Managed Detection and Response

Como a Cloud Target fornece serviços de detecção e resposta gerenciadas (MDR) usando a proteção contra ameaças da Microsoft

O serviço MDR (Managed Detection and Response, detecção e resposta gerenciada) da Cloud Target é responsável por monitorar, detectar, analisar e responder a incidentes de segurança em tempo real. O MDR da Cloud Target usa a plataforma Microsoft Sentinel SIEM, a plataforma Azure Logic Apps SOAR e a plataforma Microsoft Defender for Threat Intelligence Threat Feeds.

O MDR da Cloud Target oferece modalidades de contratação que incluem o CT Sentinel Fine Tuning, Equipe de Resposta a Incidentes (IRT) e serviços gerenciados de segurança e serviços da categoria Cyber Threat Intelligence. Esse serviço também executa o processo de Threat Hunting, que busca ameaças ativas no SIEM e no XDR do cliente que não tenham sido identificadas por uma regra de detecção.

Benefícios para o cliente

- **Monitoramento de segurança:** Monitora constantemente a infraestrutura de TI, os sistemas, os aplicativos e os registros de atividades para identificar comportamentos ou eventos suspeitos que possam indicar uma violação de segurança.
- **Detecção e análise de incidentes:** Quando um evento de segurança é detectado, a equipe de MDR investiga minuciosamente para determinar a natureza do incidente, sua gravidade e o impacto.
- **Contenção de ameaças:** Com base na análise, a MDR toma medidas para conter incidentes de segurança, como bloquear IPs mal-intencionados, desativar contas comprometidas ou fornecer orientação para que a equipe de TI da organização tome as medidas adequadas.
- **Busca de ameaças:** Busca mensal de ameaças ativas no SIEM do cliente com base na disponibilidade de registros e indicadores de comprometimento. Por meio dessa rotina, podemos identificar ameaças que não foram identificadas por uma regra de detecção. É uma segunda varredura em busca de comportamento malicioso no ambiente.