THALES

Quality, Security and Trust
SOARIZON by Thales

Version 1.0

16th September 2020

THALES

Contents

1 SOARIZON INTRODUCTION

Thales operates an in-house digital incubator, designed to refine start-up ideas from within our organisation and accelerate them to become real-world digital products. Each project is nurtured with highly skilled engineers and processes to allow a quick transition from idea to the releasable digital product. Each project includes architecture and design in the infrastructure and a defined process to ensure security.

We continuously consider our users, reviewing and updating existing processes, architecture and design to ensure continuous improvement and evolution.

2 SECURITY AND RISK GOVERNANCE

We understand the importance of maintaining and building trust with our Customers and Partners, and we are committed to keeping customer information safe from unauthorised access or processing. We implement a defence-in-depth approach to security, which is a fundamental necessity for our business, and a core value of how we behave as an organisation.

Thales has a dedicated team of security specialists, responsible for ensuring risk assessments are conducted and regularly reviewed.

3 RISK MANAGEMENT

Thales's security team have a wealth of experience across multiple methodologies for risk management which includes ISO 27001, NIST, HMG UK Information Security 1 and 2, and Industrial Control Systems (ICS) framework. SOARIZON operates a risk management framework aligned with the Cloud Security Alliance (CSA), Cloud Control Methodology (CCM).

4 SECURITY CONTROLS

4.1 THALES PRODUCT INFRASTRUCTURE

4.1.1 DATA CENTRE SECURITY

SOARIZON is hosted on Microsoft Azure; providing high levels of physical and network security with a high level of availability and resilience and resides in Western Europe. Microsoft Azure maintains an audited security program, which includes SOC 2 and ISO 27001 compliance.

Microsoft Azure leverages the most advanced facilities infrastructure such as power, networking, and security with (N+1) redundancy architectures as a minimum. SOARIZON's uptime is 99% minimum.

The physical, environmental, and infrastructure security protections, including continuity and recovery plans amongst others, are independently validated and include but are not limited to ISO27001 and PCI-DSS certification and SOC 1, 2, 3 reports.

4.1.2 NETWORK SECURITY & PERIMETER PROTECTION

The SOARIZON infrastructure is designed with security protections in mind. Network security protections are designed to prevent unauthorised network access to and within the product infrastructure. These security controls include but are not limited to containerisation technology, enterprise-grade routing and network access control lists (firewalling).

4.1.3 CONFIGURATION MANAGEMENT

Patches are applied regularly for all released vendor patches applicable to the service. For emergencies, example, out-of-band zero-day related vulnerabilities, we follow the formal change process.

4.1.4 ALERTING & MONITORING

Logs and events are monitored in real-time with integration into a Security Information Event Monitoring (SIEM) solution managed and controlled by a Security Operations Centre (SOC) team. Events are triaged, investigated, categorised, organised and escalated dependent on severity following a defined playbook process with developers, security experts and support operations teams taking appropriate action.

4.1.5 INFRASTRUCTURE ACCESS

Server-level authentication uses public-key cryptography (PKI) and token-based two-factor authentication (2FA), ensures strict access controls and active security monitoring for events.

4.2 APPLICATION PROTECTION

4.2.1 WEB APPLICATION DEFENCES

Thales has implemented a Web Application Firewall (WAF) for the SOARIZON application that actively monitors real-time traffic at the application layer. Custom blocking rules are identified, assessed and implemented as part of the ongoing fine-tuning activities. Microsoft Azure provides Distributed Denial of Service (DDoS) protection.

4.2.2 DEVELOPMENT & RELEASE MANAGEMENT

The SOARIZON development team are UK-based, employees of Thales UK Ltd, with a wide range of technical skillsets; these skills include User Interface Design (UI) to cybersecurity specialist allowing rapid design, scoping and implementation.

SOARZION development utilises SCRUM agile methodologies and principals for optimal turnaround times from user stories to implementation and value creation. Development occurs in multiple environments where key activities are conducted as part of the release pipeline. Each release must pass through a range of security, performance and quality gates giving SOARZION confidence each release has met strict criteria. SOARIZON releases to production multiple times per week, ensuring the product is continuously improving and generating value to customers.

SOARIZON utilises a Continuous Integration and Continuous Deployment strategy to ensure coding standards and quality.

New code is proposed, approved, merged and deployed. Code reviews and quality assurance performed by specialised teams with excellent knowledge of the project, supplemented by additional key resources as required. For SOARIZON, security experts are part of the overall process to ensure secure by design principles, new security requirements are captured, implemented and remain effective.

Tests in development and/or test environments include analysis of source code quality, unit and integration, quality, build, static security and dependency check, functional checks, dynamic application security testing, and vulnerability scans with remediation activities undertaken to mitigate vulnerabilities following a risk-based approach.

4.2.3 VULNERABILITY SCANNING, PENETRATION TESTING, & BUG BOUNTIES

SOARIZON has vulnerability scans periodically performed on the infrastructure and application in addition to security auditing tools built into the deployment pipeline. Penetration tests are conducted at least every cycle. The scope of penetration tests evolves as the service changes and new functionality added in order to ensure the service remains as secure as possible.

The adopted formal process ensures remediation activities completed in a timely manner consummate to the severity identified prior to release to production. Thales hires security specialists to ensure that all projects are designed and implemented in a secure by design way.

4.3 CUSTOMER DATA PROTECTION

SOARIZON complies with all applicable data protection and privacy legislation, including the General Data Protection Regulations (GDPR), UK Data Protection Act and California Consumer Privacy Act. SOARIZON is hosted and operated from Western Europe. We only use customer data to provide and improve our services and to keep our services safe and secure. We never sell customer data to third-parties. Our use of customer data is strictly managed in accordance with our internal data management processes and Privacy Notice[1], supported by our Data Protection Impact Assessment (DPIA)[2]. The majority of customer data is processed within Europe and the United Kingdom, where data is processed outside of Europe or the United Kingdom, appropriate measures are implemented to ensure compliance with European data protection and privacy standards (such as the Privacy Shield framework and standard data processing agreements)[3]. All of our third-party data processors undergo security vetting and vulnerability scanning prior to their integration into any of our services. For further information on how SOARIZON uses and protects customer data, please refer to our Privacy Notice.

4.3.2 CREDIT CARD INFORMATION PROTECTION

SOARIZON uses an industry standard PCI-compliant global payment services provider to process online card transactions and ensure that customer payment information is always processed and stored securely.

[1] Publicly available at www.soarizon.io/privacy-notice.
[2] Soarizon has completed a UK ICO standard Data Protection Impact Assessment which can be provided to business customers on request.
[3] For details on the information we process outside of the UK and EU, please see Section 7 and the Appendix of our Privacy Notice.

4.3.3 ENCRYPTION IN-TRANSIT & AT-REST

All connections to the SOARIZON service use a certificate, which enforces secure protocols (TLS 1.2 or higher) to ensure data is encrypted end-to-end, regular tests are conducted to ensure compliance. Data at rest is encrypted including backups that are FIPS140-2 compliant.

4.3.4 USER AUTHENTICATION & AUTHORISATION

SOARIZON utilises Microsoft Identity and Access Management (IAM) for registration and logon. This provides the option to register/logon using an existing account from a social provider (Microsoft, Google and LinkedIn) in addition to creating a new account. SOARIZON does not store any passwords and uses Oauth2 for the authentication framework.

4.4 INCIDENT MANAGEMENT

The SOC provides a 24 x 7 x 365 coverage to monitor and are able to respond quickly to security and privacy events. Pre-defined incident types 'playbooks' are created taking into consideration current and historical trends to facilitate timely incident tracking, escalation, and communication. Automated processes such as non-compliance alerts, malicious activity and anomalous events are in place, and continually updated based on latest trends.

If you would like to know more,

please contact us.

SOARIZON®