



Datasheet

RIS - Módulo de Vulnerabilidades

[Baixe aqui os datasheets dos outros módulos](#)

Entrega

No ambiente corporativo, o desafio é priorizar as vulnerabilidades que realmente importam em meio às centenas identificadas. Foi pensando na solução desse problema que o Módulo Vulnerabilidades foi desenvolvido.

A finalidade desse módulo é centralizar todas as vulnerabilidades encontradas no ambiente da empresa, reunindo informações de:

- Pentests efetuados pela equipe de Red Team da Redbelt;
- Integração automatizada com scanners de aplicações Web;
- Integração automatizada com o Service Now com gerenciamento de status, ou seja, quando uma vulnerabilidade é aberta no RIS, automaticamente é inserida no Service Now e quando o status muda no RIS ele também é modificado no Service Now.
- Vulnerabilidades em endpoints e redes, como por exemplo toda a família Tenable (Tenable.IO, Tenable.SC, Tenable.OT, Tenable.CS e Nessus Professional), além do Burp Suite Enterprise e Professional e das soluções da Qualys (VA e WAS).

O que é o RIS?

O RIS é a plataforma SaaS desenvolvida pela Redbelt Security que combina inteligência humana e orquestração. Combinando as soluções de diferentes fabricantes com a nossa inteligência, permite concentrar e correlacionar as informações e logs de segurança necessários para um plano de ação.

Possui 4 módulos para ajudar as empresas que desejam reduzir o tempo de resposta aos incidentes e gerenciar o ciclo de vida de vulnerabilidades no seu ambiente. Aqui, falaremos do módulo Vulnerabilidades. Aqui, falaremos do módulo Vulnerabilidades. Conheça os outros módulos [aqui](#).

Os dados são apresentados em um dashboard intuitivo com diversos indicadores, no qual as vulnerabilidades são identificadas, classificadas e categorizadas de acordo com os riscos que representam no ambiente. O RIS oferece apontamentos sobre impactos em ativos específicos, e sobre a importância desses ativos para o core business da empresa. Além disso, é possível entender, por meio do dashboard do RIS, se há a possibilidade de extração de informações e impacto em ambientes de produção, o que facilita o direcionamento e a priorização das ações de segurança.

A priorização preditiva é feita a partir da correlação de dados do próprio ambiente, como ativos expostos para a internet, serviços críticos sendo executados, aplicações do core business entre outras. O resultado garante uma redução mínima de 97% no número total de vulnerabilidades que precisam de correção imediata.

E há, ainda, a integração com o Qualys VM Scan, que eleva significativamente a eficácia e a centralização da gestão de vulnerabilidades. Essa integração possibilita:

Configuração Fácil: utilize as credenciais API do Qualys para conectar rapidamente.

Agendamento e execução de scans através do RIS: programe e configure scans do Qualys diretamente no RIS, escolhendo o agente, alvo e frequência.

Importação automática de resultados: opte por atualizações automáticas ou agendadas dos resultados dos scans no RIS.

Gerenciamento Centralizado: administre todas as vulnerabilidades detectadas em uma única plataforma.

O módulo Vulnerabilidades do RIS também conta com:

- Ciclo de vida de cada vulnerabilidade, indicando quais estão sendo tratadas, quais já foram corrigidas, abertas e quais foram aceitas como risco assumido.
- Visão de Inteligência Redbelt, traduzindo o que significa cada vulnerabilidade que identificamos como sendo as mais críticas ao negócio e o seu devido impacto.
- Vulnerabilidades que mais aparecem no seu ambiente contabilizando o total de vezes que aparecerem em hosts diferentes, exibindo também seu nível de criticidade
- Os hosts que mais possuem vulnerabilidades em seu ambiente, exibindo quantas críticas, altas, médias e baixas existem
- Total de updates que faltam em seu ambiente e em quais máquinas são necessários, possibilitando a mitigação de vulnerabilidades em massa através de aplicações de patches.
- Vulnerabilidades por tempo de vida em que foram descobertas no seu ambiente, exibindo se foram vistas pela primeira vez a menos de 7 dias chegando até a mais de 90 dias.

- Timeline com histórico comparativo do total de vulnerabilidades por dia. Elas estão sendo corrigidas ou só estamos acumulando riscos?
- Sistema de tickets e chat interno para tirar dúvidas ou direcionar vulnerabilidades para algum time da sua companhia corrigir.
- Possibilidade de solicitar redteste à nossa equipe de Red Team para vulnerabilidades inseridas através de Pentest.
- Definição personalizada de SLA por criticidade, permitindo a priorização das vulnerabilidades de acordo com o que foi definido para o seu ambiente.

Nesse módulo, é possível receber notificações sobre as vulnerabilidades diretamente no Microsoft Teams ou Slack. Assim, a empresa recebe atualizações instantâneas e gerencia a segurança do ambiente com mais dinamismo e eficiência.

> Converse com um de nossos consultores

E veja como o RIS pode elevar a segurança da sua empresa.