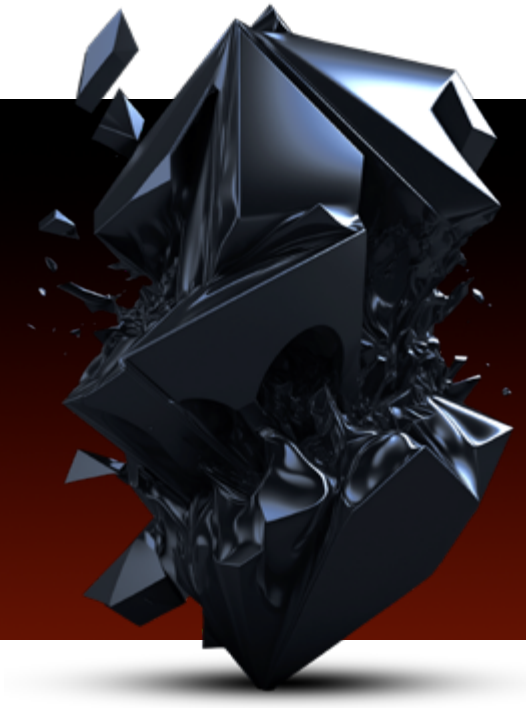
Datasheet

RIS - Módulo de Incidentes

Baixe aqui os datasheets dos outros módulos



Centralize e gerencie todos os alarmes e incidentes do seu ambiente com integrações automáticas aos principais SIEM's do mercado, adicionando enriquecimento de dados através de APIs interligadas ao RIS, integração entre times, handbooks e playbooks.

Reduzir o tempo de resposta aos incidentes é crucial. Porém, as tecnologias tendem a gerar muitos alarmes e é necessário agilidade para separar o que de fato merece atenção. O Módulo de Incidentes do RIS ajuda a qualificar os incidentes de forma ágil, adicionando metodologia e enriquecimento de dados.

Entrega

A Redbelt Security desenvolveu o Módulo de Incidentes do RIS para resolver a dor de empresas que já utilizavam outros provedores de MSS e SOC e não possuíam uma plataforma para centralizar a gerenciar seus alarmes e incidentes. A maioria das comunicações era feita apenas por e-mail ou sistemas que não tem como objetivo o gerenciamento de alarmes e incidentes, como o Jira e outros.

O Módulo de Incidentes é uma ferramenta completa no monitoramento e resposta a incidentes, com conexão automática aos principais SIEMs do mercado (IBM QRadar, Splunk e Azure Sentinel), em que tudo o que ocorre no RIS, é espelhado no SIEM, e vice-versa.

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 Incidentes. Conheça os outros módulos aqui.

Dessa forma é possível:

- Conectar o RIS a outras soluções de monitoramento com foco em ameaças de segurança, como IBM QRadar, Microsoft Sentinel, Microsoft Defender, Rapid7 Insight IDR, Imperva;
- Auxiliar os profissionais na rápida classificação de um determinado alarme, identificando se ele é de fato um evento real ou um falso-positivo;
- Grande redução no tempo de resposta e acuracidade dos dados.

Com foco sempre na excelência técnica, incluímos em todos os alarmes o que chamamos de Tasks, tarefas que seguem à risca a metodologia do SANS Institute, baseadas nas seis etapas de uma resposta a incidentes e identificação e coleta automática dos “agentes” dentro de um log (nome dado aos hosts de origem), destino, ofensor, data e outras informações importantes na análise.

Assim, o RIS gera indicadores e dados gerenciais que elevam a resposta a incidentes. Atualmente todos os clientes de MSS SOC da Redbelt Security utilizam o RIS como principal ferramenta, integrada com uma solução de SIEM implementada pelo nosso time.

Outras funcionalidades e indicadores:

- Dashboard com indicadores de todos os alarmes do ambiente, os que estão abertos, em andamento e corrigidos, dividindo-os por criticidade.
- Mapa geográfico exibindo em tempo real os ataques que estão ocorrendo no ambiente, mostrando origem, destino, criticidade e outras informações.
- Top alarmes que ocorreram em seu ambiente, identificando rapidamente quais são os 5 principais ofensores e os hosts afetados, por criticidade.
- Top hosts de seu ambiente, exibindo a quantidade total de alarmes por host afetado, único com a visão por criticidade dos alarmes.
- Gráficos exibindo os principais IPs atacantes e os principais tipos de alarmes, com curva de tendência para previsão de ataques futuros.
- Sistema de tickets e chat interno para tirar dúvidas em tempo real com a equipe da Redbelt Security ou direcionar o alarme para algum time interno da sua empresa tomar ação.
- Metodologia SANS aplicada em todos os alarmes e incidentes, com coleta de evidências em cada etapa, duração de tempo de cada atividade para avaliar SLA e captura e identificação automática dos agentes daquela ofensa.

- Dashboard gerencial contendo o SLA de todos os alarmes e incidentes tratados, para avaliar o tempo de resposta do time da Redbelt Security e do seu time interno.
- Toda segunda-feira envio automático por e-mail do resumo da semana, em formato PDF contendo informações sobre os alarmes e suas criticidades, SLA de atendimento, possíveis incidentes e outras informações gerenciais.

Nesse módulo, é possível receber notificações sobre incidentes 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 descubra como o RIS pode elevar a segurança da sua empresa.

› Converse com um de nossos consultores