerabilities.

The importance of implementing robust Salesforce security measures cannot be overstated. In general, the overall number of cyber breaches has surged significantly over the past two years, reflecting a growing and evolving threat landscape.

A study conducted by Verizon highlights a substantial growth in breaches due to vulnerabilities, particularly those related to Ransomware and Extortion attacks, which have seen a 180% increase from the previous year. (Verizon 2024 Data Breach Investigations Report)

Additionally, according to the IBM Cost of a Data Breach Report 2024, the global average cost of a data breach has escalated by 10% from the previous year, reaching a staggering **USD 4.88 million.**

This upward trend underscores the financial implications and potential disruptions that can result from inadequate security measures.

While Salesforce is widely perceived as *secure by design* and quite often referred to as "plug and play", this assumption can lead to complacency and overlooked vulnerabilities.
In one such case, dozens of financial, healthcare and governmental institutions had Salesforce Community websites that were leaking PII[2] sensitive data such as, names, addresses, full Social Security numbers, job titles, federal IDs, IP addresses, average monthly payrolls, and loan amounts. (Source: Krebsonsecurity 2023)

Additionally, due to organisational silos, CISOs often lack comprehensive visibility into the administrative and development processes within Salesforce environments, making it difficult to identify and mitigate risks effectively.
Similarly, organisations engaged in extensive custom development within Salesforce, such as Apex and Lightning Web Components (LWC), frequently neglect to allocate sufficient time and resources for security measures.

This oversight, coupled with the pressure of tight project schedules and limited budgets and resources, can result in configurations and code that are susceptible to cyber-attacks.

99%
suffered negative business impact from a breach.

94%
use more than 10 vendors for identity-related cybersecurity initiatives.

64%
of organizations have or will prioritize ITDR[1].

Source: CyberArk - Identity Security Threat Landscape 2024

1. *ITDR: Identity Threat Detection and Response*
2. *PII: Personal Identifiable Information*

Copyright © 2024 Advension™. All rights reserved.

Understanding the stakes involved is crucial. Protecting what is often considered the "Holy Grail" of an organisation's data—customer information, proprietary business insights, and sensitive operational details is paramount. The repercussions of compromised security extend beyond financial penalties to include damage to the company's reputation and brand, loss of *customer trust*, and increased churn rates.

Goals and Objectives

This white paper aims to provide a better understanding of the "Why", and "What" has to be taken into account, as well as bridge these gaps by providing a comprehensive guide to some key Salesforce security best practices.

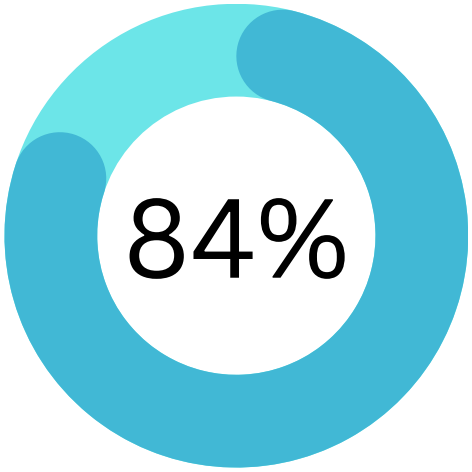
It emphasises a well-documented measures that align with overall organisational IT security principles and Salesforce's shared responsibility model.

By adopting these practices, organizations can significantly reduce the likelihood of cybersecurity breaches, enhancing their cyber hygiene and ensuring the integrity of their critical data.

The value of this paper lies in its ability to equip CISOs with a deeper understanding of the security risks and potential threats associated with improper Salesforce configuration and implementation.

It also raises awareness among Salesforce development teams about the importance of adhering to security best practices.

By highlighting the most critical security aspects that need to be addressed, this paper serves as a vital resource for organisations aiming to safeguard their Salesforce environments against the ever-evolving landscape of cyber threats.



"Percentage of critical infrastructure incidents where initial access vector could have been mitigated with best practices and security fundamentals, such as asset and patch management, credential hardening, and the principle of least privilege."

2024 IBM SECURITY



Copyright © 2024 Advension™. All rights reserved.

Global Key Challenges

To truly grasp the cybersecurity landscape and its current state, it's essential to evaluate some global key challenges that significantly impact not only organisations and their security but also the employees well-being and overall performance.

The challenges outlined in the upcoming sections are based on an extensive study and numerous recent reports and surveys that capture direct feedback from top cybersecurity experts and leaders across various industries and regions worldwide.

A global pattern emerges, affecting most companies in similar ways. This trend encompasses several dimensions, including the technical nature of diverse attacks, organisational and cultural similarities, and overarching market trends.

1 Major Geopolitical Concerns

2 Increased Attack Complexity

3 Complex Organisational Structures

4 Stress and Anxiety in Cybersecurity Roles

5 Talent and Skills Shortage

6 Inadequate Cyber Defence

Copyright © 2024 Advension™. All rights reserved.

Major Geopolitical Concerns

Geopolitical concerns are escalating global cybersecurity threats, with conflicts in Europe and the Middle East driving cyber activities by nation-states. Alliances like BRICS and NATO contribute to cyber conflicts as nations assert power. Illegal immigration, activist groups and other social movements also impacts cybersecurity, with organised crime exploiting vulnerabilities, increasing global risks.

The ongoing *conflicts in Ukraine* and the *Middle East* have heightened the global cybersecurity threats.
These wars contribute to geopolitical instability, leading to increased cyber activities from nation-state actors who exploit the chaos to further their agendas.

Geopolitical alliances like *BRICS and NATO* influence the global cybersecurity landscape. These groups often find themselves in cyber conflicts, with member nations using cyber tactics to assert power or retaliate against perceived threats, affecting international cybersecurity dynamics.

Illegal immigration intersects with cybersecurity, as it often involves organised crime groups that exploit vulnerabilities at both physical and cyber borders.
The resulting global instability from migration can contribute to increased risks of cyber incidents.

Copyright © 2024 Advension™. All rights reserved.

Increased Attack Complexity

The rapid expansion of digital infrastructure and the shift to remote and hybrid work have drastically increased cyber attack vectors, leading to millions of security events each year.
Social engineering continues to be a potent attack method, exploiting human error to breach security systems.
Meanwhile, industrial espionage is growing more sophisticated, particularly in high-value sectors like finance and manufacturing, where intellectual property and sensitive data are prime targets.

The expansion of digital infrastructure and the rise of remote/hybrid work have significantly increased the number of cyber attack vectors. Organizations now face millions of security events annually, reflecting the complexity and scale of the modern threat landscape.

Social engineering remains a highly effective attack method, as it exploits human error, which is involved in a large percentage of security incidents. Attackers use sophisticated deception mechanisms, often AI driven, to manipulate individuals into compromising security systems.

Industrial espionage is becoming more sophisticated, particularly in targeting high-value industries such as finance and manufacturing.

These sectors are vulnerable to espionage due to the high value of their intellectual property and sensitive data.

Copyright © 2024 Advension™. All rights reserved.

Complex Organisational Structures

Corporate hierarchies and bureaucratic processes often hinder cybersecurity efforts, as many CISOs struggle with navigating complex structures and securing timely decisions.
Budget constraints further challenge CISOs, who frequently lack direct access to executive leadership, making it difficult to secure necessary funding.
Only 20% of CISOs hold C-level positions, limiting their influence within organizations (IANS).

The complexity of corporate hierarchies can further obstruct cybersecurity efforts.
Many CISOs come from technical backgrounds with a lack of business acumen and struggle to navigate complex organisational structures, which can impede swift decision-making and effective security management.

Bureaucratic processes and rigid siloed teams structures within organizations can slow down responses to cyber threats.
CISOs often face delays in getting approvals and making decisions due to the layers of bureaucracy, which can be detrimental during cyber incidents.

Budget constraints are a common challenge for CISOs, who often struggle to secure adequate funding for cybersecurity initiatives, especially when lack direct access to executive leadership.

In a study conducted by IANS, only 20% of the CISOs reported that they are at the C-level on the overal organisational hierarchy. (State of the CISO, 2023-2024 Benchmark Summary Report)

Copyright © 2024 Advension™. All rights reserved.

Stress and Anxiety in Cybersecurity Roles

Cybersecurity professionals experience significant stress and anxiety due to constant pressure to prevent evolving threats, leading to burnout and high turnover rates.
The no-fail culture and uncertainty about job security further increase anxiety.
Toxic workplace environments also contribute to stress, leaving many feeling unsupported and undervalued.



Cybersecurity professionals face high levels of stress and anxiety due to the pressure to protect against constant and evolving threats, often leading to burnout and decreased job satisfaction.

Uncertainty about job security and the ever-changing threat landscape further contribute to anxiety, resulting in higher turnover rates, as highlighted in the CyberArk Identity Security Threat Landscape 2024 Report.

The no-fail culture and toxic workplace environments create unrealistic expectations, leaving many feeling unsupported, which exacerbates stress and negatively impacts overall well-being.

Copyright © 2024 Advension™. All rights reserved.

Talent and Skills Shortage

The cybersecurity industry is engaging with several critical challenges that undermine its effectiveness in combating rising cyber threats.
A significant shortage of skilled professionals, inadequate leadership guidance, and insufficient training are compounded by unclear roles and responsibilities within teams.
These issues collectively weaken the ability of organisations to protect themselves in an increasingly complex and dangerous cyber landscape.

The cybersecurity industry is facing a critical shortage of skilled professionals, with the global workforce gap growing by 12.6% in 2023, resulting in a shortfall of approximately 3.99 million cybersecurity professionals worldwide. (ISC2 Cybersecurity Workforce Study 2023)

A lack of clear leadership guidance in cybersecurity leads to ineffective security strategies and misalignment with organisational goals, as many professionals feel they do not receive adequate direction from senior management.

Insufficient training and ambiguity in roles and responsibilities are major issues, causing confusion and gaps in security coverage, which weaken the organisation's defence against evolving cyber threats.

Copyright © 2024 Advension™. All rights reserved.

Inadequate Cyber Defence

Organizations face significant cybersecurity challenges due to inadequate defense technologies, misconfigurations, and weaknesses in security design.
The rapid evolution of cyber threats demands constant updates, yet many struggle to maintain the necessary tools. Misconfigurations, such as those seen in recent Salesforce incidents, expose sensitive data, while the lack of robust security design and proper code hardening leaves systems and applications vulnerable to exploitation.

Many organisations lack adequate cyber defence technologies, struggling to keep up with the rapid evolution of threats, which leaves them vulnerable to sophisticated attacks.

Misconfigurations of cloud platforms like Salesforce are a common cause of security incidents, often leading to major breaches that expose highly sensitive information.

The absence of robust security design principles and failure to properly harden code leave systems and applications vulnerable to exploitation, increasing the risk of successful attacks.

Copyright © 2024 Advension™. All rights reserved.



Threats, Principles, Defence Surface

“Security is not a product, but a process. It’s about understanding the principles behind the technology to truly protect what matters.”

BRUCE SCHNEIER, CRYPTOGRAPHER AND SECURITY EXPERT

Copyright © 2024 Advension™. All rights reserved.

Top Security Threats

To discuss Salesforce security effectively, we must also address the broader security threats that organisations face daily.
Based on the latest report conducted by "CSA, 2024 Top Threats", *Platforms Misconfiguration, IAM, Insecure API, Lack of Cloud Security Implementation, Insecure Third-Party Resources, and Insecure Software Development*, make among the top 10 critical cybersecurity threats.

To support this study, according to an IBM Security report, cyberattacks leveraging stolen or compromised credentials have surged by 71% year-over-year. This rise is largely because accessing credentials is often easier than breaching a physical network or other infrastructure. Many of these compromised credentials, including Salesforce logins, were compromised by infostealers, a type of malware that harvests sensitive identity data such as passwords, secrets, and cookies. This malware is typically initiated through phishing emails, SMS, and chat apps like WhatsApp and Telegram.

Forbes reports that "94% of organisations have reported email security incidents." Additionally, a SoSafe - Human Risk Review 2024 report describes that "37% of users click on harmful content in emails," highlighting the ongoing effectiveness of phishing attacks. Further more, users unawarely download infected .docx or a .pdf files which typically are delivered as an attachment to an email, or apps such as Microsoft Teams, Slack, Discord, etc. Despite this being an older method, the use of phishing has increased, partly driven by the rise of generative AI. In fact, according to SoSafe, "79% of security leaders agree that the use of generative AI by cybercriminals to create social engineering attacks is a concern for their organisation".

Regardless of how advanced an organisation's defences are, the weakest link remains its people. Social engineering attacks, whether by phone, video call, or in person, target humans. Phishing emails aim for the same, relying on a person to click a compromised link. Therefore, investing in the human aspect of security has become a priority for many organisations.

Top 10 Cloud Threats

1. Misconfiguration & Inadequate Change Control
2. Identity and Access Management
3. Insecure Interfaces and APIs
4. Inadequate Selection/Implementation of Cloud Security Strategy
5. Insecure Third-Party Resources
6. Insecure Software Development
7. Accidental Cloud Disclosure
8. System Vulnerabilities
9. Limited Cloud Visibility/Observability
10. Unauthenticated Resource Sharing

CSA: TOP THREATS TO CLOUD COMPUTING 2024

In recent years, the cybersecurity awareness industry is increasingly focusing on human risk management, which is a more holistic approach to building strong security cultures.
However, as already mentioned, the challenge is compounded by a significant talent shortage in the cybersecurity field. According to the "ISC2's 2023 Workforce Study", the industry faces the largest professional shortage ever, with around 274,000 unfilled positions in the EU and *3.9 million vacancies* globally. Moreover, 44% of companies reported that they cannot find candidates with the necessary skills, reflecting a growing awareness of the specific expertise and experience required for cybersecurity roles. This trend also suggests a reduced capacity and willingness to invest in training and upskilling, as organisations increasingly seek ready-made talent to meet their needs.
This paper addresses these challenges and obstacles by offering a path forward and a collection of best practices that Salesforce organisations should follow to minimise potential cyber threats. It is crucial to engage with your CISO or head of IT security to address these potential vulnerabilities within Salesforce as part of your overall IT security defence strategy.

Copyright © 2024 Advension™. All rights reserved.

Cyber-Security Principles

Before discussing security principles, it is important to highlight the Confidentiality, Integrity, Availability (CIA) triad. This key model is widely used across many industries as a fundamental framework, guiding the development and implementation of an organization's security principles and measures.



Source: www.geeksforgeeks.org

In Salesforce, the CIA model is fully addressed, either through its core architecture or configurable features.
Confidentiality: This focuses on keeping data secure and private. In Salesforce, confidentiality is maintained through strong Authentication mechanisms and Access Controls, ensuring that only authorised users can access sensitive data.
Integrity: Integrity ensures that the data stored in Salesforce is accurate and protected from unauthorised changes. This is achieved by implementing effective Data Validation processes, such as validation rules, workflows, and approval processes. Additionally, Audit Trails and Data Backup and Recovery procedures play a critical role in preserving data integrity.
Availability: Salesforce is designed with high availability in mind, supported by a resilient and redundant architecture. The platform includes robust disaster recovery plans and DDoS protection measures to ensure that services remain available and reliable.

Salesforce Zero-Trust

While the CIA Triad provides high-level guidance for cybersecurity practices, Salesforce has fully adopted the Zero Trust model, a cybersecurity approach that assumes no connection to a corporate network is trustworthy by default. In this model, all users, devices, and systems must be authenticated before connecting and continuously re-verified at various checkpoints during their access.
This approach evolved from traditional perimeter-based security, which relied heavily on firewalls. The older model extended trust to all users and systems within the perimeter, leaving the infrastructure vulnerable to potential cybersecurity attacks. Zero Trust addresses these weaknesses by eliminating implicit trust and enforcing strict access controls.

The concept of Zero Trust was popularised by Forrester Research analyst John Kindervag in 2010, who emphasised that organisations should not extend trust to anything inside or outside their perimeters. (Forester.com)
However, the concept of a deperimeterization approach to cybersecurity dates back to 2004, when Jericho Forum member Paul Simmonds highlighted the challenges of relying solely on traditional perimeter-based security models.

At the core of the Zero Trust model is the Principle of Least Privilege (PoLP). PoLP dictates that users, systems, and processes should have only the minimum level of access or permissions necessary to perform their tasks. This ensures that individuals or systems are granted only the specific access rights needed for their job or function, reducing the risk of misuse or unauthorised access.

Other key security and architectural principles that should be carefully considered include:
Separation of Concerns (SoC): dividing a system into distinct sections, each with a specific responsibility, to reduce complexity and enhance security.
Segregation of Duties (SoD): ensures that critical tasks are divided among multiple individuals or systems to prevent fraud, errors, and conflicts of interest.

Copyright © 2024 Advension™. All rights reserved.

Defence Surface

The following sections explore the most critical security threats that could significantly impact Salesforce Org landscape and the organisation as a whole.

They provide a comprehensive guidelines and recommendations for the essential actions required to ensure robust protection.

The report is focused specifically on Salesforce best practices, however slightly expanding to related topics such as SSDLC, cultural challenges and organisational processes.

In alignment with the Salesforce Shared Responsibility Model, the report does not extensively cover security measures managed by Salesforce itself, though these are referenced where relevant.

The content of this report is based by the latest cybersecurity studies from Salesforce, IBM, Verizon, Cloudflare, and other leading organisations, as well as additional sources such as OWASP, CIS, and CWE, which are detailed in later sections.

Key Salesforce Security Topics

Salesforce Security Assessment
A comprehensive overview of the key reasons and critical aspects that need to be assessed within your Salesforce environment.

Salesforce Platform and System Security
An outline of the essential configurations required to safeguard your Salesforce orgs effectively.

Salesforce Application and Code Security
An in-depth exploration of the most critical security measures to implement in your code.

Development and Deployment Processes
Guidance on ensuring secure coding practices and a streamlined, secure deployment process.

Culture and Organizational Security
An evaluation of how your organization's culture, people, and related processes impact overall security.

Some of the most critical cyber threats around which defence points should be established, as discussed in this paper, include but are not limited to:

- **Phishing Attacks:** Deceptive emails or messages to trick users into revealing sensitive information or credentials.
- **Malware and Ransomware:** Malicious software that infiltrates systems to steal data, encrypt files, and demand a ransom for their release.
- **Insider Threats:** Unauthorised actions by rogue employees or contractors with access to Salesforce data, leading to data leaks or intentional harm.
- **Misconfigured Security Settings:** Exposing data and systems to unauthorised access due to incorrect configuration.
- **API Exploits:** Taking advantage of vulnerabilities in APIs to gain unauthorised access to data and functionality within Salesforce.
- **Data Exfiltration:** Unauthorised transfer of data from Salesforce to an external location, often facilitated by compromised credentials or insider actions.
- **SOQL/SOSL Injection:** Improperly sanitised input allows attackers to manipulate database queries, leading to unauthorised data access or modification.
- **Cross-Site Scripting (XSS):** Malicious scripts injected into web pages can compromise user sessions and steal sensitive information.
- **Cross-Site Request Forgery (CSRF):** Unauthorised commands transmitted from a trusted user, leading to unintended actions on behalf of the user.
- **Weak Password Policies:** Inadequate password complexity and expiration requirements make it easier for attackers to gain access to user accounts.

Approximately 46,000 new phishing sites are created every day, and on average, they are only active 4-8 hours.

MATTHEW GARDINER, DIRECTOR OF PRODUCT MARKETING

Copyright © 2024 Advension™. All rights reserved.

Salesforce Security Assessment

Can’t protect what you don’t know!

In a study conducted by Bitdefender involving 1,200 IT and cybersecurity experts across multiple countries, it was found that 44.7% of companies are conducting regular security assessments to monitor their cloud infrastructure. This is a growing trend!

BITDEFENDER 2024 CYBERSECURITY ASSESSMENT REPORT

Copyright © 2024 Advension™. All rights reserved.

Securing Salesforce: Why Security Assessment Matter

All stages of your implementation, from requirements to design, code to testing, and deployment, should adhere to specific security standards, typically structured within a Secure Development Lifecycle (SDL) framework. As part of your Salesforce SDL, conducting a thorough Security Assessment is critical for identifying and mitigating risks related to misconfigurations, weak coding practices, and improper access controls. These assessments enable organisations to gain a clear understanding of their Salesforce security landscape, uncover vulnerabilities, and implement the necessary controls to safeguard sensitive data.

Without regular security assessments, organisations risk exposing valuable data to cyber threats, which can result in significant financial losses, reputational damage, and a ultimately loss of customer trust.

This risk overview highlights the critical importance of conducting comprehensive and ongoing security assessments in Salesforce.

By proactively identifying and closing security gaps, organisations can better protect their most critical data and maintain the trust and confidence of their stakeholders.

Do you have a clear understanding of your current Salesforce setup? - *what has been configured and why!*

In fast-paced environments with tight deadlines, shortcuts often lead to neglecting key security practices, increasing the risk of Salesforce cybersecurity breaches. Understanding your Salesforce ecosystem, including configurations, access controls, and code security, is essential for safeguarding your organisation. Regular security assessments are crucial to identify vulnerabilities, ensure compliance with best practices, and protect against evolving cyber threats.



> *Security is always excessive, until it's not enough!*

ROBBIE SINCLAIR - HEAD OF SECURITY, COUNTRY ENERGY, NSW AUSTRALIA

Copyright © 2024 Advension™. All rights reserved.

Critical Areas for Assessment

In order to gain a comprehensive understanding of your Salesforce org's current security state, the security assessment should, at a minimum, address the following key areas.

Authentication and Access Control

Session Settings: Evaluate whether session timeouts and other security levels are appropriately configured to minimise the risk of unauthorised access during periods of inactivity.

Login Access Policies: Assess the effectiveness of login access policies, including IP restrictions and trusted networks, to ensure controlled and secure user logins.

Password Policies: Review the strength of password policies, focusing on complexity, expiration, and reuse rules, to ensure robust protection of user accounts.

Guest User Access: Examine how permissions and data access levels for guest users are managed, ensuring that public-facing Salesforce pages are appropriately safeguarded.

Connected Apps and Integration Users: Assess how connected apps have been configured, their scope and OAuth Policies. Additionally review existing integration user accounts and assess their access permissions.

> *71% Year-over-year increase in cyberattacks that used stolen or compromised credentials.*
>
> 2024 IBM X-FORCE THREAT INTELLIGENCE INDEX

Tools and Frameworks:

- Salesforce Security Health Check
- Salesforce Security Center
- Salesforce Optimizer



Copyright © 2024 Advension™. All rights reserved.

Sharing and Accessibility

Organisation-Wide Defaults (OWD): Determine if baseline access levels for data are correctly set across your organisation, ensuring users only access the data they need.

Profiles and Permission Sets: Review the definition and assignment of specific permissions and access rights to users, ensuring adherence to the principle of least privilege. Best practice: refactor profiles into needs/function specific permission sets.

Sharing Rules: Evaluate the configuration of additional sharing rules to ensure that data access is extended or restricted based on specific criteria, maintaining appropriate data sharing across teams.

Public Groups: Within the overall sharing model, Public Groups can grant unwanted access to records. Review and map group memberships to ensure their access is still appropriate and necessary.

> *Miscellaneous Errors, Privilege Misuse and System Intrusion represent 83% of breaches. Where financial and espionage motives contribute to 88%, and 46% respectively.*
>
> VERIZON 2024 DATA BREACH INVESTIGATION REPORT

Tools and Frameworks:

- Salesforce Security Center
- AppExchange Apps



Copyright © 2024 Advension™. All rights reserved.

Code Security

Apex: Assess the security of Apex code, ensuring it is free from vulnerabilities like SOQL injection, record and FLS[1] verification aligns with best practices.

Lightning Components (Aura, LWC): Assess the input validation and data handling to prevent client-side attacks such as XSS and CSRF, ensuring strong coding standards are in place to protect against common web vulnerabilities.

Visualforce: Examine Visualforce pages for security, ensuring inputs are validated and vulnerabilities like CSRF and XSS are mitigated.

Flows: Validate the security of Salesforce Flows, ensuring they operate with proper access controls and do not expose sensitive data.

Installed Packages: Assess and monitor installed packages to ensure they do not introduce security risks or conflicts within your org.

Tools and Frameworks:

- Salesforce Code Analyzer
- Checkmarx Code Scanner
- Apex PMD
- ESLint
- Salesforce Extension Pack for VS Code



OWASP's Web Application Penetration Checklist highlights that inadequate validation of input, such as insufficient checks for SQL injections and other script injections, is a common vulnerability in weak code security, leading to breaches.

OWASP WEB APPLICATION PENETRATION CHECKLIST

1. *FLS: Field Level Security*

Copyright © 2024 Advension™. All rights reserved.

Salesforce Platform and System Security

It's a Shared Responsibility Model!

According to a CyberArk report based on a global survey of 2,400 security decision-makers across 18 countries, platform misconfiguration is identified as one of the leading security concerns.

CYBERARK THREAT LANDSCAPE REPORT 2024

Copyright © 2024 Advension™. All rights reserved.

Essential Security Configurations and Best Practices

In today's evolving cybersecurity landscape, ensuring the security of your Salesforce environment is paramount. This section identifies key areas within Salesforce that, if not properly configured or implemented, could serve as potential attack vectors.

To maintain a clear focus, we've highlighted the most critical aspects while providing a more comprehensive list of Salesforce features requiring attention in the appendix.

Each section is supported by relevant industry statistics to emphasise the importance of these security measures.

From authentication and access control to data encryption and third-party integrations, this guide outlines essential strategies your organisation must consider to safeguard sensitive data, prevent breaches, and maintain a robust security posture.

How confident are you that your Salesforce setup is securely configured and capable of defending against potential cyber threats?

This is a challenging question, particularly for fast-growing organisations where the priority is often speed to market. In such environments, implementation and configuration can unintentionally overlook security measures and best practices, leading to critical vulnerabilities. These gaps can become highly attractive targets for unauthorised individuals and groups looking to exploit them.



> *Defenders have to be right every time. Attackers only need to be right once.*
>
> UNKNOWN AUTHOR

Copyright © 2024 Advension™. All rights reserved.

Key Areas to Address

The following sections highlight key areas within Salesforce that, if not properly configured or implemented, could be vulnerable to various attack vectors. To keep this overview concise, only the most critical aspects are emphasised.

Authentication and Access Control

Session Settings: Configure session timeouts and security settings to automatically log users out after inactivity, minimising the risk of unauthorised access.

Browser Security Settings: Enforce browser security settings to protect against common web-based threats, such as Referrer URL Protection and Public Key Pinning.

Login Access Policies: Implement strict login access policies, controlling when and from where users can access Salesforce, including setting login hours and IP restrictions.

Custom Login Flows: Develop custom login flows for high-risk users, such as administrators, incorporating additional authentication methods or security checks.

Password Policies: Enforce strong password policies with complexity, expiration, and reuse restrictions to secure user accounts.

High-assurance Session: Require high-assurance sessions for accessing sensitive data or performing critical tasks to ensure the highest level of security.

Single Sign-On (SSO): Implement SSO to streamline authentication and enforce consistent security policies across all connected applications.

Multi-Factor Authentication (MFA): Mandate MFA for all users to add an extra layer of security, ensuring that compromised credentials alone are not enough to gain access.

> *Compromised credentials were involved in approximately 38% of all data breaches!*
>
> 2024 VERIZON DATA BREACH INVESTIGATIONS REPORT

IP Whitelisting: Restrict access to Salesforce from trusted IP addresses only, enhancing security by blocking unauthorised network access.

Disable Dormant Accounts: Regularly review and deactivate inactive user accounts to minimise security risks and reduce access points for attackers. Maintain a clear inventory of all accounts, including alias and shared accounts used by multiple users.

Copyright © 2024 Advension™. All rights reserved.

> *21% of data breaches involve misuse of internal privileges, highlighting the importance of proper data sharing and visibility controls.*
>
> 2023 VERIZON DATA BREACH INVESTIGATIONS REPORT

Data Sharing and Visibility

Organisation-Wide Defaults (OWD): Set OWDs to establish baseline access levels, ensuring that users only have access to the data they need. Keep in mind the impact on performance, especially if the org hosts large volume of records.

User Roles: Define and structure user roles that reflect access to information rather than organisation's hierarchy, ensuring that data access aligns with job responsibilities.

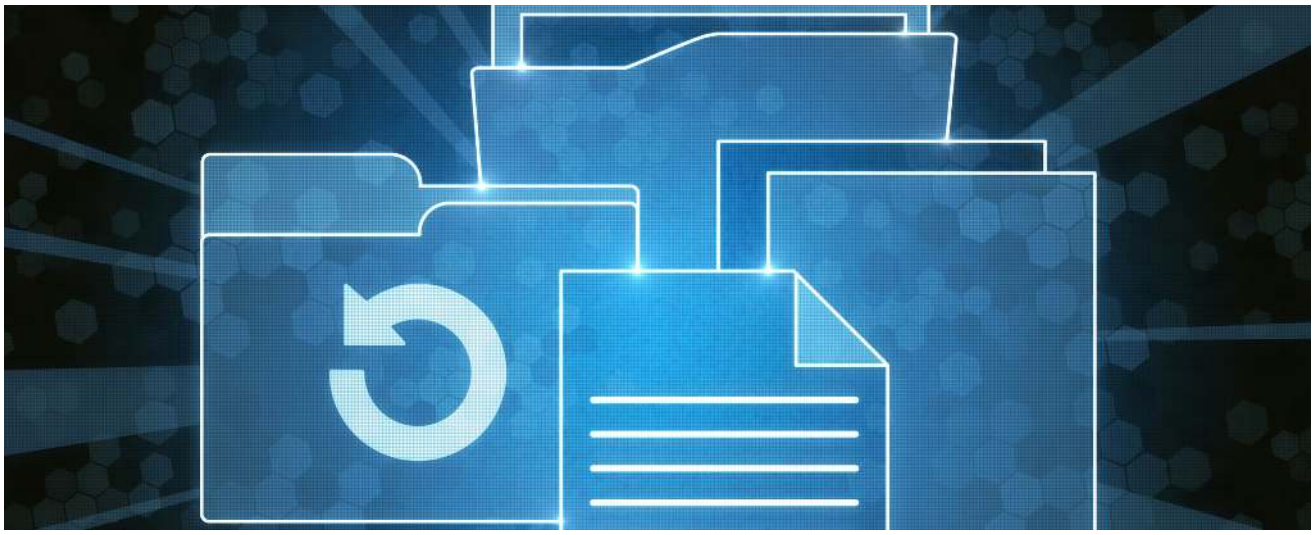
Sharing Rules: Configure sharing rules to extend or restrict data access based on specific criteria, allowing for controlled and secure data sharing across teams.

User Access and Permissions

Profiles and Permission Sets: Keep profiles configured with minimal access and refactor permissions into need/function-specific permission sets. This approach enforces the principle of least privilege, ensuring users have only the permissions necessary for their specific roles.

Experience Cloud Guest User Access: Carefully manage guest user access in Experience Cloud, ensuring they only interact with public data and resources.

Salesforce Public Groups: Use public groups to manage user permissions and sharing settings to reduce the overall sharing rules complexity, and reducing the risk of uncontrolled data access. *Keep in mind the impact on performance!*



Copyright © 2024 Advension™. All rights reserved.

> *A study by Varonis revealed that 53% of companies have over 1,000 sensitive files open to all employees, emphasizing the importance of controlling data exports.*
>
> VARONIS DATA RISK REPORT

Data Export Controls

Transaction Policies: Implement transaction policies to monitor and control data exports, ensuring they align with security and compliance requirements.

Connected Apps Scope: Limit the scope of connected apps to restrict the data they can access and export, reducing the risk of unauthorized data sharing.

Data Export Service: Monitor and restrict the use of the Data Export Service, ensuring that only authorized personnel can perform large-scale data exports.

Data Loader: Control access to the Data Loader tool, allowing only trusted users to perform bulk data imports and exports.

Browser Apps: Restrict the use of browser extensions and apps that can interact with Salesforce data to prevent unauthorised exports.

Backup Solutions: Ensure that backup solutions are configured to securely store and encrypt data, preventing unauthorised access to backup files.

Data Encryption

Data Classification: Implement data classification to identify and categorize sensitive data, applying appropriate encryption measures.

File Encryption: Encrypt files and attachments stored in Salesforce to protect them from unauthorized access, both at rest and in transit.

Data Masking: Apply data masking techniques to anonymize sensitive data in non-production environments, reducing the risk of exposure.

Bring Your Own Key (BYOK): Use BYOK to manage your own encryption keys, giving you control over encryption processes and enhancing data security.

Monitoring and Auditing

Event Monitoring: Leverage Event Monitoring to track and analyze user activity and system events, enabling proactive detection of security threats.

Event Log Files: Regularly review Event Log Files to monitor access and changes within Salesforce, identifying any suspicious behavior.

Audit Trail: Maintain an audit trail of administrative changes and access to sensitive data, ensuring accountability and compliance.

Field History Tracking: Enable Field History Tracking to monitor changes to critical data fields, providing visibility into data modifications.

API Anomaly Event: Monitor API Anomaly Events to detect unusual API usage patterns that could indicate a security breach.

SessionHijackingEvent: Track SessionHijackingEvents to identify and respond to potential session hijacking attempts, protecting user sessions from unauthorized access.

Copyright © 2024 Advension™. All rights reserved.

Third-party Apps and Integrations

Integration Users: Create dedicated integration users with limited permissions for third-party apps, ensuring they only access necessary data and functions.

Connected Apps: Regularly review and secure connected apps to prevent them from introducing vulnerabilities or exposing sensitive data. Visit Salesforce for more technical details.

Salesforce Connect: Use Salesforce Connect to securely integrate external data sources, ensuring that data is accessed and shared in a controlled manner.

Installed Packages: Evaluate installed packages for security risks, ensuring they do not introduce vulnerabilities into your Salesforce environment.

Sandbox Management

Dormant Sandbox Orgs: Regularly review and deactivate dormant sandbox orgs to reduce the attack surface and prevent unauthorized access.

User Account Control: Manage user accounts in sandbox environments carefully, ensuring that only necessary users have access and that sensitive data is masked or anonymised.



The Verizon 2024 Data Breach Investigations Report notes that third-party apps and integrations are among the top vectors for cyber breaches in cloud environments. This highlights the importance of vetting third-party applications and ensuring they adhere to strict security protocols before integration.

VERIZON 2024 DATA BREACH INVESTIGATIONS REPORT

Copyright © 2024 Advension™. All rights reserved.

Salesforce Application and Code Security

Code fast, fail fast, lose everything!

79% of security breaches are caused by vulnerabilities in application code, often due to inadequate testing or failure to adhere to secure coding practices.

IBM X-FORCE THREAT INTELLIGENCE INDEX 2024

Copyright © 2024 Advension™. All rights reserved.

Best Practices for Securing Apex, Visualforce, and LWC

As the complexity of applications grows and the sensitivity of the data they handle increases, so does the potential for cybersecurity threats.

Salesforce developers and administrators must be vigilant in defending against key threats, including SOSL/SOQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), and the use of insecure external library resources.

This section provides a comprehensive approach to securing your Salesforce environment by implementing best practices across key areas such as Apex, Lightning Components (Aura, LWC), Visualforce, and Flows.

By following these guidelines, you can effectively mitigate these threats, ensuring that your applications are both resilient and secure, thereby protecting your critical data and maintaining the trust of your users.

Is your code truly secure? Have you conducted thorough penetration testing? Are you prepared to stake your career on it?

These are critical questions to consider, especially when the average cost of a cybersecurity breach hovers around $4 million USD—not to mention the potential damage to your company's reputation and customer loyalty. In the EU, failing to invest in adequate security measures, particularly when customer and employee data is compromised, can lead to fines of up to €10 million or 2% of global revenue, whichever is higher. This underscores the immense pressure CISOs face daily to protect their organisations from devastating breaches.



> *It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently.*
>
> WARREN BUFFETT

Copyright © 2024 Advension™. All rights reserved.

Essential Code Security Measures

The following sections explore the most critical security practices to consider when building Lightning Components, Visualforce pages, and Apex controllers, aimed at minimizing the potential attack surface.

Apex Security

SOQL Injection: Always use bind variables in your Apex code to prevent SOQL injection. Avoid dynamic SOQL queries and ensure that any user input is properly escaped or sanitized before it's used in a query. This prevents attackers from inserting malicious code that could compromise your database.

Insecure Direct Object References (IDOR): Implement thorough access checks in your Apex controllers to ensure users can only access records they have permission to see. Always use the “with sharing” keyword to enforce sharing rules and avoid exposing sensitive records through URLs or unprotected APIs.

Input Validation: Validate all user inputs rigorously using built-in Salesforce methods like “isNumeric()”, “isEmail()”, or custom validation logic. This prevents unexpected or malicious data from being processed in your applications, reducing the risk of security vulnerabilities.

Apply FLS (Field-Level Security): Respect field-level security in your Apex code. Use “Schema.getGlobalDescribe()” and “SObjectType” methods to check FLS before performing CRUD operations. This ensures that sensitive fields are not exposed to users who should not see them.

Hardcoded Credentials: Never hardcode credentials or sensitive information in your Apex code. Instead, use Named Credentials, Custom Metadata Types, or Encrypted Custom Settings to store and retrieve such data securely.

> *Over 90% of security incidents can be traced back to vulnerabilities in software code, with poor coding practices being a significant contributor to these breaches*
>
> 2024 VERIZON DATA BREACH INVESTIGATIONS REPORT

Error Handling: Implement robust error handling in your Apex code, but avoid exposing sensitive details in error messages. Use custom exceptions to manage errors gracefully and log them securely for further investigation without leaking sensitive information.

Sensitive Data in Debug Logs: Avoid logging sensitive data in debug logs. If logging is necessary, use obfuscation techniques or ensure that sensitive data is masked before it's logged. This prevents exposure of sensitive information through logs that might be accessible to unauthorized users.

Copyright © 2024 Advension™. All rights reserved.

Lightning Components (Aura/LWC)

Data Binding: Use secure data binding practices by avoiding direct binding of sensitive data to components. Always validate and sanitise data before binding it to prevent injection attacks or data leakage.

Component Access Control: Define strict access controls for your Aura and LWC components using “access” modifiers like “public”, “private”, or “global”. This ensures that only authorised components can interact with each other, reducing the risk of unauthorised data access.

Client-Side Logic: Avoid placing sensitive business logic in client-side controllers. Instead, delegate critical operations to server-side Apex controllers where security checks can be more thoroughly enforced. This minimises the risk of client-side manipulation.

Event Handling: Handle events dispatching in a way that prevents unauthorised access to data. Limit the scope of event communication to only those components that need to know, and validate event data to avoid unintended data exposure.

Error Handling: Implement client-side error handling that gracefully handles failures without exposing internal logic or sensitive data to the end user. Display user-friendly error messages while logging detailed errors on the server for further analysis.

Input Validation: Perform input validation both on the client side and the server side. Ensure that all user inputs are checked for type, format, and length to prevent injection attacks or data corruption.

Referencing Third-party Libraries: Only include third-party libraries from trusted sources, and ensure they are kept up to date with the latest security patches. Never load directly from an external location, but always save the library as a Static Resouce. Validate and sanitize any data processed by these libraries to avoid introducing vulnerabilities into your application.

Visualforce

Input Validation: Validate all user inputs before processing them on the server. Use Visualforce standard validation functions and implement custom validation logic to prevent injection attacks and ensure data integrity.

Access Control: Enforce access control on Visualforce pages by using the “with sharing” keyword in associated Apex controllers and checking for appropriate user permissions before displaying sensitive data.

Prevent Clickjacking: Implement protections against clickjacking by including the “X-Frame-Options” HTTP header in your Visualforce pages. This ensures that your pages cannot be embedded in iframes on other sites, protecting users from malicious redirects.

Errors and Warnings Information Leakage: Avoid exposing detailed error messages to end users. Instead, provide generic error messages while logging detailed information securely on the server. This prevents attackers from gaining insights into your application's inner workings.

Sensitive Data in URLs: Refrain from including sensitive information in query strings or URLs. If necessary, use POST methods or secure session storage to transmit sensitive data, reducing the risk of data exposure.

Referencing Third-party Libraries: Reference third-party libraries from reputable sources, and ensure they are served over HTTPS. Regularly update these libraries to patch any known vulnerabilities and validate all data processed by them.

Copyright © 2024 Advension™. All rights reserved.

Salesforce Flows

Access Control: Apply appropriate access control settings on Flows to ensure that only authorised users can execute them. Use permission sets or profiles to restrict access based on the principle of least privilege.

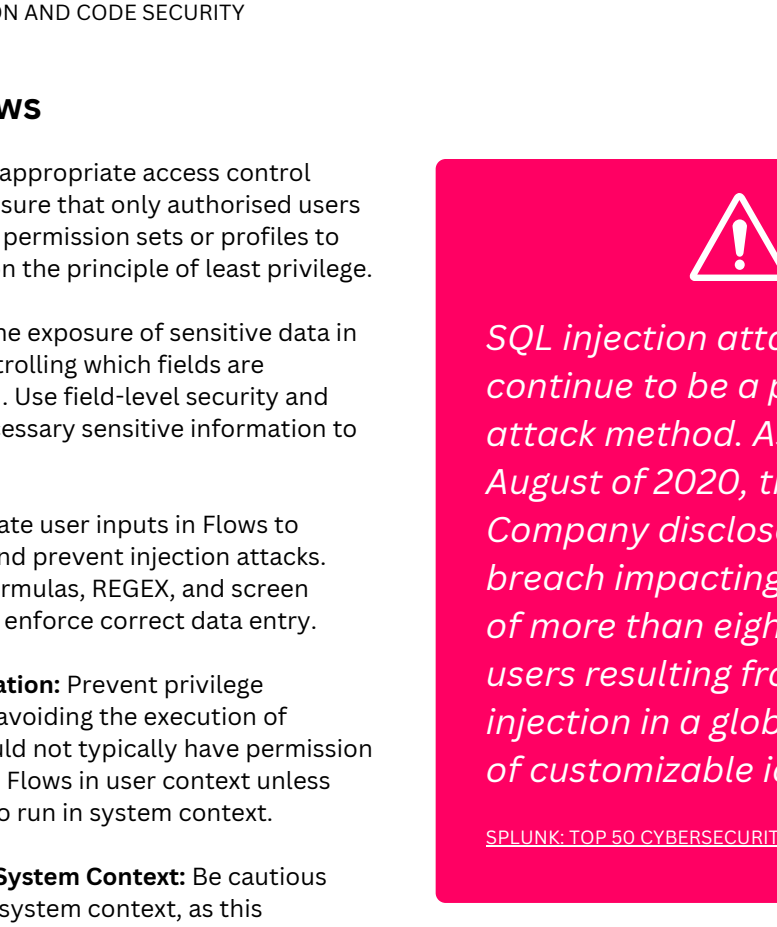
Data Exposure: Limit the exposure of sensitive data in Flows by carefully controlling which fields are accessed and modified. Use field-level security and avoid displaying unnecessary sensitive information to users.

Input Validation: Validate user inputs in Flows to ensure data integrity and prevent injection attacks. Use validation rules, formulas, REGEX, and screen component settings to enforce correct data entry.

Misuse Privilege Escalation: Prevent privilege escalation in Flows by avoiding the execution of actions that a user would not typically have permission to perform. Always run Flows in user context unless absolutely necessary to run in system context.

Unrestricted Access - System Context: Be cautious when running Flows in system context, as this bypasses user permissions. Only use system context for operations that genuinely require it and ensure thorough validation and auditing of such Flows.

Sensitive Data in Debug Logs: Avoid logging sensitive information in Flow debug logs. If logging is necessary, ensure that data is masked or obfuscated to prevent unauthorised access to sensitive information through logs.



SQL injection attacks continue to be a popular attack method. As recently as August of 2020, the Freepik Company disclosed a data breach impacting the logins of more than eight million users resulting from an SQL injection in a global database of customizable icons.

SPLUNK: TOP 50 CYBERSECURITY THREATS



Copyright © 2024 Advension™. All rights reserved.

Development and Deployment Processes

S!#t ...but it worked great in Sandbox!

The cost to fix a defect found after product release was 4 to 5 times more expensive than fixing one found during the design phase, and up to 100 times more expensive than one identified during the coding phase.

IBM SYSTEMS SCIENCE INSTITUTE

Copyright © 2024 Advension™. All rights reserved.

The Importance of Secure Code and Controlled Deployment Process

In Salesforce development, while the risks of unintentional misconfigurations are well-recognised, the dangers posed by insecure code and loose deployment processes can be equally severe.

Poor coding practices and inadequate deployment controls can lead to security breaches, exposing your organisation to significant threats. Strengthening your Salesforce security defences requires a focus on robust development and deployment practices.

Secure coding is your first line of defence, ensuring your code is resilient against vulnerabilities. Automated testing is vital for enhancing code security compliance, with unit tests helping to identify vulnerabilities early in the development cycle.

Regression tests are crucial for detecting unintended loopholes that may emerge as your codebase evolves.

Additionally, leveraging automated deployment processes, such as Continuous Integration and Continuous Deployment (CI/CD), enables seamless integration of security checks, version tracking, and rollback capabilities, preventing flawed and insecure code from being deployed.

Utilising scratch orgs to enforce compliance and detect issues early in the development process further bolsters your security posture. By adopting these practices, you can release updates quickly and securely, minimising risks while maintaining the integrity of your Salesforce environment.

Is your production code and deployment process truly Secure by Design? Is your development following any SSDLC[1] or DevSecOps[2] framework?

If not, you're teetering on the brink of a cybersecurity disaster that could strike without warning. A single mistake, like accidentally setting your Git repository to public could expose your entire Apex, LWC, and Salesforce Org metadata. Automated crawlers relentlessly search for such vulnerabilities, and by the time you realise it, it may already be too late.
Rushing to write code without rigorous testing isn't just risky, it's a disaster waiting to happen. Ignoring the "Secure by Design" principle opens dangerous attack vectors, and when a breach occurs, poorly structured code turns a quick fix into a long, painful process, delaying critical security patches and leaving your organisation vulnerable. The consequences could be catastrophic.

1. *SSDLC: Secure Software Development Lifecycle*
2. *DevSecOps: Development, security and operations*

Copyright © 2024 Advension™. All rights reserved.



> *If you spend more on coffee than on IT security, you will be hacked. What's more, you deserve to be hacked!*
>
> RICHARD CLARKE

Key Development and Deployment Strategies

Ensuring your Salesforce apps are robust and secure begins with safeguarding your code and deployment processes.
These straightforward steps will help you avoid common pitfalls and maintain a stable, secure platform.

Development Security

Code Readability: Ensure that your code is clean, well-organized, and easy to understand. Clear and readable code reduces the likelihood of introducing security vulnerabilities and makes it easier for others to review and maintain.

Code Review / Audit: Implement a mandatory code review process where peers audit code before it is merged. Regular audits help identify potential security issues early and enforce adherence to secure coding practices.

Static Code Analysis: Use tools like PMD and Salesforce Code Analyzer to automatically scan your code for vulnerabilities. Integrate these tools into your CI/CD pipeline to catch security flaws before they reach production.

Code Hardening: Apply secure coding standards and principles, such as input validation, output encoding, and proper error handling. Harden your code to resist attacks like injection, XSS, and CSRF.

GIT Repository Security: Protect your Git repositories with Multi-Factor Authentication (MFA) and ensure frequent secret resets. Always keep repositories private to prevent unauthorised access and accidental data exposure.

Managed Packages: For critical functionality, consider compiling it into a second-generation managed package (2GP). This approach can protect your intellectual property and ensure that critical code is securely distributed.

Unit Tests: Apex Test Classes: Develop comprehensive Apex test classes to cover all possible security scenarios, ensuring your code behaves as expected. Check for Sensitive Information: Ensure that unit tests do not include or expose sensitive information, such as credentials or personal data, which could be inadvertently leaked.

Verify NPM Packages: Regularly verify the integrity and security of NPM packages used in your projects. Only use packages from trusted sources, and keep them up to date with the latest security patches.

Copyright © 2024 Advension™. All rights reserved.

Deployment Security

Controlled Environments: Deploy code only to controlled and secured environments. Use isolated environments for development, testing, and production to minimize the risk of unauthorized access and data leakage.

Localized Responsibility: Restrict deployment permissions to a small group of trusted individuals. Ensure that responsibilities are localized to specific roles, reducing the risk of accidental or malicious deployments.

Versioned Artifacts, Clear Release Notes: Ensure that all deployment artifacts are versioned, and accompany each release with clear and detailed release notes. This practice helps in tracking changes and understanding the impact of each release.

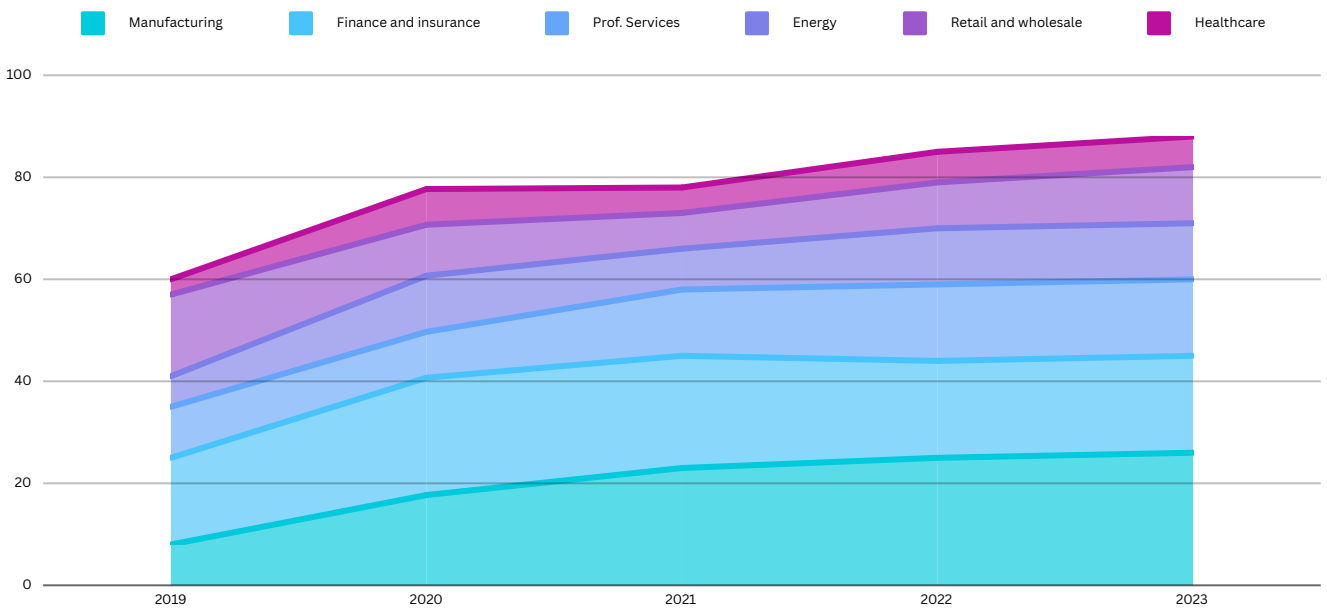
Automated Testing: Integrate automated testing into your deployment pipeline, covering functionality, load, and performance tests. Automated tests ensure that the application meets security and performance standards before going live.

Security Checks: Include security checks as a mandatory step in the deployment process. Automate the verification of security configurations and compliance with security policies to prevent vulnerabilities from being deployed.
Involve your CISO team!

Quick Security Patch Releases - Hot Fixes: Establish a rapid deployment process for security patches and hot-fixes. Ensure that critical vulnerabilities can be patched and deployed to production as quickly as possible to minimise exposure.

Clear Release Planning: Develop and follow a clear release plan that includes security considerations. Plan for potential security issues and ensure that all stakeholders are aware of the deployment schedule and any associated risks.

Share of attacks by industry 2019–2023



Source: IBM X-Force Threat Intelligence Index 2024

Copyright © 2024 Advension™. All rights reserved.

Culture and Organisational Security

...people, a weakest link, or a strongest defence!

In a survey conducted by SoSafe, 68% of security professionals are suffering from burnout, with 32% experiencing high burnout and 36% experiencing moderate symptoms. Alarmingly, 83% of IT security professionals admit that burnout has caused errors in their department that led to security breaches.

SOSAFE - HUMAN RISK REVIEW 2024

Copyright © 2024 Advension™. All rights reserved.

Building a Strong Security Culture: The Key to Organizational Resilience

In today's digital landscape, the greatest threat to organisational security is not merely technological flaws but the behaviours and attitudes of the people within the organisation. As cyber threats continue to evolve in complexity and frequency, the role of human factors in maintaining robust cybersecurity has become increasingly critical.

A strong security culture is the bedrock upon which an organisation's defence mechanisms are built. It not only empowers employees to recognise and mitigate risks but also ensures that cybersecurity becomes an intrinsic part of the organisation's DNA.

The impact of a well-embedded security culture extends far beyond compliance and awareness. It influences every aspect of the organisation's security posture. From reducing the incidence of human error, often the weakest link in cybersecurity defences, to fostering an environment where security is prioritised at every level, a proactive and pervasive security culture is essential.

This section delves into how cultivating a strong security culture can fortify an organisation's defences, mitigate risks, and ultimately contribute to a more resilient and secure enterprise.

Are mounting stress and burnout among your employees creating dangerous vulnerabilities in your cybersecurity defences, risking a catastrophic breach?

Unaddressed employee stress is a leading cause of toxic work environments, where individuals prioritise personal interests and survival over the organisation's well-being. Such cultures often lead to privilege misuse, with disgruntled employees turning against the organisation, resulting in serious data and cybersecurity breaches. Additionally, IT security teams, deeply affected by these toxic environments, experience significant stress, potentially compromising the most critical segment of the organisation's defence.



> *A lot of companies are clueless, because they spend most or all of their security budget on high-tech security like fire walls and biometric authentication - which are important and needed - but then they don't train their people.*

KEVIN MITNICK

Copyright © 2024 Advension™. All rights reserved.

Addressing the Human Side of Cybersecurity

Effective cybersecurity relies on every team member. This guide offers actionable steps to address the key challenges, improve training, and build a security-first culture across your organisation.

The impact of a toxic culture on cybersecurity defence

An unhealthy culture can severely undermine your organisation's cybersecurity defences, leading to both employee attrition and high customer churn rates. In toxic cultures, where a blame-game mentality prevails, individuals are often punished for mistakes.

In such environments, a significant number of incidents may go unreported, as employees are less likely to come forward with errors or suspicious activities.

A toxic or punitive security culture increases the likelihood that incidents caused by employees will be hidden rather than disclosed, further compromising organisational security. (SANS 2024 Security Awareness Report)

> *75% of employees are more likely to report a security issue if they believe it will be addressed positively and without retribution.*
>
> SANS 2024 SECURITY AWARENESS REPORT

Key Challenges

Based on our analysis and data insights provided by sources such as CyberArk, SANS, ISC2, SoSafe, and more, we have compiled a list of the top five most common challenges faced by companies with unhealthy cultures.

These challenges not only have a significant impact on overall cybersecurity defence but also perpetuate and exacerbate degrading cultural behaviours

Top 5 Cultural Challenges

1. Poor Accountability and Lack of Ownership
2. High Employee Turnover
3. Complacency and Resistance to Change
4. Lack of Communication and Collaboration
5. Inadequate Training and Continuous Learning

The following section, dives into some key best practices that can help address some of these challenges.

Copyright © 2024 Advension™. All rights reserved.

Outcomes with direct impact to the Organisational Security

The challenges mentioned before are just a few among a long list of potential cultural obstacles that significantly impact security defence but are often overlooked and not prioritised.
Ignoring these challenges leads to outcomes that place an enormous burden on security team operations and compromise overall organisational security integrity.
The following outcomes are among the most critical and demand full attention to be effectively addressed:

Unresolved Security Issues: Poor accountability and lack of ownership result in critical security vulnerabilities being neglected, leaving the organisation exposed to potential attacks.

Loss of Institutional Knowledge and Security Gaps: High employee turnover disrupts continuity and creates knowledge gaps, weakening the organisation's ability to maintain and enhance its security posture.

Stagnant Security Practices: Complacency and resistance to change prevent the adoption of necessary updates and technologies, making the organisation more susceptible to emerging threats.

Disjointed Security Efforts and Missed Threats: Lack of communication and collaboration leads to fragmented security strategies, increasing the likelihood of overlooked vulnerabilities and ineffective threat responses.

Unprepared Workforce: Inadequate training and continuous learning result in a workforce that is ill-equipped to recognise and respond to evolving cybersecurity threats, heightening the risk of security breaches.

Inconsistent Enforcement of Security Policies: When there is a lack of consistent enforcement of security policies, employees may become lax in following procedures, leading to widespread non-compliance and increased risk of breaches.

Increased Insider Threats: Unhealthy cultures can foster resentment or disengagement among employees, increasing the likelihood of malicious insider activities such as data theft or sabotage.

Low Employee Morale and Engagement: In an unhealthy culture, low morale and disengagement can lead to negligence or even intentional disregard for security practices, making the organisation more vulnerable to insider threats.

Ineffective Incident Response and Recovery: A culture that does not prioritise or adequately support its security teams may result in slow, disorganised, or ineffective responses to security incidents, exacerbating the damage caused by breaches.

Lack of Innovation in Security Measures: A risk-averse or stagnant culture may discourage innovation, leading to outdated security practices and tools that are ineffective against modern cyber threats.

Erosion of Trust in Security Leadership: If leadership fails to support or communicate effectively with the security team, it can lead to a lack of trust and respect, undermining the overall effectiveness of security initiatives.

Increased Compliance Risks: An unhealthy culture may lead to neglect in meeting regulatory requirements and industry standards, resulting in legal penalties, reputational damage, and increased vulnerability to attacks.

Fragmented Security Architecture: In organisations where departments do not collaborate or share information effectively, the result is often a disjointed and inefficient security architecture, with gaps that can be easily exploited by attackers.

Proliferation of Shadow IT: In environments where employees feel unsupported or restricted, they may resort to using unauthorised tools and applications (shadow IT), which can introduce vulnerabilities and increase the attack surface.

High Cost of Security Breaches: The cumulative effect of these cultural issues often leads to more frequent and severe security breaches, which not only harm the organisation financially but also damage its reputation and customer trust.

Copyright © 2024 Advension™. All rights reserved.

Best Practices to heal and grow a healthy Security Culture

Define Clear Roles and Responsibilities: Ensure every employee understands their role in maintaining cybersecurity and holds themselves accountable for their actions.

Establish Accountability Structures: Implement mechanisms for monitoring and enforcing security responsibilities across all levels of the organisation.

Regular Training Programs: Implement ongoing, role-specific cybersecurity training to keep employees updated on the latest threats and best practices.

Encourage Certifications and Skill Development: Support employees in obtaining cybersecurity certifications and participating in professional development opportunities.

Break Down Departmental Silos: Establish cross-functional teams and regular meetings focused on cybersecurity to foster collaboration and information sharing.

Implement Transparent Reporting Channels: Create secure, anonymous channels for reporting security concerns or suspicious activities without fear of retaliation.

Embrace New Technologies: Encourage the adoption of new cybersecurity tools and practices, ensuring they are integrated smoothly into the organisation.

Promote a Culture of Continuous Improvement: Regularly review and update security policies and procedures to reflect evolving threats and innovations.

Address Workload and Burnout: Provide resources and support to reduce stress and prevent burnout among cybersecurity teams.

Recognise and Reward Good Practices: Acknowledge and reward employees who demonstrate strong cybersecurity practices, reinforcing positive behaviour.

Adjust Strategies Based on Data: Use the insights from surveys and feedback to continuously improve and adapt your cybersecurity culture initiatives.

> *85% of employees feel more motivated to adhere to security practices when they are recognized and rewarded for their efforts.*
>
> SANS 2024 SECURITY AWARENESS REPORT

C-Level Engagement: Ensure that leadership visibly supports and prioritises cybersecurity initiatives, setting the tone for the entire organisation.

Embed Security in Corporate Values: Integrate cybersecurity into the core values and mission of the organisation, making it a fundamental part of the company's culture.

Develop a Robust Incident Response Plan: Create and regularly update an incident response plan that outlines specific steps for managing security incidents.

Conduct Regular Drills: Perform simulations and tabletop exercises to ensure all departments are prepared to respond effectively to cybersecurity incidents.

Gamify Security Training: Use gamification techniques in training programs to engage employees and encourage active participation in security initiatives.

Host "Lunch and Learn" Sessions: Organise informal educational sessions where employees can learn about cybersecurity in a relaxed setting.

Regular Surveys and Feedback: Conduct regular surveys to gauge employee attitudes towards cybersecurity and gather feedback on the effectiveness of security initiatives.

Copyright © 2024 Advension™. All rights reserved.

Summary

Security should be seen not merely as an IT concern but as an organisational asset that provides significant value to customers, directly impacting the business revenue model, product development, and service offerings.
The global surge in cyberattacks, especially against cloud solutions, is undeniable and demands full attention and proactive measures.
While traditional phishing emails remain prevalent, there has been a rise in deep fake phone and video calls attacks due to AI advancements and an increase in malware spread through chat applications.

The key reason for the success of phishing campaigns is their cost-effectiveness compared to attacking fortified networks, as human error remains the weakest link.

However, fostering a strong security culture, implementing training, and using recognition methods can greatly enhance security.

In Salesforce, security can be significantly strengthened by making improvements at the platform, code, and deployment level.

Limitations

This research is primarily focused on the Salesforce Core, including Sales and Service Cloud as well as Industry Cloud, though it does not exclude other Salesforce cloud solutions, such as Account Engagement (formerly Marketing Cloud and Pardot), or the broader IT landscape.

While this paper does not cover overall IT and physical security, these areas remain crucial and should be thoroughly evaluated. Most statistical data is from 2022 and 2023, but recent trends, particularly in the US, suggest changes in the CISO role, with some reports indicating a decline in traditional CISO positions. This could indicate that the role is evolving, requiring new skill sets such as strong business acumen and the ability to translate complex technical concepts into simpler, business-relevant terms.

Implications

Employees can indeed be your greatest threat to organisational security or your strongest defence, a “human firewall”.

Numerous reports indicate that poorly treated employees can become disgruntled insiders who directly compromise security.

That being said, if security is not properly managed, the consequences for customer trust, business operations, and brand reputation can be severe.

Additionally, security failures can increase employee stress, lead to higher turnover, and make it difficult to attract skilled talent, ultimately harming the company’s image and its ability to recruit top professionals.

Next Steps

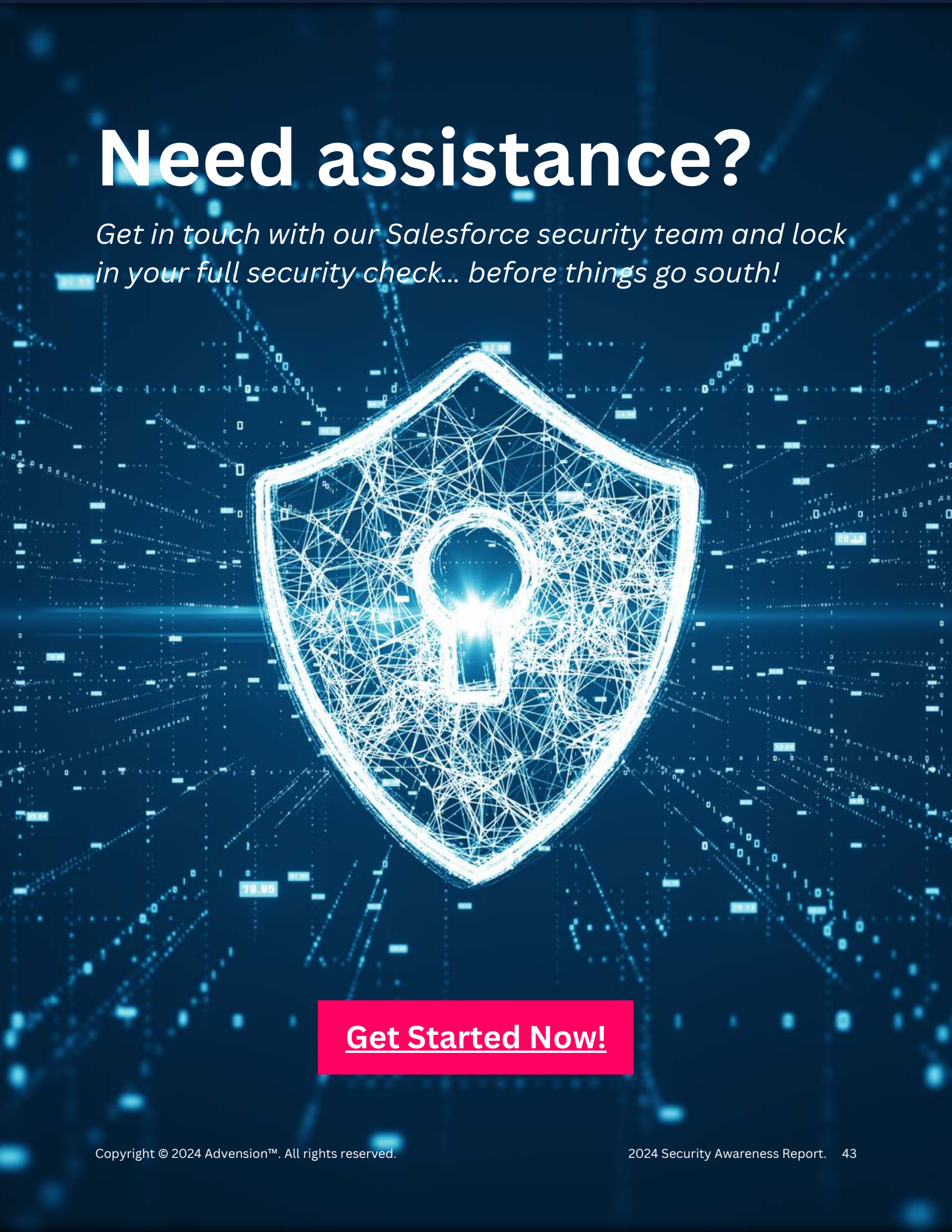
The purpose of this report is to equip you with comprehensive information, resources, analytical data, and best practices, particularly focused on the technical aspects of Salesforce, to safeguard your customers' data.
However, to fully ensure that all cloud-specific configurations align with your security practices, additional steps are necessary.
Here are a few next steps you can take to elevate this process to the next level:

1. *Clearly define what is that you want to protect*
2. *Engage your CISO in your Salesforce dev activities.*
3. *Train your people to think Security First.*
4. *Invite external experts to share best practices.*
5. *Perform regular security assessment.*
6. *Pentest your solutions.*
7. *Automate Security Regression Testing.*
8. *Create an internal bounty program.*
9. *Establish continuous monitoring and threat analysis.*
10. *Implement Zero Trust Architecture.*

Copyright © 2024 Advension™. All rights reserved.

Need assistance?

Get in touch with our Salesforce security team and lock in your full security check... before things go south!



Get Started Now!

Copyright © 2024 Advension™. All rights reserved.

Acknowledgement

About the Author

Alexander Stojanovic is a seasoned Business, Technology, and Security Strategist, and a certified Salesforce Solution Architect with a strong background in MedTech, Health Services, and Financial Services.
He specializes in Cloud Security, particularly with Salesforce CRM, Oracle, and AWS, focusing on bridging the gap between technology and business.
With over two decades of technical experience, Alex began his career in electronics and computer science, hacking various devices, especially his favourite, long-range radio transmitters. He gradually expanded his expertise to include enterprise cloud solutions like Salesforce, Oracle, and AWS. His approach to cybersecurity emphasises business value, prioritising market growth, customer satisfaction, and ROI.

As a founder of several startups, Alex has led diverse technical teams across development, CRM, IT operations, and CyberOps. His security strategies are customized to address the unique challenges of various industries, driving value through innovative solutions, deep technical expertise, and culture-driven security best practices.
Alex holds multiple technical degrees and over 35 certifications, with a significant number accredited to his role as a Salesforce Architect.

He currently leads Advension, a company based in Copenhagen, Denmark, dedicated to providing deep technical expertise in multiple Salesforce Clouds and development solutions.

Key Collaborators

We extend our heartfelt thanks to our key collaborators, whose invaluable feedback and advice have been pivotal in shaping this report. We're also deeply grateful to everyone who contributed to this project, in any capacity, making it the success it is!

Vipendra Singh

Digital Engineering Manager - D&RT @Pandora

With extensive experience in omni-channel retail, data integration, and business & IT architecture, Vipendra is a passionate advocate for composable enterprise.
He excels in building connected experiences and realizing digital strategies with measurable impact.

LinkedIn | Newsletter

Ahmed Hussein

Cybersecurity Consultant | MSc Cyber Security @SecureDevice

Ahmed is a seasoned cybersecurity consultant specialising in cyber threat intelligence and enterprise cyber-security, with a strong passion for web development and AI. With a solid foundation in computer science, Ahmed has dedicated his career to protecting organisations from digital threats.

LinkedIn

Simon Andersen

Business Analyst and Salesforce Architect @Advension

Simon is an experienced Business Analyst and Developer with deep expertise in CRM and MarTech, focusing on Sales, Marketing and the Financial Sector.
As a co-founder of Advension, he's leveraged his skills to drive growth and innovation.

LinkedIn



Any questions, comments, or cool ideas?
We'd love to hear from you! Reach out directly to the Advension Research team at research@advension.com.
Enjoyed the content? Share it with your network using the hashtag #Advension
If you find our content valuable and are interested in contributing to our next research project, please contact us at research@advension.com

Copyright © 2024 Advension™. All rights reserved.

Appendix

Knowledge Resources

Podcasts

- Security Management Highlight:
  - https://open.spotify.com/show/77qJqWtTaYazNBYhdCJbEA
- Human Firewall Podcast:
  - https://open.spotify.com/show/2e1FilaEZuuLtOJ9s747p2?si=d0b325ef9ff24514
- CIO Mind:
  - https://open.spotify.com/show/6YTaRb23mo84CEWwHnsvfv?si=33309336350a47d8
- CISO's Secrets:
  - https://open.spotify.com/show/6pS6AquulLxRdyUZx9jZgU?si=3f3d5ebcba344472
- CIONET:
  - https://open.spotify.com/show/6F9JzB3sQd5dvRyIQYtxKh?si=51c378b8bf5f4979
- CISO Talks:
  - https://open.spotify.com/show/49mF3CcCbFhCgb2xylKjnX?si=c95d7004d6464452
- CISO Insiders:
  - https://open.spotify.com/show/2lWuYF58XNSsMM6vRMmzPw?si=df054a6ea9894317
- CISO Tradecraft:
  - https://open.spotify.com/show/0w9mqg1SY4ytTnehjeGnP1?si=cca559d925d54de2
- CISOnomics Podcast:
  - https://open.spotify.com/show/4yXdTkMpm4bPS56k1bQdUM?si=703e901a397c4610
- CISO Series Podcast:
  - https://open.spotify.com/show/2GNPgHa4J8TGf1bFkHxoiF?si=a122990a864a443e
- The New CISO:
  - https://open.spotify.com/show/5WJfpaJaKJp3UtQ4yJGaHT?si=c448d9ab57e94f9c
- The Virtual CISO Podcast
  - https://open.spotify.com/show/0vPFRmrlo3fahWBakzbSTp?si=d156804ab2684860
- CISO Insights:
  - https://open.spotify.com/show/3W4OnFQbBE55iFtFNTcPbv?si=e43dd3291da14e52
- The Virtual CISO Moment:
  - https://open.spotify.com/show/3A9PI9NlmBbSKAhHGivspV?si=cff5cad1db464365
- Security Now:
  - https://twit.tv/subscribe

Cybersecurity News and Communities

- OWASP:
  - https://owasp.org/membership/
- We Live Security:
  - https://www.welivesecurity.com/en/
- The Hacker News:
  - https://thehackernews.com/
- CISOExecNet:
  - https://cisoexecnet.com/
- Wilders Security Forums:
  - https://www.wilderssecurity.com/
- Security Week:
  - https://www.securityweek.com/
- Cyber Security:
  - https://www.linkedin.com/groups/3821801/
- Information Security - Security Stack Exchange:
  - https://security.stackexchange.com/
- CyberWire:
  - https://thecyberwire.com/pro
- r/cybersecurity:
  - https://www.reddit.com/r/cybersecurity/
- ISC2:
  - https://www.isc2.org/professional-development
- MalwareBytes:
  - https://forums.malwarebytes.com/
- Aphinia:
  - https://aphinia.com/

Copyright © 2024 Advension™. All rights reserved.

References

- Salesforce Security Documentation:
  - https://developer.salesforce.com/developer-centers/security
- Salesforce Security Guide:
  - https://developer.salesforce.com/docs/atlas.en-us.securityImplGuide.meta/securityImplGuide/salesforce_security_guide.htm
- Salesforce Security Best Practices:
  - https://security.salesforce.com/security-best-practices
- Salesforce Well-architected - Secure:
  - https://architect.salesforce.com/well-architected/trusted/secure
- Salesforce Secure Coding Guidelines:
  - https://developer.salesforce.com/docs/atlas.en-us.secure_coding_guide.meta/secure_coding_guide/secure_coding_guidelines.htm
- Salesforce Security Review Overview:
  - https://partners.salesforce.com/pdx/s/learn/article/isv-security-review-overview-MC4QVWO6S2FVFD5MNRMLIEF3UBGQ?language=en_US
- Building an Information Technology Security Awareness and Training Program:
  - https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf
- Embedding a Strong Security Culture:
  - https://www.sans.org/mlp/ssa-2024-security-awareness-report/
- Shared Responsibility for Cloud Security: What You Need to Know:
  - https://www.cisecurity.org/insights/blog/shared-responsibility-cloud-security-what-you-need-to-know
- Shared Responsibility Model:
  - https://aws.amazon.com/compliance/shared-responsibility-model/
- Center for Internet Security (CIS) - Critical Security Controls
  - https://www.cisecurity.org/controls
- MITRE ATT&CK:
  - https://attack.mitre.org/
- Cloud Security Alliance:
  - https://cloudsecurityalliance.org/
- What is Application Security:
  - https://www.vmware.com/topics/application-security
- OWASP Top 10:
  - https://owasp.org/Top10/
- OWASP Developer Guide:
  - https://owasp.org/www-project-developer-guide/release/
- OWASP Secure Coding Practices:
  - https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/
- OWASP Cross-site Request Forgery (CSRF):
  - https://owasp.org/www-community/attacks/csrf
- 4 Must-Have Technologies That Made the Gartner Hype Cycle for Cloud Security:
  - https://www.gartner.com/smarterwithgartner/4-must-have-technologies-that-made-the-gartner-hype-cycle-for-cloud-security-2021
- HTML5 Security Cheatsheet:
  - https://html5sec.org/
- CWE - Top 25 Most Dangerous Software Weaknesses:
  - https://cwe.mitre.org/top25/
  - https://cwe.mitre.org/top25/archive/2023/2023_top25_list.html
- IBM Security - Be confident in your security with threat intelligence:
  - https://www.ibm.com/reports/threat-intelligence
- IBM Framework for Securing Generative AI:
  - https://www.ibm.com/blog/announcement/ibm-framework-for-securing-generative-ai/
- IBM X-Force Exchange:
  - https://exchange.xforce.ibmcloud.com/
- AoSafe - Human Risk Review 2024:
  - https://sosafe-awareness.com/resources/reports/human-risk-review
- CSA:
  - https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2024

Copyright © 2024 Advension™. All rights reserved.

Find more about us!

Amager Strandvej 60,
Copenhagen DK-2300

+45 27 51 22 92
+45 22 40 62 12

contact@advension.com
www.advension.com

LinkedIn | Twitter
#AdvensionSalesforceSecurity #Advension

About Advension

Advension is a leading Salesforce Consultant and ISV Partner based in Copenhagen, Denmark, with a primary focus on the Nordic region.

With over 50 certifications across different Salesforce Clouds and other platforms, Advension is committed to delivering high-quality, secure solutions across various Salesforce platforms, including Salesforce Sales/Service Cloud, Industry, Account Engagement and CPQ. Advension's expertise spans multiple industries, including IT, Finance, Insurance, and Healthcare.

The information contained in this white paper is provided for general informational purposes only. While every effort has been made to ensure the accuracy and completeness of the content, the authors and publishers assume no responsibility for any errors, omissions, or inaccuracies in the information provided. The content is not intended to serve as legal, financial, or professional advice and should not be relied upon as such. Readers are encouraged to consult with appropriate professionals for advice specific to their individual circumstances. The views and opinions expressed in this white paper are those of the authors and do not necessarily reflect the official policy or position of any organisation or company mentioned. The use of any information provided in this white paper is at the reader's own risk. The authors and publishers disclaim any liability for any direct, indirect, incidental, consequential, or other damages arising out of or in connection with the use of the information presented herein.

Copyright © 2024 Advension™. All rights reserved.