Estudo de Caso
Cyber Defense Center

VOTORANTIM

Perfil da companhia

Empresa brasileira fundada em 1918 com atuação em 20 países entre eles Espanha, Estados Unidos e Canada, nos setores de metais, siderurgia, cimento, celulose, energia, financeiro e alimentício.

- 34.658 funcionários
- 52,2 Mihões de toneladas materiais de construção / ano
- 475 mil toneladas de alumínio / ano
- 49 empreendimentos de geração de energia

* Fonte: Internet

Localização:

Sede localizada em São Paulo - SP com presença global e escritórios nas principais cidades dos países onde possui atuação.

O grupo Votorantim tinha o desafio de descobrir, responder e gerenciar os eventos de segurança da plataforma Microsoft 365 e Azure. O time de segurança da informação optou então pela busca de um parceiro especializado em Cloud Security.

O ambiente Votorantim possui uma média de 81 mil EPS decorrente de seus 27 mil usuários, fazer a gestão e tomada de decisões sobre esses eventos era um grande desafio. A Cloud Target buscou então entregar uma experiência com a utilização de inteligência artificial e *machine learning* centralizando os eventos de segurança na plataforma de SIEM e SOAR da Microsoft, o Azure Sentinel.

Obter melhor entendimento sobre como identificar e mitigar potenciais ameaças ao ambiente.

Uma vez tendo o **Azure Sentinel** como ponto central, eventos das soluções como **Azure Active Directory**, **Azure Identity Protection**, **Microsoft Cloud App Security, Microsoft Defender for Identity**, assim como os eventos de segurança e auditoria do **Office 365** foi possível entender os níveis de riscos que o ambiente encontrava-se exposto, o time então definiu uma estratégia para a aplicação de controles de segurança automatizados, através dos **playbooks** com o objetivo de remediar e proteger os usuários, de maneira eficaz e sem impactos ao dia-a-dia da companhia.

Com os *insights* e indicadores apresentados pelos dashboards em tempo real e relatórios mensais, as decisões passaram a ser tomadas com base em dados e fatos pelo time de segurança de informação.

Gestão de segurança centralizada e eficaz para elevar os níveis de segurança da informação de forma a não afetar a produtividade dos colaboradores.

PRODUTIVIDADE + SEGURANÇA + GOVERNANÇA

Cloud Target: +55 11 3181-7011 / contato@cloudtarget.com.br - www.cloudtarget.com.br