

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

# O que é o RIS?

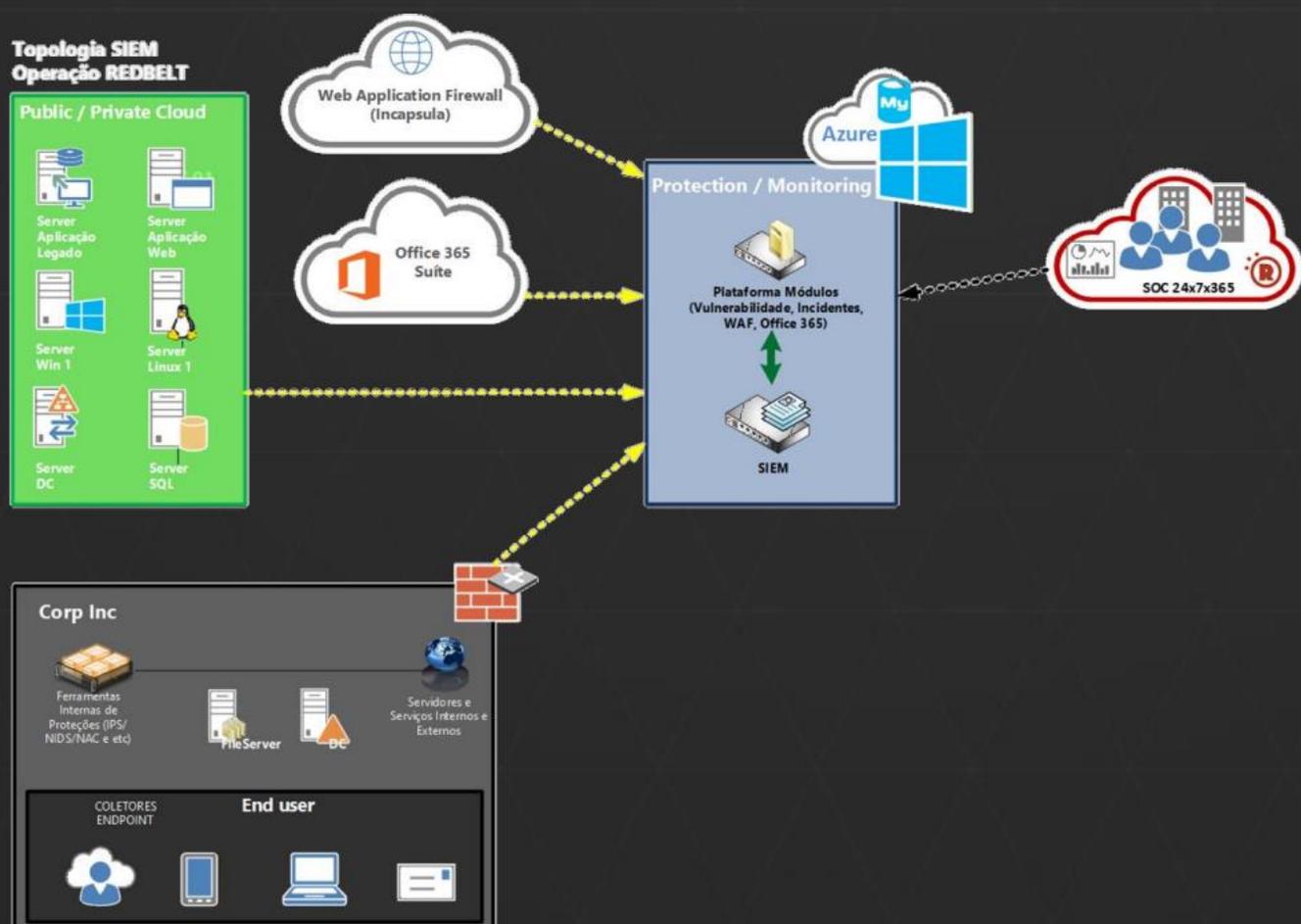
O RIS (Risk Information Security) é uma plataforma SaaS que integra soluções de diferentes fabricantes e permite concentrar e correlacionar as informações de segurança necessárias para um plano de ação, viabilizando a gestão do ciclo de vida de **vulnerabilidades** e **incidentes** de segurança.



## 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 ciclo 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.



Usuário Homologação [RedBelt]

Dashboard Vulnerabilidades

## Dashboard Vulnerabilidades

Empresa: Todas | Data Inicial: Dt. Inicial | Data Final: Dt. Final |

VUL. ALTAS - ABERTAS

233



23 em andamento  
135 corrigidas

Total de 391 Vulnerabilidades

VUL. MÉDIAS - ABERTAS

86



22 em andamento  
88 corrigidas

Total de 196 Vulnerabilidades

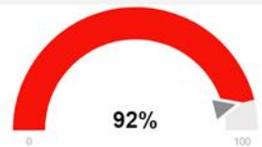
VUL. BAIXAS - ABERTAS

110



14 em andamento  
29 corrigidas

Total de 153 Vulnerabilidades



Pontuação de Risco

### Top 5 Servidores Vulneráveis

- Urano - Site Institucional
- Ceres - DRHUNET
- Cygni - wwwj
- Teste - Site Institucional
- Urano - CompraSH

### Top 5 Sistemas Vulneráveis

- Júpiter - Gestão Drawback
- Raiz - Site Institucional
- Andromedae
- Ceres - DRHUNET
- TESTE - Site Institucional

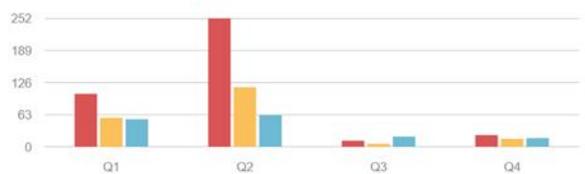
### Resumo de Tickets



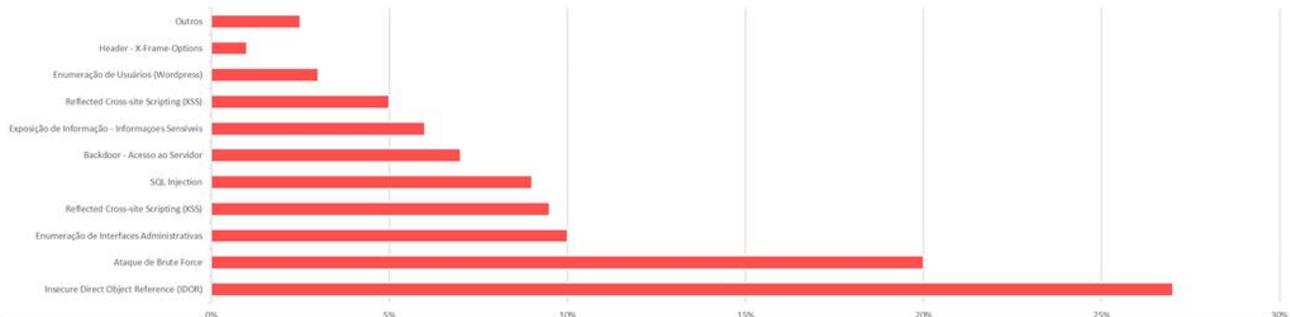
### Vulnerabilidades Abertas

Dias	Baixa	Média	Alta	Total
< 7	2	2	6	10
< 15	0	0	0	0
< 30	0	0	0	0
> 30	122	106	250	478

### Vulnerabilidades Por Quarter



### Top 10 Vulnerabilidades - Total



# 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 clio 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.

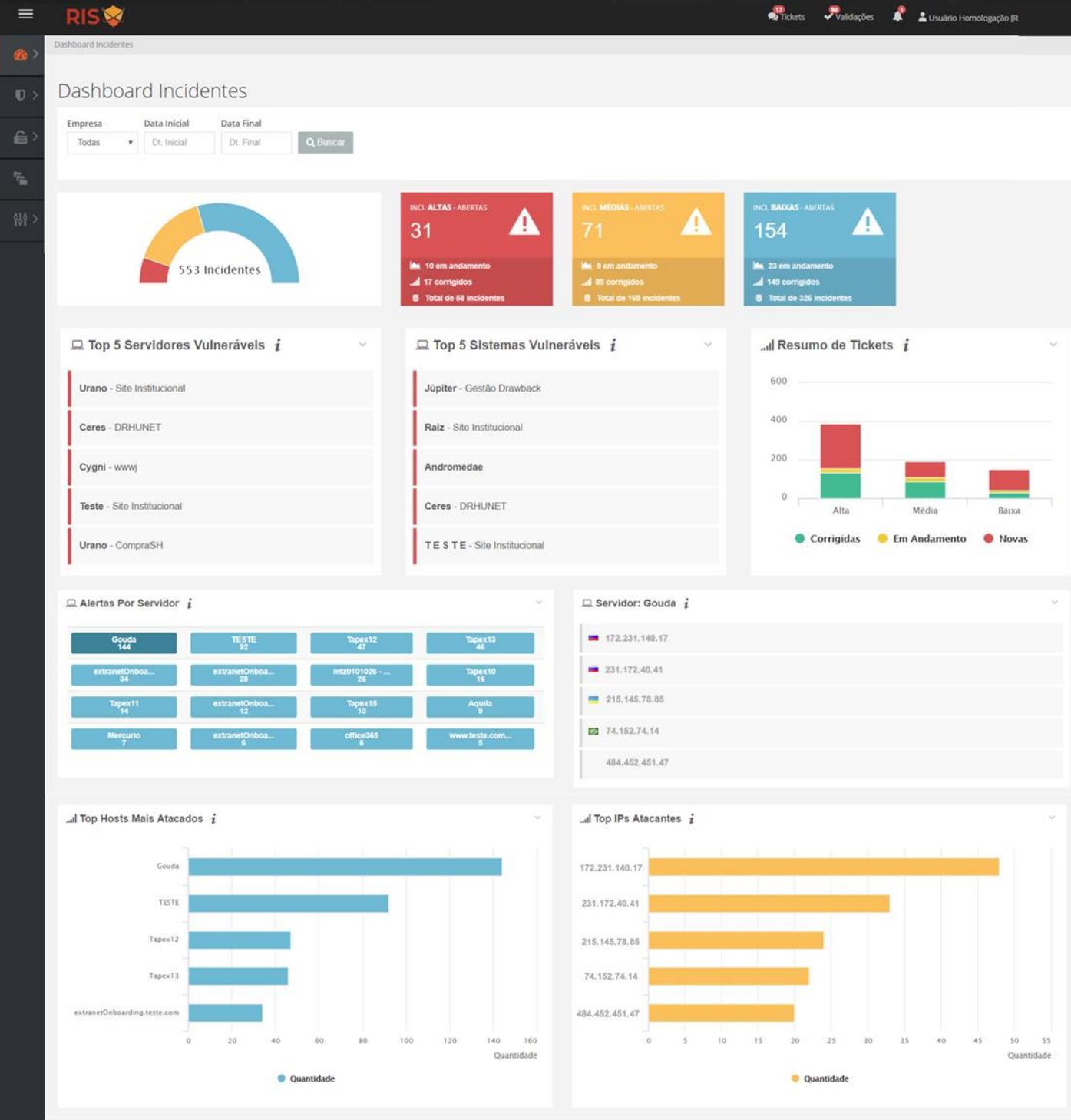
Interação entre equipe do cliente e equipe da Redbelt, via tickets, para resolução de incidentes ou dúvidas referente aos mesmos.

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 decisões 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 e IPs 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.

## Dashboard WAF

dezembro 4, 2017 - janeiro 30, 2018 [Aplicar](#)

Visitas de humanos

 1.691.299

Visitas de bots

 1.775.735

Tráfego em cache

 6.19%

Ameaças

 2.685

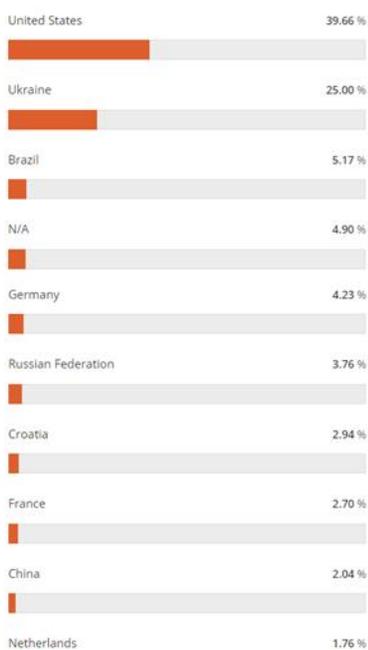
Bandwidth

 1.24 TB

### Principais países visitantes



### Principais países atacantes



### Principais IPs atacantes



### Alertas de Segurança

Tipo de alerta	Incidentes
Visitas de países em blacklist	0
Visitas de IPs em blacklist	939
Visitas de URLs em blacklist	0
Bots bloqueados	1048
Bots suspeitos	0

### Ataques

Tipo de ataque	Incidentes
Backdoor Protect	0
Cross Site Scripting	14 <a href="#">Exibir IPs</a>
DDoS	0
Illegal Resource Access	393 <a href="#">Exibir IPs</a>
Remote File Inclusion	5 <a href="#">Exibir IPs</a>
SQL Injection	286 <a href="#">Exibir IPs</a>

### auth.teste.com

78.012 74.643 0,00 % 1 487.714 7.92 kB 411.32 kB 0 bytes 3.51 GB  
Visitas de humanos Visitas de bots Tráfego em cache Ameaças Hits Bps (média) Bps (pico) Bps (95 percentil) Bandwidth

### Principais países atacantes



### Principais IPs atacantes



### Alertas de Segurança

Tipo de alerta	Incidentes
----------------	------------

### Ataques

Tipo de ataque	Incidentes
----------------	------------

# Módulo Office 365

Com a integração do RIS com o 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 nível 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 auxílio de um mapa.

**Exibir** todas as conexões com sucesso e mal sucedidas do ambiente.

## Incidentes de Segurança (Análise Comportamental através de Aprendizado)

Quando algum **privilegio** administrativo é dado a algum usuário novo.

Quando algum **privilegio** administrativo é removido de algum usuário.

Quando algum usuário administrador é **deletado** do tenant.

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

Dashboard Office 365 > Teste

### Teste: Dashboard Office 365

[ Alterar Cliente ]

Data Inicial: 
 Data Final:

<b>Usuários e Administradores Ativos</b> <span>👤 101</span>	<b>Grupos Existentes</b> <span>👥 208</span>	<b>Atividades de Todos os Usuários</b> <span>📄 675</span>
<b>Riscos de Usuários e Acessos</b> <span>🛡️ 106</span>	<b>Recomendações de Segurança</b> <span>🛡️ 33</span>	<b>Incidentes de Segurança</b> <span>🚨 1</span>

### Office 365 - Usuários e Administradores



Filtros: Nome: silva

Usuário	Tipo de Usuário	Licenças	IP	Último Acesso	Status
Nome do Usuário	Comum	> 24 Aplicativos	157.854.145	> 23/04/2018 12:36	Ativo
<div style="display: flex; justify-content: space-between;"> <div> <b>Nome do Usuário</b> func@customer.com.br  Cargo: N/A <span>Interno</span> <span>Comum</span> </div> <div> <b>Grupos</b> Acesso Remoto ao GA                 </div> <div> <b>Licença Ativa</b>                      Audio Conferencing                      Office 365 Enterprise E5 without PSTN Conferencing                      Power BI for Office 365 Standard                 </div> <div> <b>Último Acesso</b>                      Data: 23/04/2018 12:36                      Local: Toronto - ON - Canada                      Endereço de IP: 157.854.145                      Aplicativo: Office 365 Exchange Online                      Dispositivo: Microsoft BITS/7.8                 </div> </div>					
Nome do Usuário	Administrador	> 38 Aplicativos	458.415.174.14	> 09/05/2018 13:38	Ativo
Nome do Usuário	Comum	> 27 Aplicativos	458.415.174.14	> 09/05/2018 09:59	Ativo
Nome do Usuário	Comum	> 26 Aplicativos	N/A	> N/A	Inativo
Nome do Usuário	Comum	> 28 Aplicativos	458.415.174.14	> 08/05/2018 21:07	Ativo

# Módulo Office 365



Dashboard Office 365 > Teste

## Teste: Dashboard Office 365

[Alterar Cliente]

Data Inicial: 02/05/2018 Data Final: 09/05/2018

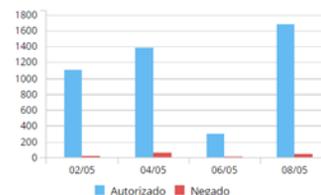
<b>Usuários e Administradores Ativos</b> 101	<b>Grupos Existentes</b> 208	<b>Atividades de Todos os Usuários</b> 675
<b>Riscos de Usuários e Acessos</b> 106	<b>Recomendações de Segurança</b> 33	<b>Incidentes de Segurança</b> 1

### Office 365 - Riscos de Usuários

#### Riscos por Status



#### Acessos por Período



#### Últimos Acessos Negados

Usuário	Logons Negados	Última Atividade
func.pires@customer.com.br	26	07/05/2018 09:39
func.lopes@customer.com.br	13	07/05/2018 17:10
func.pires@customer.com.br	13	04/05/2018 13:15
func.lopes@customer.com.br	10	08/05/2018 05:14
func.pires@customer.com.br	9	07/05/2018 09:15
func.lopes@customer.com.br	8	06/05/2018 05:25
func.pires@customer.com.br	8	08/05/2018 16:17
func.lopes@customer.com.br	7	08/05/2018 11:48
func.pires@customer.com.br	7	07/05/2018 06:56
func.lopes@customer.com.br	7	02/05/2018 11:40

10 por página 1-10 de 25

#### Atividades de Acesso



#### Riscos de Usuários

Por Tipo Por Usuário

- > Alteração de Privilégios 103
- > Viagem Impossível 59

Usuário	Tipo de Usuário	Origem	Destino	Tempo de deslocamento	Criticidade	Status	Data
func.pires@customer.com.br	Comum	Sao Paulo/SP - BR	Ouro Preto/MG - BR	00:15:48	Alto	Aberto	08/05/2018 18:14
func.lopes@customer.com.br	Comum	Ouro Preto/MG - BR	Sao Paulo/SP - BR	00:24:42	Alto	Aberto	08/05/2018 17:58
func.pires@customer.com.br	Comum	Indaiatuba/SP - BR	São Paulo/SP - BR	00:02:06	Alto	Aberto	08/05/2018 16:57
func.lopes@customer.com.br	Comum	Indaiatuba/SP - BR	São Paulo/SP - BR	00:01:03	Alto	Aberto	08/05/2018 16:56

# Módulo Office 365

## Visão de Score e recomendações de segurança



Usuário Homologação [RedBelt]

Dashboard Office 365 > Teste

### Teste: Dashboard Office 365

[Alterar Cliente]

Data Inicial: 02/05/2018  
Data Final: 09/05/2018  
[Buscar]

#### Usuários e Administradores Ativos

101

#### Grupos Existentes

208

#### Atividades de Todos os Usuários

675

#### Riscos de Usuários e Acessos

106



#### Recomendações de Segurança

33



#### Incidentes de Segurança

1



### Office 365 - Recomendações de Segurança

#### Timeline



#### Secure Score



#### Score em 30/04/2018

190 -1pts

Última alteração: 26/04/2018 | Score: 191

#### Máximo Score

364 +174pts

Score Atual: 190 | Score Máx: 364

#### Riscos

As seguintes ameaças podem ser evitadas ao tomar as ações recomendadas.

Você está atualmente em risco de ataque:

- Violação de conta
- Elevação de Privilégios
- Quebra de senha

#### Compare seu ambiente com outros semelhantes



- 190 - Your Secure Score Summary
- 49 - Office 365 Seat Size Average Score
- 30 - Office 365 Average Score

Recomendação	Pontos	Impacto	Custo
Ativar o MFA para todos os administradores globais	50/50pts	Impacto	Custo
Verifique semanalmente o relatório de acessos ocorridos após várias tentativas negadas	0/45pts	Impacto	Custo
Ativar regras de bloqueio de encaminhamentos do cliente	20/20pts	Impacto	Custo
Ativar Console de Gerenciamento de Segurança Avançado	20/20pts	Impacto	Custo
Habilitar políticas de prevenção de perda de dados (DLP)	0/20pts	Impacto	Custo
Ativar serviços de gerenciamento de dispositivos móveis	20/20pts	Impacto	Custo
Ativar MFA para todos os usuários	17/30pts	Impacto	Custo
Armazenar os documentos do usuário no OneDrive for Business	10/10pts	Impacto	Custo
As informações alternativas de contato estão completas para todos os usuários	1/1pts	Impacto	Custo
Permitir links anônimos de compartilhamento para sites e documentos	0/1pts	Impacto	Custo
Usar dados de auditoria	0/5pts	Impacto	Custo
Ativar recurso de lockbox do cliente	5/5pts	Impacto	Custo

**Reduza o tempo de respostas aos incidentes** e tenha uma experiência de segurança da informação integrada

Solicite a sua demonstração do RIS em <https://www.redbelt.com.br/ris.html>

