Threat Management & Protection

Serviço de segurança gerenciado da Cloud Target para o Microsoft 365 Defender

O serviço de Gerenciamento e Proteção contra Ameaças fornece às organizações o gerenciamento de plataformas de proteção contra ameaças cibernéticas. Combinando tecnologia de ponta e experiência em segurança cibernética, nosso serviço visa garantir a integridade, a confidencialidade e a disponibilidade de seus ativos digitais, protegendo sua organização contra ameaças cada vez mais sofisticadas. O serviço Threat Protection and Management é uma solução de segurança cibernética que aproveita as plataformas do Microsoft 365 Defender para proteger os ativos digitais das organizações contra ameaças sofisticadas. O serviço oferece recursos como implementação de políticas de segurança, gerenciamento de agentes, consultoria especializada, campanhas de conscientização e proteção contra phishing, além de relatórios e insights sobre a postura de segurança da organização. O serviço tem modalidades de contratação opcionais, como gerenciamento de comportamento de entidades e usuários, gerenciamento unificado de dispositivos e centro de operações de segurança.

Benefícios para o cliente

- **Implementação da política de segurança:** Configuramos e gerenciamos as políticas de segurança do Microsoft 365 Defender de acordo com as necessidades de sua organização, garantindo uma postura de segurança robusta e consistente
- **Gerenciamento de agentes:** Monitoramos a integridade e a segurança dos dispositivos, aplicando atualizações de agentes e políticas de segurança para manter seus dispositivos protegidos.
- **Consultoria especializada:** Nossos especialistas em segurança estão disponíveis para fornecer consultoria personalizada sobre práticas recomendadas de segurança, treinamento de conscientização e adaptação às tendências de ameaças emergentes.
- **Campanhas de conscientização e proteção contra phishing:** Configuramos campanhas de phishing e malware para conscientizar os usuários sobre e-mails maliciosos, reduzindo o risco de ataques de engenharia social