



Zensar's Service Definition Document for Zensar AI-Led VAPT

January 2026

Disclaimer & Confidentiality

The information in this document shall not be disclosed outside the Crown Commercial Service and shall not be duplicated, used or disclosed, in whole or in part, for any purpose other than to evaluate the document. This restriction does not limit the right of the Crown Commercial Service to use information contained in this document if it is obtained from another source without restriction. This proposal is valid up to 90 days from the date of submission of the proposal.

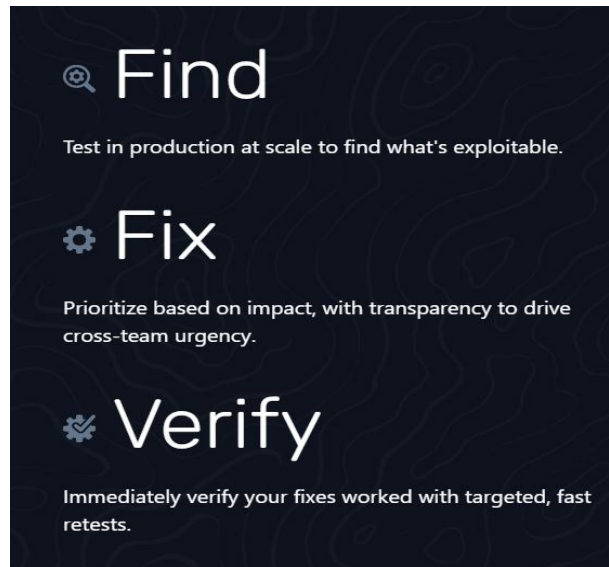
Table of Contents

1	Introduction.....	1
2	Service Overview (What is ZenVAPT?).....	1
3	Reference Architecture & Components	2
4	Operating Model & Service Flow	3
5	Service Tasks & Deliverables.....	4
6	Open Weaknesses Over Time.....	5
7	NodeZero Insights	5
8	Reporting, Integrations & Automation.....	7

1 Introduction

This document defines Zensar's **AI-Led Vulnerability Assessment & Penetration Testing (VAPT)** service powered by **Horizon3.ai NodeZero**, covering approach, architecture, delivery model, tasks, scope boundaries, assumptions and customer obligations.

Why AI-led VAPT now. Traditional VA/PT often over-indexes on scan results and CVSS scores, making remediation noisy and slow. NodeZero performs **production-safe, autonomous Pen Tests** that **prove exploitability**, chain weaknesses into **attack paths** and provide **proof-of-exploit** with **1-Click Verify** to confirm fixes, accelerating true risk reduction.



2 Service Overview (What is ZenVAPT?)

ZenVAPT is a **managed, attacker-validated VAPT** program running across **on-prem, cloud, perimeter and identity**. It is agentless, self-service/on-demand and integrates **Cloud Pen testing (AWS/Azure)**, **Internal/External tests**, **Azure Entra ID**, **AD Password Audit**, **Phishing impact**, **Segmentation/Insider tests** and **Rapid Response** for KEVs.

Core outcomes.

- **Prove what's exploitable** (not just "potential vulnerabilities") with **path, proof and impact** for every finding.
- **Prioritise the right fixes** using systemic guidance (one change can remove many paths).
- **Verify remediations quickly** with **1-Click Verify** and trend your MTTR and exposure using **NodeZero Insights™**.
- **Compliance support** (e.g., **PCI DSS v4.0 11.4** pen testing with evidence and retest)

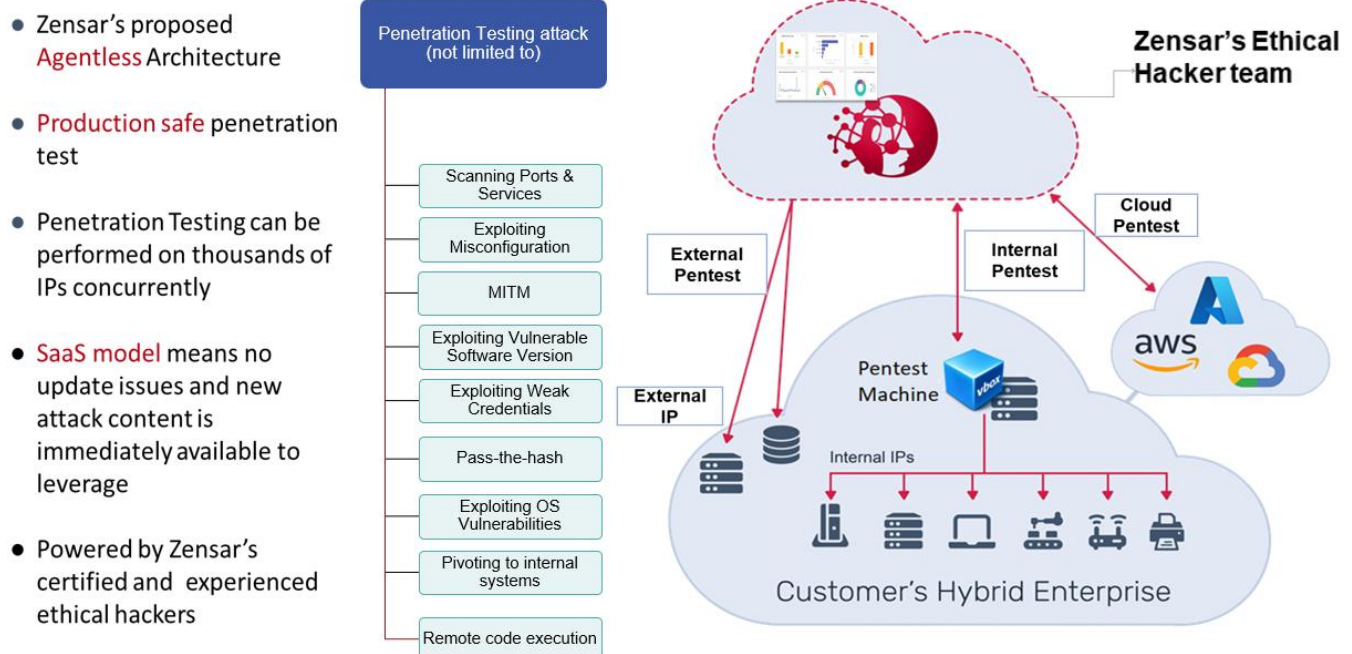
3 Reference Architecture & Components

Components.

- **NodeZero Portal (SaaS):** Orchestrates tests, provides real-time view, attack paths, proof and APIs.
- **NodeZero Host (Internal tests):** Lightweight Ubuntu/Docker host placed in customer network; **min 2 vCPU/4GB/20GB; recommended 4/8/40.**
- **Network/Egress:** Allowlisted outbound to Horizon3 endpoints (per US/EU region); **NodeZero Gateway** option for restricted networks.
- **Test Types:** Internal, External (cloud-run), **Cloud Pen testing (AWS/Azure), Azure Entra ID, AD Password Audit, Segmentation/Insider/Phishing.**
- **Insights/Rapid Response/Tripwires:** Org-wide trending (Insights), KEV alerting & targeted tests (Rapid Response), decoy traps aligned to exposures (Tripwires).

Cloud coverage. NodeZero Cloud Pen testing provides deeper identity-centric attack content for AWS/Azure and can pivot to on-prem to emulate real attacker operations end-to-end.

Zensar's Proposed Autonomous AI-Led VAPT



Infrastructure Attack Surface

NodeZero Infrastructure Attack Surface tests are it's autonomous network penetration tests. These all-inclusive tests are deployable from various perspectives and identify attack paths across on-premise, hybrid-cloud, perimeter, and cloud networks.

Internal Pentest

A pentest run against an internal network. NodeZero is deployed on a Docker host within your private network.

External Attacks

NodeZero runs from the Horizon3.ai cloud and tests your public-facing or external assets.

Kubernetes Pentest

Deploy NodeZero directly into a Kubernetes cluster, either on-prem or in the cloud, to pentest its security controls and vulnerabilities.

Identity Attack Surface

NodeZero's Identity Attack Surface tests find and exploit real-world attack-paths and vulnerabilities in IAM controls and platforms.

AWS Pentest

NodeZero uses a privileged role in your AWS account to discover vulnerabilities and misconfigurations.

Azure Entra ID Pentest

NodeZero runs on a docker host within your private network to discover and assess attack paths within your hybrid Entra ID environment.

Active Directory Password Audit

Audit your users' Active Directory Passwords. NodeZero will reveal weak, breached, and re-used passwords.

Operational Scenario Testing

NodeZero's Operational Scenario tests are used to validate your organization's security readiness by using real-world attack techniques to tests its resilience to operational scenarios.

Segmentation Testing

Discover your internal attack surface. NodeZero enumerates IPS, ports, services and applications within your network.

Phishing Pentest

Use NodeZero to measure the impact of phishing campaigns by injecting the phished credentials into an internal pentest

Insider Threat Testing

Use NodeZero to validate your organization's security posture against insider threats.

4 Operating Model & Service Flow

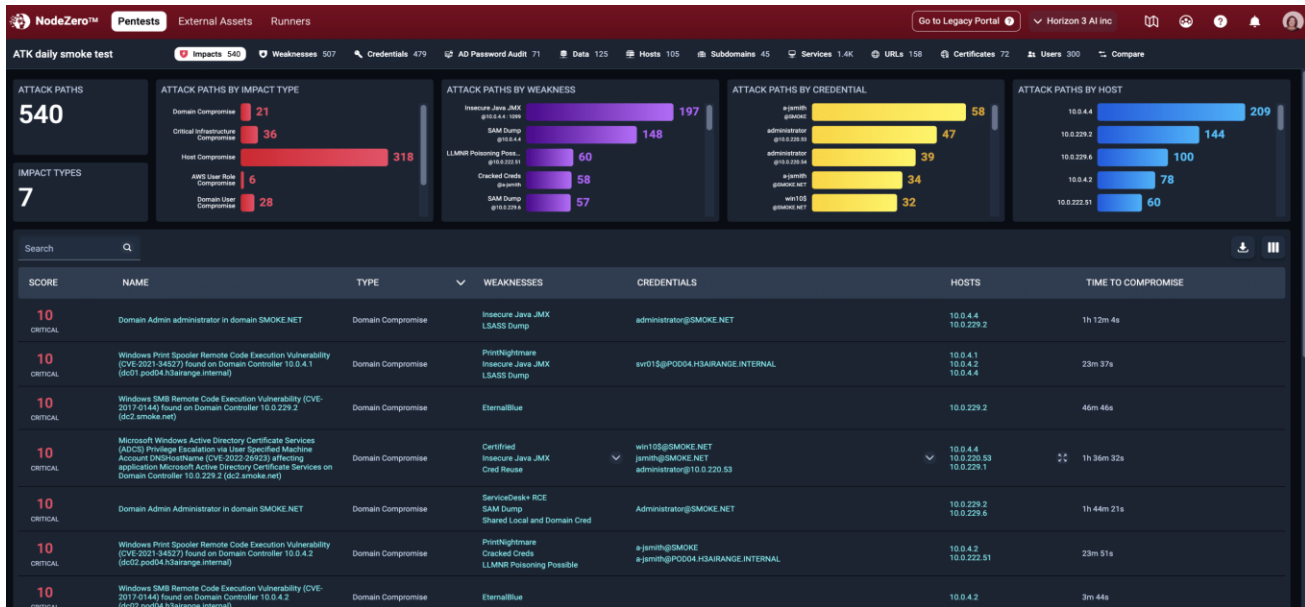
Define. Scope/authorisation, guardrails (assets, time windows), safe-run controls, external IP allow-listing for external pen tests and pen test templates/schedules.

Discover & Attack (Autonomous). NodeZero enumerates and **chains** misconfigurations, credentials, CVEs and insecure defaults; safely exploits to produce **proof** and **impact—production-safe** and proven at scale.

Prioritise & Plan Fix. Zensar runs **Fix Action Workshops** to identify **systemic fixes** and quick wins; we push tickets into **ServiceNow/Jira** with webhook sync for status.

Verify. Use **1-Click Verify** (targeted retests) or scheduled incremental pen tests to confirm remediation; publish auditor-ready evidence.

Measure. **NodeZero Insights** tracks open weaknesses, assets at risk, attack paths, MTTR, systemic issues—ideal for leadership reporting.



5 Service Tasks & Deliverables

- Scoping & Authorisation (letters, allowlists, templates, test windows).
- Host Setup & Validation (Ubuntu/Docker; network egress tests).
- Pentest Orchestration & Oversight (safe execution; exception handling).
- Analysis & Prioritisation (attack paths, proof, impact; systemic fix map).
- Remediation Governance (tickets to **Jira/SNOW**, webhook status sync).
- Retesting & Evidence (**1-Click Verify** / scheduled retests for closure).
- Executive Reporting (**Insights** trends, MTTR, KEV focus area).

Deliverables.

- **Pentest Report** (exec summary, attack paths, proof, business impact).
- **Fix Action Report** (prioritised systemic remediation actions; one-to-many fixes mapping).
- **Ticket Packs** (SNOW/Jira) + **Retest Evidence (1-Click Verify)**.
- **Insights Trend Pack** (Open Weaknesses over Time, Assets at Risk, severity/type trends, MTTR).

1-Click Verify Pentest

1-Click Verify uses the settings from the original pentest, focusing on specific weaknesses on specific hosts. 1-Click Verify may find new weaknesses.

Pentest Name *

Runner - Optional
Select...

NEW Setup a NodeZero Runner to automatically deploy NodeZero on your Docker host. [Learn More](#)

Weaknesses

Scope

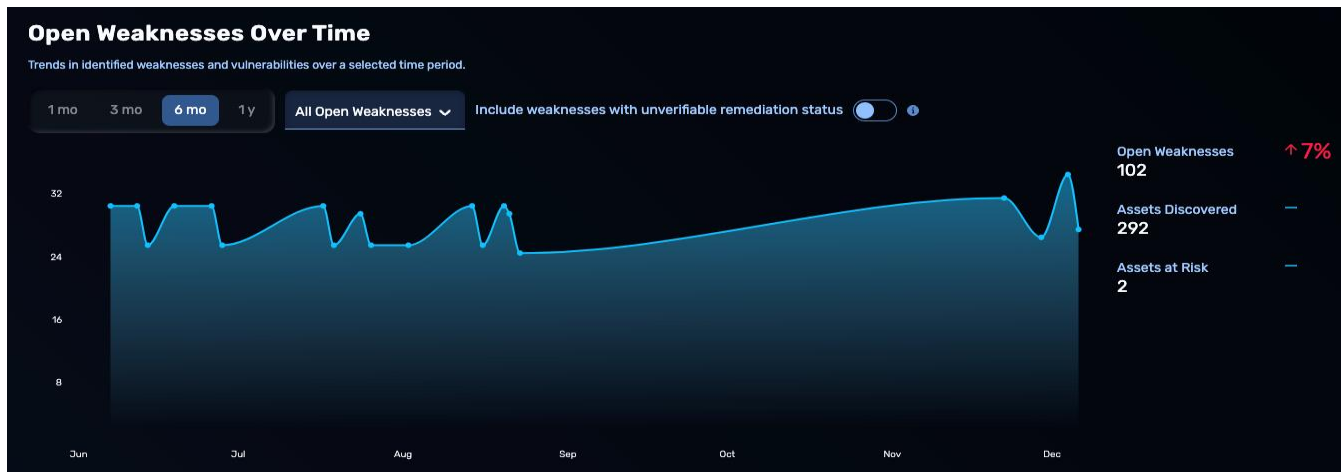
[View Configuration](#)

☐ I have reviewed all configuration settings and accept the risk. *

[Close](#) [Run Pentest](#)

6 Open Weaknesses Over Time

This section shows the un-mitigated weaknesses across the entire organisation as reported from NodeZero pentests. Each data point on the graph shows the total number of open weaknesses reported from all the pen test operations that were completed on that day. Users can visualise the data over 1 month, 3 month, 6 months and 1-year periods. The list at the right of the graph summarises counts of Open Weaknesses, Assets Discovered and Assets at Risk as of today as well as the percentage change over the time period selected.



7 NodeZero Insights

What it is. An add-on that aggregates **trend data** from all pen tests, helping leaders **prioritise, prove impact** and produce **strategic executive reports**.

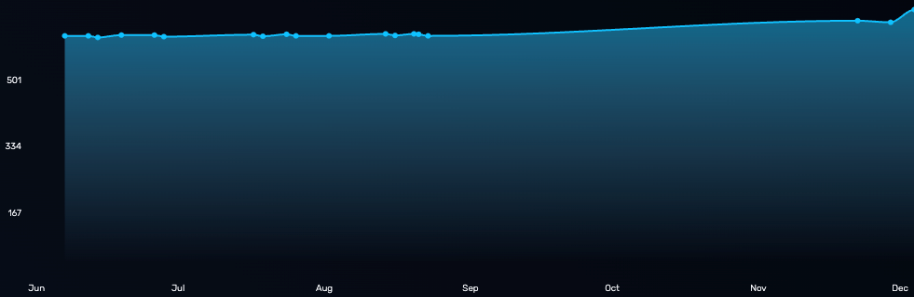
Key capabilities.

- **Visualise Attack Surface Evolution:** Identify systemic blind spots; validate control effectiveness.
- **Monitor Progress (MTTR):** Track remediation velocity by severity; quantify improvements.
- **Analyse Weakness Trends:** By severity and type to focus on maximum-impact fixes.
- **Proactively Identify Risks:** Outdated controls, misconfigurations, policy gaps.
- **Unverifiable Weaknesses control:** Toggle to include/exclude unverifiable categories for reporting completeness.
- **Attack Paths Over Time and Pentest Series Analysis:** Track paths, schedule cadence and upcoming runs.
- **CISA KEV filter:** Focus MTTR and open counts on KEVs to show fast risk reduction on known-exploited items.
- **Systemic Issues panel:** Two 3-month periods (last 6 months) to show whether policy/initiative changes are closing enterprise-wide gaps.

Attack Paths Over Time

Trends in identified attack paths discovered by NodeZero over a selected time period.

1 mo 3 mo **6 mo** 1 y



Open Attack Paths	664	↑10%
Host Compromise	341	↑5%
Domain User Compromise	94	↑27%
Domain Compromise	85	↑20%
Sensitive Data Exposure	81	↑12%

Pentest Series Analysis

Trends in identified attack paths across all scheduled pentest series.

1 mo 3 mo **6 mo** 1 y



Upcoming Pentests...

Tiny scope on the range
Internal Pentest

Scheduled for Dec 11, 2024

password audit on dev-runner
Active Directory PW Audit

Scheduled for Dec 13, 2024

Remediation Summary

Visualizing open weaknesses by severity, age, and mean-time-to-remediation.

Include weaknesses with unverifiable remediation status ☐ Show Only CISA KEV ☐

Mean Time to Remediation | CISA KEV

1 mo 3 mo **6 mo** 1 y



Toggle to View: ☒ Critical ☐ High ☐ Medium ☐ Low ☐ Info

Open Weaknesses by Severity | CISA KEV

CRITICAL	3 OPEN
HIGH	1 OPEN
MEDIUM	0 OPEN
LOW	0 OPEN

Open Weaknesses by Age | CISA KEV

1D	0 OPEN
30D	0 OPEN
6M	2 OPEN
1Y	2 OPEN
1Y+	0 OPEN

All Severities ☐

8 Reporting, Integrations & Automation

- Reporting. **Real-time view + Pentest Report + Fix Action Report + Insights executive summaries.**
- Ticketing integrations. ServiceNow VR and Jira: **create/update remediation tasks, enable webhooks for status sync so closures are reflected back in NodeZero/Insights.**
- API for automation. **Public GraphQL API enables CI/CD hooks, programmatic scheduling/exports and custom analytics.**

Configure NodeZero API



ServiceNow

Attach your ServiceNow API to allow NodeZero to automatically create and manage remediation tickets in the Vulnerability Response module. Tickets will be created in the `sn\_vul\_vulnerable\_item` table.

ServiceNow Domain URL *

ServiceNow API Token *

Email *
user@company.com

Only org admins can create and manage remediation tickets ☒

Cancel

Save and Test

Configure NodeZero API



Jira

Attach your Jira API to allow NodeZero to automatically create and manage remediation tickets.

Jira Domain URL *

Jira Project Key *

Work Type *
Task

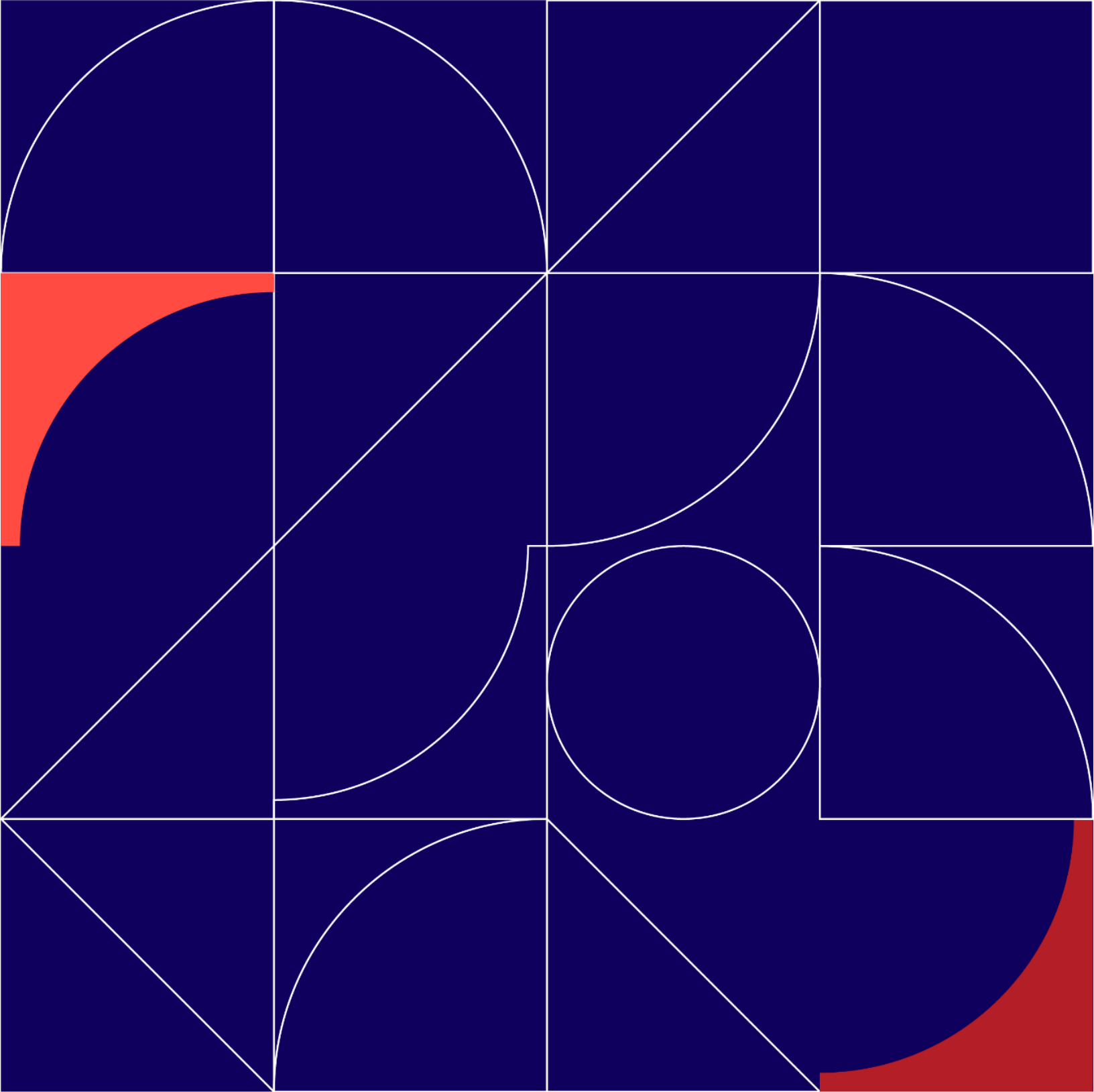
Jira API Token *

Email *
user@company.com

Only org admins can create and manage remediation tickets ☐

Cancel

Save and Test



We conceptualise, build and manage digital products through experience design, data engineering and advanced analytics for over 130 leading companies. Our solutions leverage industry-leading platforms to help our clients be competitive, agile and disruptive while moving with velocity through change and opportunity.

With headquarters in Pune, India, our 10,000+ associates work across 33 locations, including San Jose, Seattle, Princeton, Cape Town, London, Singapore and Mexico City.

For more information please contact: marketing@zensar.com | www.zensar.com

An  Company