
Diminua o tempo de resposta
aos incidentes com uma plataforma que combina inteligência humana e orquestração
RIS

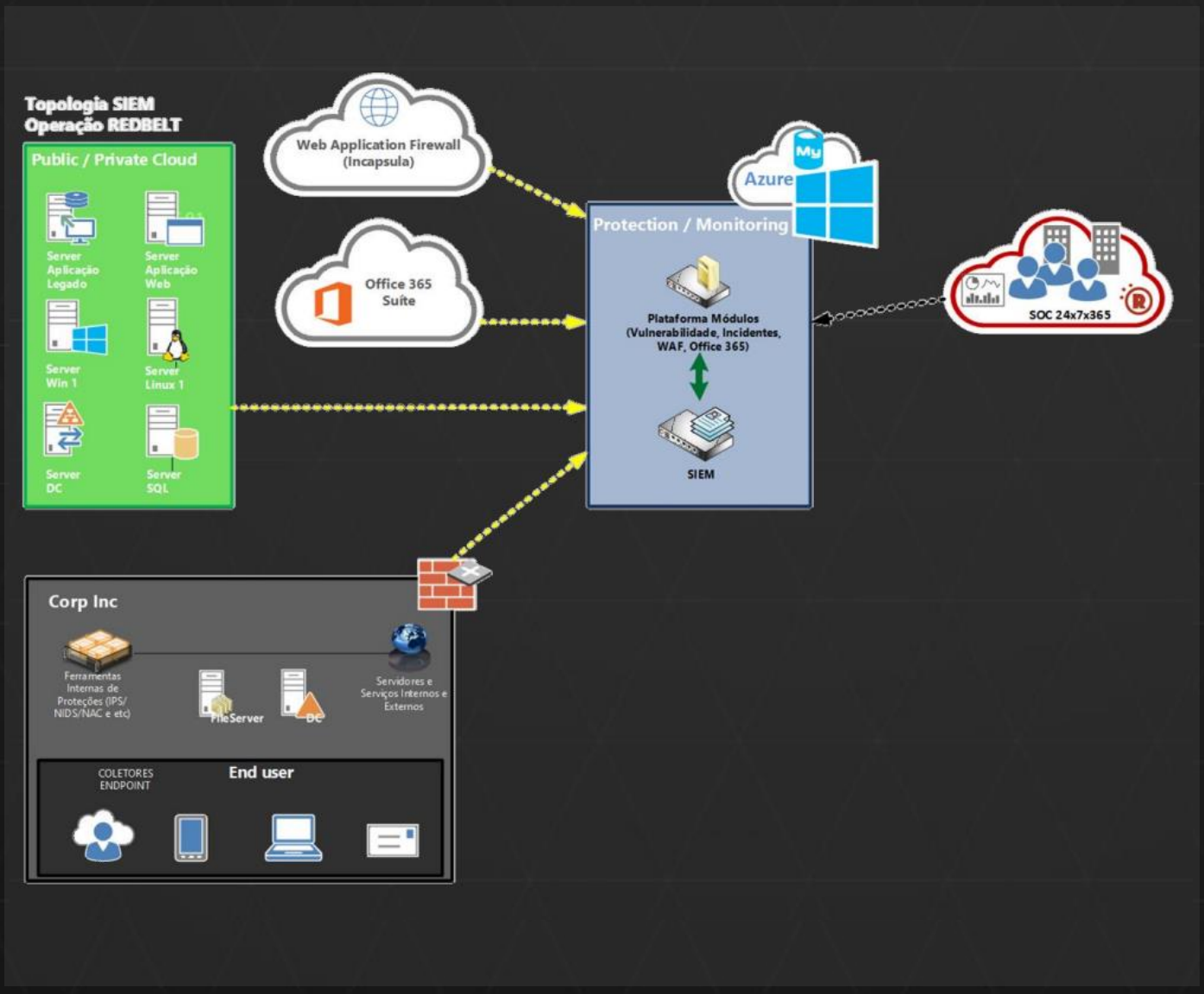
O que é o RIS?

O RIS (Risk Information Security) é uma plataforma SaaS que integra soluções de diferentes fabricantes e permite concentrar e correlacionar as informações de segurança necessárias para um plano de ação, viabilizando a gestão do ciclo de vida de **vulnerabilidades** e **incidentes** de segurança.

Para quem o RIS é interessante?

O RIS é importante para empresas que desejam **reduzir o tempo de resposta aos incidentes de segurança e o gerenciamento do ciclo de vida de vulnerabilidades** no seu ambiente.

Como a plataforma funciona?



A plataforma conta com quatro módulos de monitoramento:

- Gestão Vulnerabilidades
- Gestão de Incidentes
- WAF (Web Application Firewall)
- Office 365

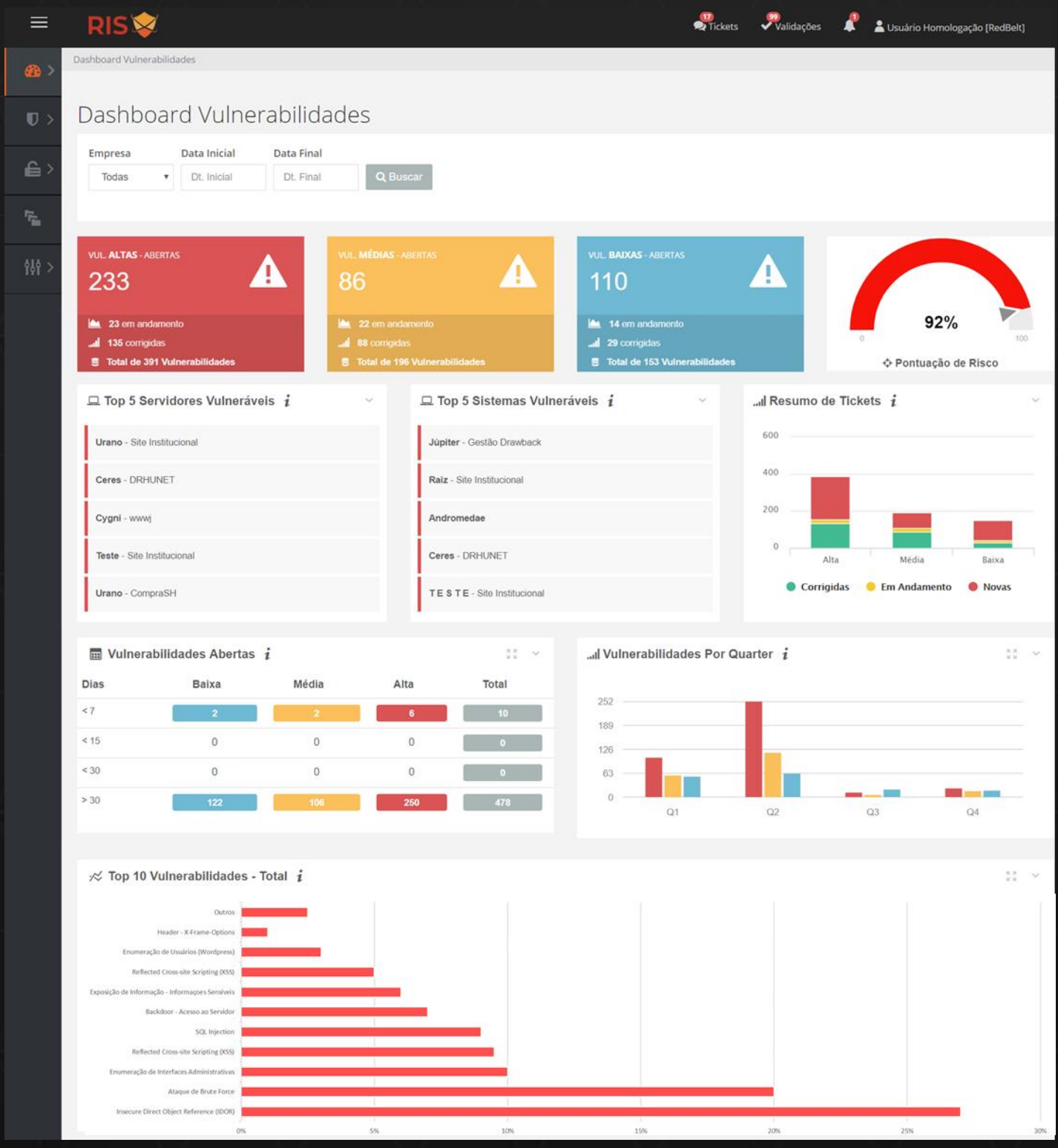
Módulo de Gestão de vulnerabilidades

Quem já viu um relatório de PENTEST entende a proposta de valor do módulo de vulnerabilidades. São páginas e mais páginas relatando erros em códigos e possíveis ataques que a empresa pode sofrer. É um relatório destinado para um leitor técnico e de difícil entendimento. A entrega de um PENTEST via RIS permite que o cliente tenha informações em formato gerencial, além de permitir o acompanhamento do status de cada vulnerabilidade e o registro de todo o esforço feito em torno da segurança do ambiente. O módulo conta com as seguintes funcionalidades:

Funcionalidades
Centralização de todas as vulnerabilidades de uma determinada aplicação, servidor ou ambiente.
Acesso em tempo real a todas as vulnerabilidades que foram identificadas no ambiente, podendo verificar o que está sendo corrigido, vulnerabilidades abertas e as que já foram corrigidas.
Classificação de cada vulnerabilidade seguindo a classificação CVSS, baseando-se também no impacto do ambiente em questão.
Criação de um clico de vida para vulnerabilidades, identificando quando as mesmas foram identificadas, ações tomadas para sua correção ou até mesmo aceite do risco.
Dashboard gerencial com métricas (KPI) de acompanhamento sobre as vulnerabilidades e riscos existentes do ambiente, com gráficos de sistemas e aplicações mais vulneráveis, top 10 de vulnerabilidades encontradas dividindo por período customizados de tempo.
Acesso e criação de relatórios técnicos baseado em vulnerabilidades identificadas por ambiente, sistema ou até mesmo por um único host.
Interação entre equipe do cliente e equipe da Redbelt, via tickets, para resolução de vulnerabilidades ou dúvidas referente as mesmas.
Evidências sobre cada vulnerabilidade, incluindo a sua descrição, prova conceito do impacto, formas de correção e links de referência além da possibilidade de interação com a equipe responsável por identificar a falha, evitando assim qualquer tipo de falso positivo.
Histórico de todas as vulnerabilidades identificadas no ambiente como base para a tomada de decisões na aquisição de novas soluções de segurança.

Módulo de Gestão de vulnerabilidades

O módulo de vulnerabilidades não é uma ferramenta automatizada de scan de vulnerabilidades. Ele é alimentado por PENTESTs realizados pelo time de especialistas da Redbelt e cada vulnerabilidade encontrada é devidamente explorada e evidenciada na ferramenta.



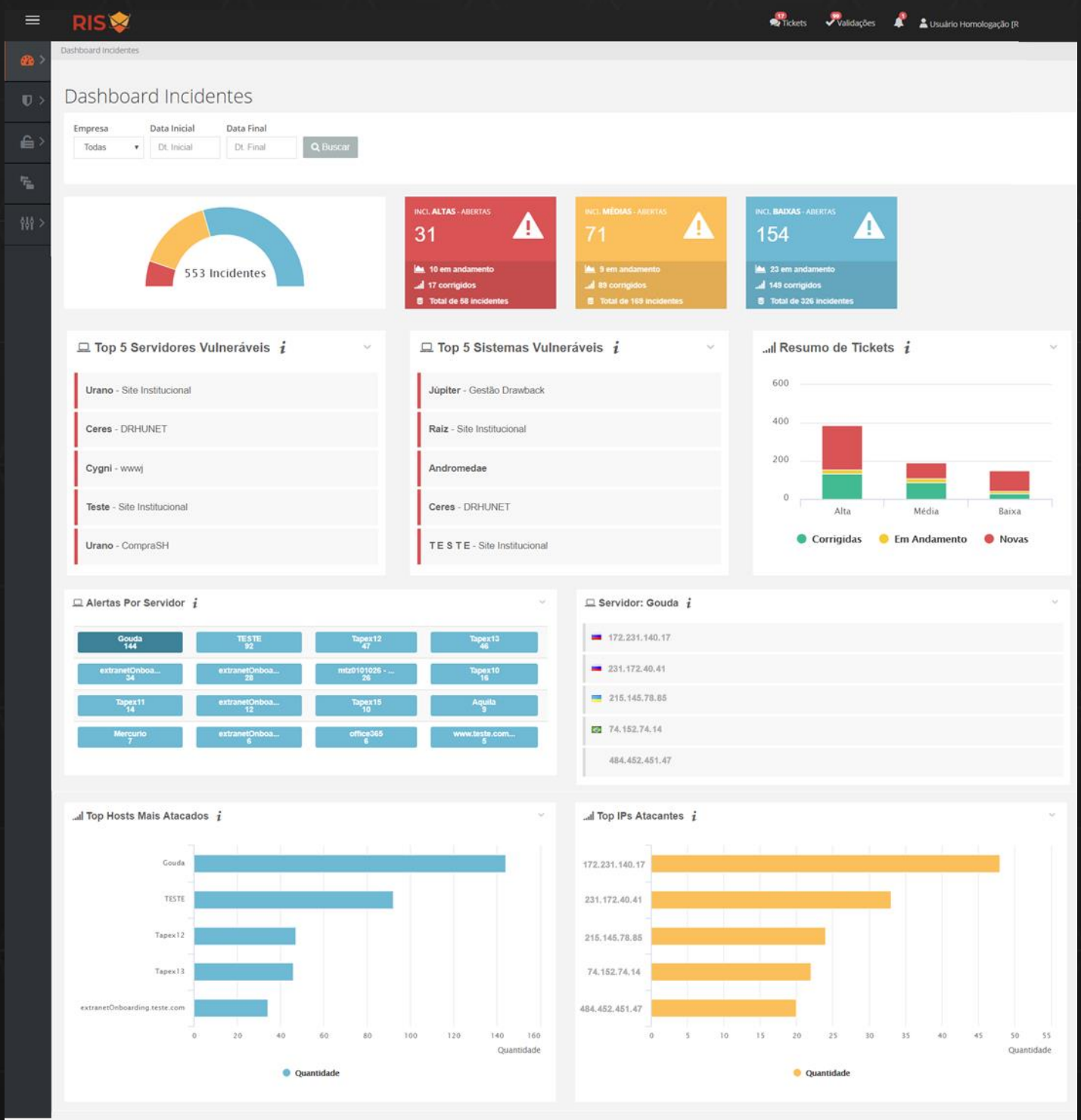
Módulo de Gestão de incidentes

O módulo de gestão de incidentes do RIS coleta de diferentes tecnologias todos os incidentes mapeados. Esses incidentes são analisados e qualificados pelo time de especialistas da Redbelt, eliminando falsos positivos (ruído), e permitindo que o time de resposta se concentre apenas nos incidentes que merecem atenção. Esse é o primeiro passo para a **redução do tempo de resposta aos incidentes.**

Funcionalidades
Centralização de todos os incidentes identificados em um determinado ambiente, capturados através de um SIEM (SaaS), endpoints security, web application firewall, next generation firewall e várias outras fontes de logs.
Validação de todos os incidentes por uma equipe de SOC evitando assim possíveis falsos positivos.
Criação de um clico de vida para cada incidente, incluindo sua descrição, seu nível de criticidade, impacto ao negócio, causa, possíveis soluções e ações tomadas.
Dashboard gerencial com um mapa que é populado em tempo real mostrando de forma gráfica a origem de possíveis ataques e incidentes, seu nível de criticidade e seu destino.
KPIs e métricas de acompanhamento de cada incidente, hosts que são mais atacados, IPs que mais atacam com o seus países de origem
Correlacionamento de dados identificando quais são os tipos de incidentes mais gerados em um determinado ambiente, exemplo: São identificados mais incidentes e ataques em endpoints e em segundo nos Firewalls do ambiente.
Interação entre equipe do cliente e equipe da Redbelt, via tickets, para resolução de incidentes ou dúvidas referente aos mesmos.
Possibilidade de exportar um ou mais incidentes com todas as suas informações para análise externa.
Histórico de todas os incidentes identificados no ambiente, para base de tomada de decições na aquisição de novas soluções de segurança, direcionamento do time interno e outros.

Módulo de Gestão de incidentes

O módulo conta com um dashboard de acompanhamento que facilita a gestão à vista dos incidentes e do esforço da equipe



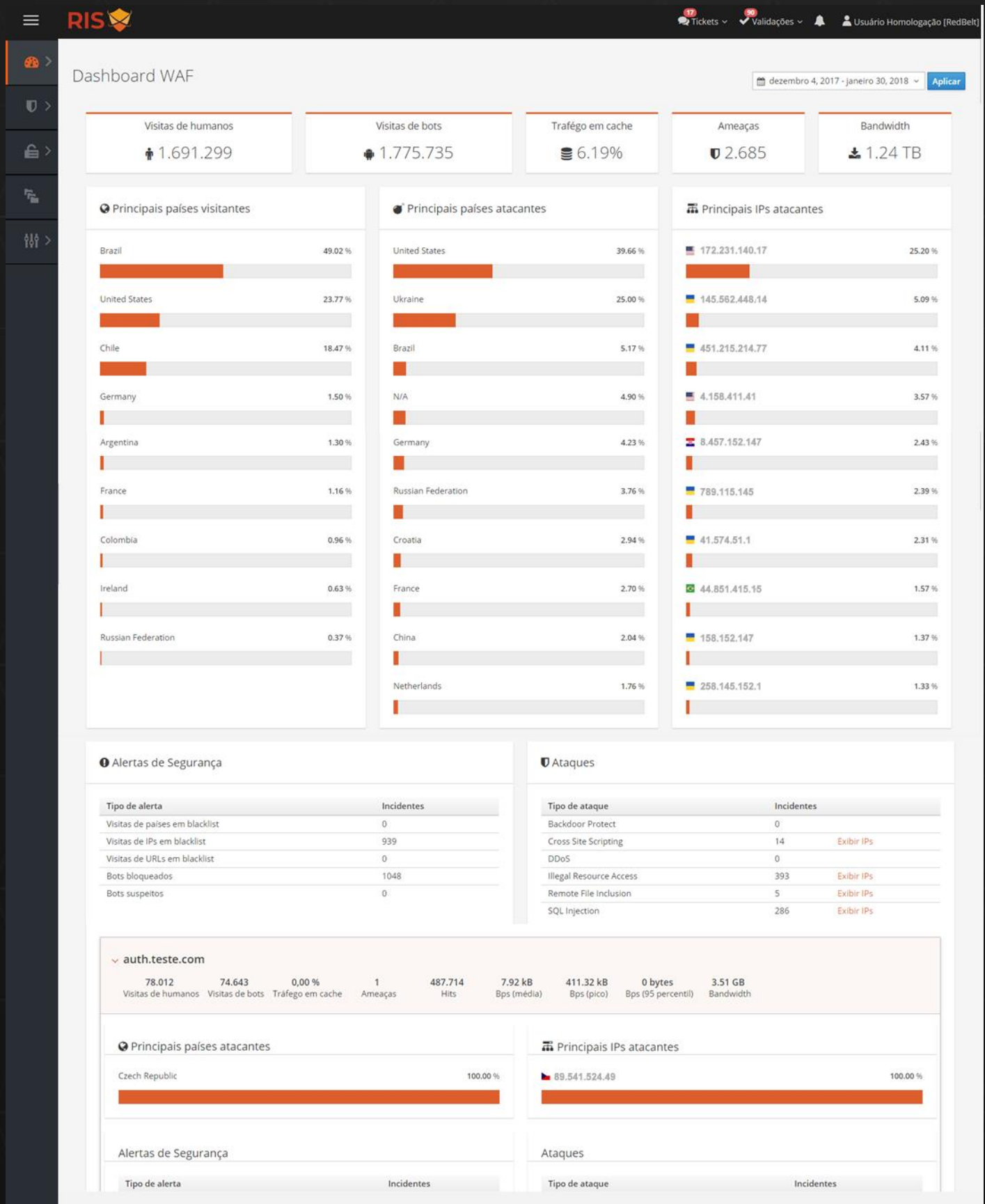
Módulo WEB Application Firewall

Através deste módulo é possível visualizar em tempo real todos os acessos, ataques e bloqueios que estão sendo realizados pelo WAF, correlacionando informações e identificando quais são os IPs que mais atacam o ambiente, sua localidade, recorrência e histórico com reputação.

Funcionalidades
Solução de Web Application Firewall (INCAPSULA) e de Anti-DDoS como SaaS, para aplicações Web.
Dashboard gerencial contendo informações sobre cada aplicação Web protegida como: quantidade de acessos realizado por "humanos" e por "bots", quantidade de tráfego analisado pelo WAF, quantidade de "cache" realizado e banda poupada, quantidade de ataques identificados e protegidos e seus tipos seguindo a OWASP Top 10, países eIPs que mais atacaram determinada aplicação e quais os tipos de ataques que mais acontecem por aplicação.
Visualização em real-time de todos os ataques que estão ocorrendo no ambiente ou em determinadas aplicações protegidas.
Tomada de decisões para bloqueios de Ips ou regiões geográficas, com base em ataques realizados e identificados.

Módulo WEB Application Firewall

O módulo conta com um dashboard de acompanhamento que facilita a gestão à vista dos incidentes.



Módulo Office 365

Com a integração do RIS com ao Office 365 é possível identificar ataques relacionados à identidade de usuários e administradores, escalação de privilégios, engenharia social, execução de ataques internos e espionagem industrial. Uma vez que esses incidentes são mapeados, ações podem ser tomadas para cessar os ataques. A ferramenta realiza ações de orquestração que são acionadas quando um ataque é identificado. Esse é o principal diferencial da ferramenta para cumprir o seu propósito: **o de reduzir o tempo de resposta a incidentes.**

Funcionalidades de Usuários e Administradores Ativos
Identificar a quantidade de usuários ativos, usuários que foram deletados e usuários inativos.
Identificar a quantidade de usuários com licença ativa e usuários não licenciados.
Identificar a quantidade de administradores ativos, dividindo por qual tipo de privilégio administrativo.
Identificar quais são os usuários ativos, inativos ou que foram excluídos.
Identificar quais são os usuários que estão com licença atrelada ou sem licença.
Identificar quais são os usuários administradores, dividindo por qual tipo de privilégio administrativo.
Identificar quais são os usuários internos ou externos com acesso a sua organização (por compartilhamento).
Correlacionar informações identificando quais são os usuários inativos com licenças atreladas ativas.
Correlacionar informações identificando quais são os usuários de serviços internos e se alguém o está usando, identificando pela última localidade de login.
Identificar quais grupos um determinado usuário faz parte ou pesquisar um grupo e identificar quais usuários estão dentro dele.
Identificar qual foi o último acesso de determinado usuário com informações detalhadas de sua localidade e de qual tipo de dispositivo ele acessou.
Identificar quais aplicativos estão sendo utilizados por um usuário dentro do plano dele.
Identificar quais foram os últimos 5 acessos de um determinado usuário com localização no mapa, informando também os respectivos dispositivos utilizados.
Informações detalhadas de cada usuários, com cargo, grupos pertencentes, licenças ativas, último acesso com hora, localidade, endereço IP e dispositivo.

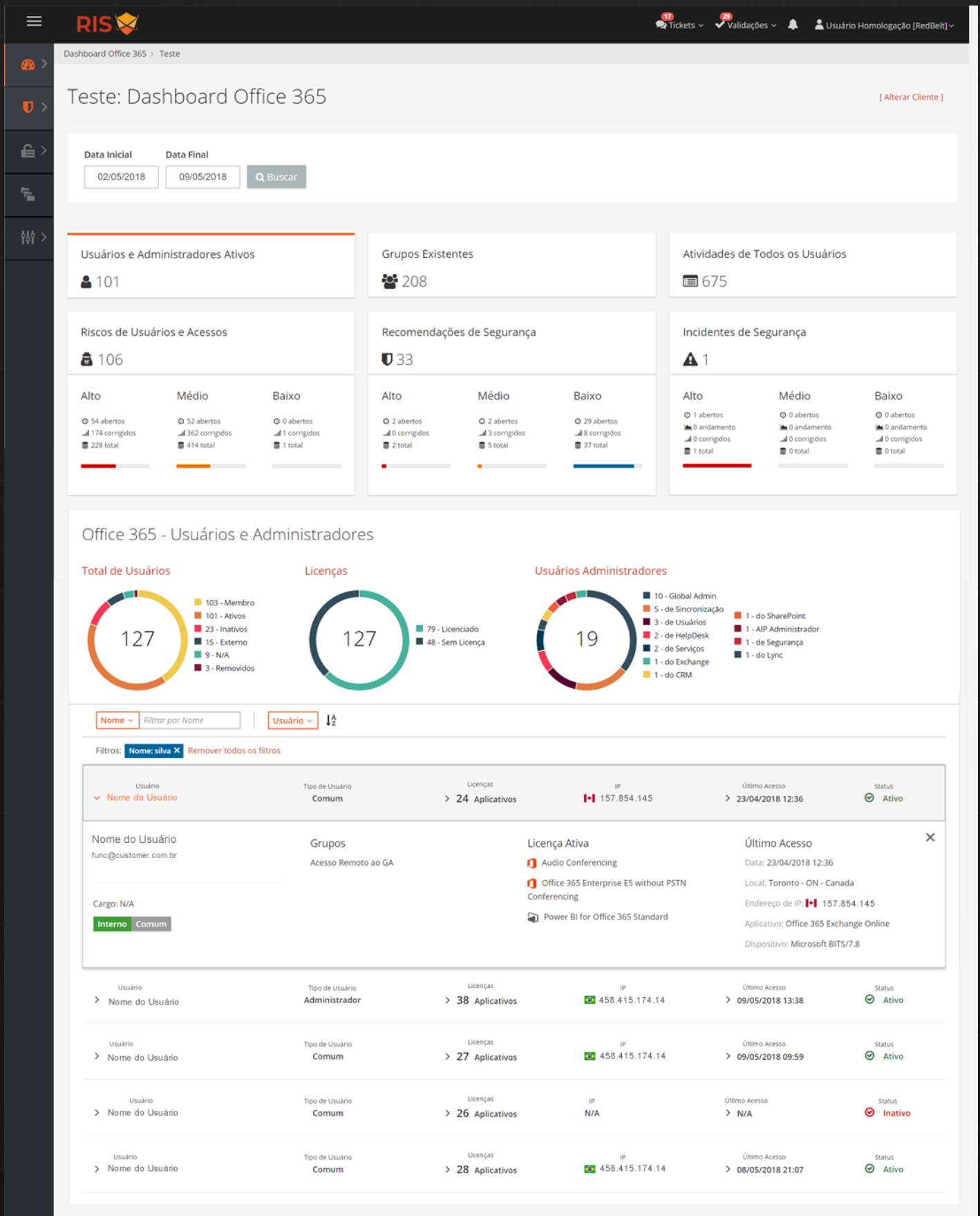
Módulo Office 365

Riscos de Usuários e Acessos (Análise Comportamental através de Aprendizado)
Correlacionar informações identificando que um determinado usuário está acessando através de uma conexão proxy para se tornar anônimo.
Correlacionar informações identificando que um determinado usuário está acessando através da rede TOR (Deep Web) para se tornar anônimo.
Correlacionar informações identificando quando um usuário acessa através de um IP identificado com alto risco por diversas blacklists.
Correlacionar informações identificando quando as credenciais do ambiente foram vazadas.
Correlacionar informações identificando "viagens impossíveis", baseando-se nos últimos 5 acessos dividindo por nivel de criticidade de país (alto) e estado (baixo)
Correlacionar informações identificando usuários que nunca logaram em 30 dias e "de repente" realiza uma conexão.
Correlacionar informações identificando ataques de Brute-force a determinadas contas.
Correlacionar informações identificando quais são os usuários novos externos.
Identificar e exibir todas as tentativas mal sucedidas de login de todos os usuários, mostrando suas últimas tentativas e localidades com auxilio de um mapa.
Exibir todas as conexões com sucesso e mal sucedidas do ambiente.

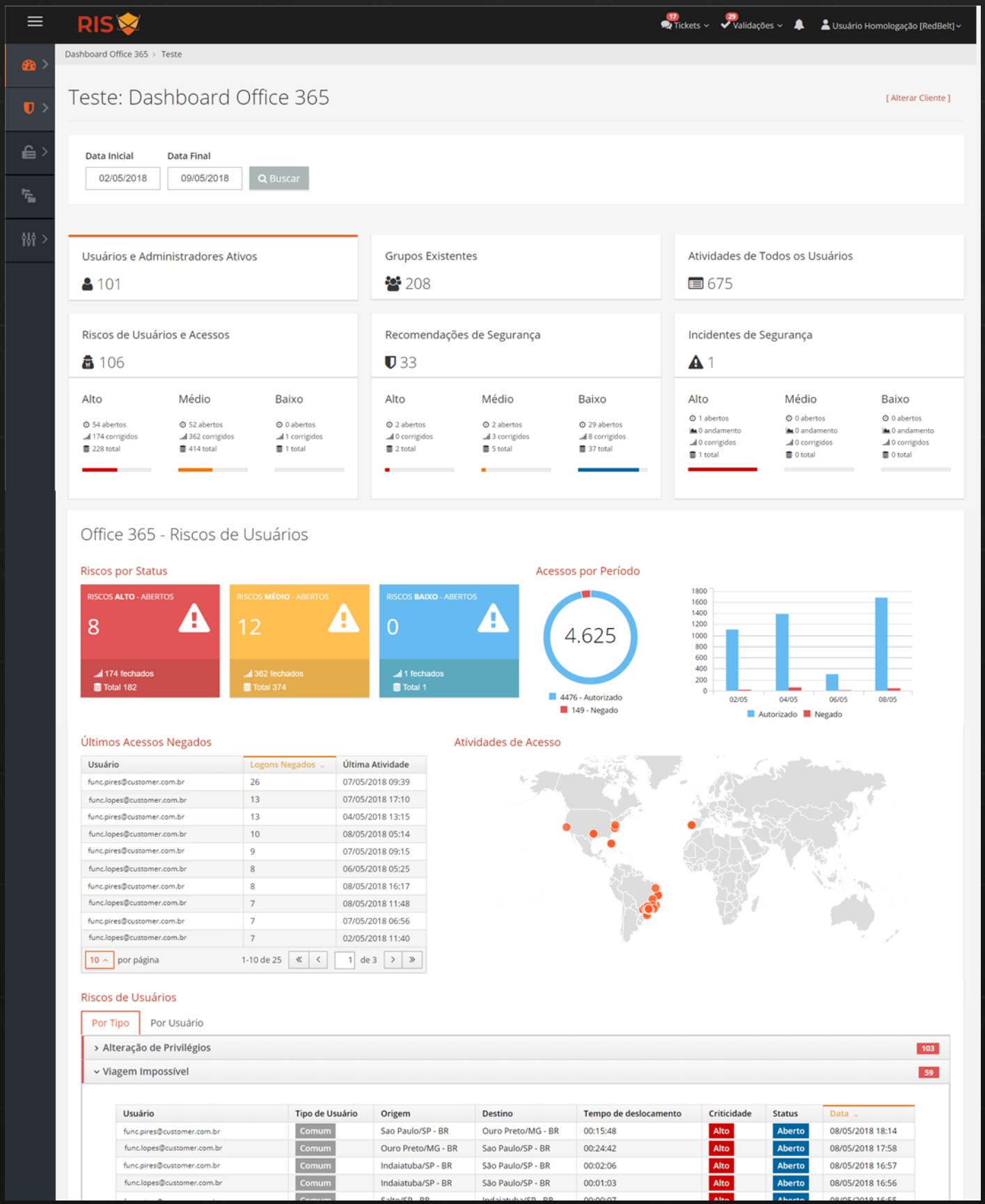
Incidentes de Segurança (Análise Comportamental através de Aprendizado)
Quando algum **privilégio** administrativo é dado a algum usuário novo.
Quando algum **privilégio** administrativo é removido de algum usuário.
Quando algum usuário administrador é **deletado** do tennant
Quando algum usuário **acessa** através de uma rede TOR (Deep Web).
Quando algum usuário administrativo que nunca se logou antes e "derrepente" realiza uma conexão, baseado nos últimos 30 dias (user behavior)

Módulo Office 365

Visão de usuários e administradores



Módulo Office 365



Módulo Office 365

Visão de Score e recomendações de segurança