1.1 Gerenciamento de Entidades e Comportamento de Usuários

CATEGORIA: Managed Security Services

1.1.1 Descrição

A oferta de Gerenciamento de Entidades e Comportamento de Usuários é uma oferta de segurança cibernética para auxiliar organizações na proteção de ativos, contra ameaças internas e externas. Especificamente, essa oferta concentra-se no monitoramento, análise e resposta a atividades de entidades (como usuários, dispositivos e aplicativos) e seus comportamentos dentro do ambiente da organização.

1.1.2 Modalidades de Contratação

- Gerenciamento e Proteção contra Ameaças – Opcional
- Gerenciamento Unificado de Dispositivos – Opcional
- Security Operations Center - Opcional

1.1.3 Tecnologias utilizadas

Identity Access Management - IAM: Atualmente a Cloud Target opera exclusivamente a plataforma de IAM, Microsoft Entra ID. O licenciamento da solução é baseado por usuário mês.

Cloud Access Security Broker – CASB: Atualmente a Cloud Target opera exclusivamente a plataforma de CASB, Microsoft Defender for Cloud Apps. O licenciamento da solução é baseado por usuário mês.

Security Service Edge – SSE: Atualmente a Cloud Target opera exclusivamente a plataforma de SSE, Microsoft Entra Internet Access e Microsoft Entra Private Access. Não existe atualmente licenciamento da solução (preview).

Cloud Infrastructure Entitlement Management - CIEM: Atualmente a Cloud Target opera exclusivamente a plataforma de CIEM da Microsoft, Microsoft Entra Permissions Management. O licenciamento da solução é baseado por recurso mês.

1.1.4 Premissas

1.1.5 Escopo Serviços Gerenciados

Nosso serviço de Gerenciamento de Entidades e Comportamento de Usuários tem as seguintes capacidades:

Auditoria e Conformidade: O serviço ajuda a organização a cumprir requisitos regulatórios e padrões de segurança, mantendo registros de atividades e eventos relevantes;

Gerenciamento de Identidade e Acesso: O serviço auxilia na criação, alteração e remoção de contas de usuário, garantindo que apenas as pessoas autorizadas tenham acesso aos sistemas e dados;

Gerenciamento de Acesso Privilegiado: Entidades com privilégios elevados, como administradores de sistema, possuem maior acesso aos recursos críticos.

Gerenciamento de Tráfego e Atividades: O tráfego de rede, logs de eventos e atividades do usuário são monitorados para identificar quaisquer padrões suspeitos ou anomalias que possam indicar uma violação de segurança.

Itens incluso no Relatório de Métricas e Melhorias:

Métricas de Atendimento: visibilidade e transparência sobre as métricas de SLA, quantidade de requisições em andamento e resolvidas;

Taxa de conformidade: Avaliar a conformidade das aplicações em relação aos padrões de conformidade estabelecidas. Isso envolve monitorar se as configurações de segurança, como senhas fortes, criptografia de dados e atualizações do sistema operacional, estão sendo aplicadas corretamente nas aplicações utilizadas gerenciados;

Alertas e Relatórios: Alertas mensais para a organização, informando sobre atividades suspeitas, tendências de segurança e recomendações para melhorias contínuas.