



Serviço Red Team

Cliente

Banca
Dimensão: 20.000
Presença Global

Desafio

O cliente procurou melhorar a sua postura de segurança e os seus protocolos de resposta para melhor se defender contra as ameaças cibernéticas, tais como ataques direcionados ou resgates. O seu objetivo era identificar pontos fracos nos seus sistemas e processos.

Solução

Forneceu-se um serviço de Red Team que cobria diferentes táticas, técnicas e procedimentos (TTPs), imitando ataques direcionados e ransomware. Durante o compromisso, a nossa equipa realizou várias atividades para recolher informações sobre a superfície de ataque exposta do cliente, tentar penetrar na rede do exterior e persistir dentro da rede.

Para o compromisso, definiu-se em conjunto com o cliente os diferentes vetores a serem realizados e as técnicas a serem usadas, que incluíam engenharia social, e-mails de phishing, dropped-media, movimento lateral e comunicação C2.

Após a execução do exercício, forneceu-se uma descrição detalhada das ações realizadas, dos caminhos de ataque utilizados e das vulnerabilidades exploradas para que o cliente pudesse analisar e melhorar a postura geral, incluindo os processos de deteção e resposta.

Durante o processo, trabalhamos com a equipa SOC/Blue Team do cliente para ajudar a identificar pontos cegos e avaliar as melhorias implementadas após o exercício.

Impacto

O cliente agora tem uma compreensão melhor da superfície de ataque exposta, das fraquezas nos sistemas e processos, e melhorou a resiliência geral aos ataques e os mecanismos e processos de deteção e resposta, reduzindo consideravelmente o risco para a organização.

Serviços Relacionados

- Red Teaming

Making your tech journey **more secure.**

Para mais informações visite

www.integrity.pt