FICHA TÉCNICA

MANAGED SECURITY SERVICES

MSS SOLUÇÕES MICROSOFT

Após realizar diversos projetos de implantação de soluções Microsoft em seus clientes, a RedBelt Security identificou que grande parte dessas soluções acabavam caindo em desuso ou não havia uma adoção significativa. Isso se dá por dois principais fatores:

- O cliente não tem um time especializado com conhecimento nessas tecnologias;
- O cliente não tem profissionais disponíveis para o gerenciamento e suporte dessas soluções.

Para resolver essa questão, a RedBelt Security criou o MSS Soluções Microsoft: serviços de gerenciamento e operação de Segurança em soluções Microsoft, implementando e garantindo a conformidade do ambiente com as práticas de Segurança do mercado e segmento corporativo.

Assim como o serviço de Monitoramento de Segurança, o MSS Soluções Microsoft também é realizado pelo nosso time especializado de SOC, responsável pela coleta, correlacionamento e análise dos eventos de Segurança provindos das ferramentas Microsoft, para assim identificar possíveis atividades maliciosas e ataques e responder de forma imediata.

SERVIÇOS PRESTADOS

> Monitoramento de segurança digital
> Classificação e Prevenção contra perda de dados
> Atendimento de N1 a N3 com mitigação de incidentes
> Tempo menor em resposta a incidentes de Segurança
> Visibilidade e consulta em tempo real de acontecimentos no mundo
> Visibilidade de Postura de Segurança em tempo real
> Relatórios de acompanhamento
> Planejamento de melhorias
> Criação de novas regras

> Criação de playbooks para resposta a incidentes e passagem de conhecimento para o time do cliente

> Assessments de políticas e regras de monitoria

> Simulação de ativações das regras

> Aumento na maturidade da Segurança do ambiente através da aplicação de Asessment de Segurança

TIME RESPONSÁVEL

Time de consultores Microsoft

+

SOC

FORMATO DE ENTREGA

SOC N1: monitoramento e identificação de alarmes e incidentes com remoção de falsos positivos.

SOC N2 e N3: resolução e resposta completa ao incidente com fechamento ao incidente, sem a necessidade de intervenção do time do cliente.

RIS: plataforma de gerenciamento de todos os alarmes, incidentes e Tickets com relatórios em tempo real.

SOLUÇÕES TRABALHADAS

Microsoft

> Solução de Antivírus e EDR (Microsoft Defender ATP);

> Suíte Microsoft 365 (Antispam, Antiphishing, DLP, Auditoria avançada e segurança em e-mails);

> Microsoft CASB (monitoramento e auditoria de segurança em aplicativos em nuvem e Shadow IT);

> Solução de MDM e MAM (gerenciamento de acessos e dispositivos através do Microsoft Intune);

> Classificação de dados e documentos (Microsoft AIP);

> Aplicação de Assessments de Segurança para identificar melhores práticas a serem aplicadas no ambiente.

EM CASO DE INTEGRAÇÃO

RIS: O365 e seus alertas integrado com o RIS. Azure ATP/ATA integrado com o RIS.