Infraestrutura Hi Platform

A Hi Platform utiliza uma infraestrutura em nuvem para rodar sua aplicação.

O acesso é feito através da Internet através dos navegadores dos computadores, tablets e celulares.

Antes de alcançar os servidores da Hi Platform (aplicação e banco de dados), as requisições passam por um sistema de segurança, isto é, um WAF (Web application firewall).

Ambiente é formado por:

- Servidores: Windows server e Linux server
- Linguagem: PHP, .net, C#, HTML, Javascript, CSS.

Toda comunicação entre o usuário e a plataforma da Hi Platform se dá através de um túnel criptografado via TLS/SSL, garantindo seguranças com detalhamento da infraestrutura, rotinas de backups e perfis de acesso pode ser acessado pelo link

Autenticação

Os acessos às soluções da Hi Platform são realizados apenas por usuários devidamente registrados e autenticados

Todos os usuários precisam ser cadastrados primeiramente na solução e liberado o seu acesso, através do perfil de administrador. Apenas os usuários com perfil de administrador poderão editar, remover ou criar um novo usuário com acesso a solução.

A autenticação através de 2 fatores existe na solução HiFlow e é obrigatória para todos os usuários.

Além disso, a Hi Platform possui sistema de autenticação único (SSO).

Datacenter

Utilizamos servidores da AWS e OCI para hospedagem dos serviços da Hi Platform. A solução HiFlow está hospedada na OCI e as demais na AWS.

Infraestrutura localizada nos Estados Unidos, Virgina (AWS) e Brasil, São Paulo (OCI).

O acesso físico a ambos os datacenters é registrado e monitorado. Centros de monitoramento 24/7, sistema de monitoramento via circuito fechado de televisão (CFTV). Existem mecanismos para controlar o clima e manter uma temperatura operacional apropriada, equipamentos de detecção e supressão de incêndio e detecção de vazamento de água.

Para mais detalhes sobre a infraestrutura provida pela OCI e pela AWS.

Backups

Realizamos 8 backups completos diariamente que são enviados para servidores remotos para garantir a distribuição e segurança dos dados.

Mantemos rotinas de análise e conferência dos backups de forma semanal.

Disaster Recovery

A disponibilidade da infraestrutura da Hi Platform e nossos parâmetros de atendimento estão sempre atualizados e disponíveis neste link.

Navegadores

Os navegadores compatíveis com a Hi Platform são:

- Chrome, última versão;
- Firefox, última versão;
- Microsoft Edge, última versão;
- Safari, última versão;

Pentest e Análises automatizadas

Processo de Pentest Externo

Atualmente, realizado duas vezes por ano, realizamos a contratação de serviço especializado externo para a elaboração de testes de intrusão em nosso ambiente, onde uma vez identificadas as falhas, é realizada uma validação dos achados por parte do prestador de serviços, e em seguida os problemas encontrados são direcionados às respectivas equipes responsáveis por cada segmento do ambiente (desenvolvimento, infraestrutura, etc). As vulnerabilidades e problemas então são corrigidos pelos squads e um relatório da correção realizada é enviado de volta ao prestador para que o mesmo realize uma nova validação para garantir que o problema tenha sido solucionado.

Uma vez que o processo é finalizado e os problemas são endereçados ou riscos mitigados. É realizada uma validação interna, por meio do processo de replicação de testes para todos os achados durante o processo do Pentest. Realizando essa verificação, estruturamos uma documentação em cima do que nos foi passado no relatório final por parte do prestador de serviço, e caso algum dos pontos tenha ficado em aberto, aplicamos as devidas correções conforme a necessidade.

Sendo assim, durante o período do Pentest externo, e posteriormente, são realizadas um mínimo de 3 verificações, sendo inicialmente a descoberta do problema, em seguida uma validação de correção, e por fim, uma validação geral por meio da reprodução do processo de exploração para garantir a mitigação do problema.

Processos Internos

Atualmente, nossos processos de SI estão segmentados nas categorias em uso, e em desenvolvimento:

Em uso

- Análise de vulnerabilidades, bugs e outros problemas no código em HTML, CSS, JS e PHP com ferramentas SAST integradas à pipeline;

- Auditoria e análise de vulnerabilidades, problemas de configuração e hardening na infraestrutura realizada internamente;

- Auditoria e análise de vulnerabilidades, problemas de configuração e hardening na infraestrutura realizada externamente;

- Análise de vulnerabilidades, bugs e outros problemas no código com ferramenta DAST;

- Monitoramento de recursos, requisições e outros dados para análise contínua;

- Plano de conscientização corporativa em SI;

- Consultoria externa referente à Legislação e Compliance;

- Detecção de Hardcoded Credentials integrada à Pipeline;

Em Desenvolvimento

- Melhoria do processo de Threat Modelling;

- Implementação de análise de vulnerabilidades, bugs e outros problemas em dependências utilizadas;

- Melhoria do processo de análise DAST e integração à Pipeline;

- Implementação do ciclo contínuo de análise e integração das ferramentas;

- Implementação de mais ações de conscientização ao plano atualmente em uso;

- Melhoria do processo de monitoramento;

- Enforce de Cifras e Versão do SSL/TLS (atualmente apenas em Stage)