FRUSTRE CYBER-ATAQUES ANTES MESMO QUE ACONTEÇAM

VISUALIZE SUA REDE PELOS OLHOS DE UM HACKER

Um hacker dedicado avaliará suas medidas de segurança e encontrará maneiras de contorná-las. A questão é o que acontece depois que eles violam seu perímetro.

A XM Cyber oferece a capacidade de visualizar sua rede da maneira que o hacker a vê, ajudando a encontrar todos os vetores ocultos de ataque existentes, incluindo aqueles que normalmente ficam abaix do radar da maioria das medidas de proteção. E uma vez que um caminho de ataque é identificado, a XM Cyber fornece um relatório de remediação focado e priorizado para que você possa corrigir esses pontos fracos antes que o hacker alcance.

A XM Cyber oferece a única solução disponível que simula com segurança uma ameaça persistente avançada (APT) contra os ativos críticos da sua organização.

Nossa abordagem patenteada ajuda a reduzir o seu risco, expondo lacunas resultantes de sistemas não-corrigidos, erros de configuração, falhas de software e erro humano.

Independentemente dos seus controles de segurança, se houver um vetor de ataque que, por qualquer meio, possa alcançar os seus ativos críticos, a XM Cyber vai encontrá-lo.

Mais do que uma simulação de brecha e ataque: um APT totalmente automatizado

Identifique cada vetor de ataque que os hackers podem

Proteja dados críticos armazenados na AWS

Arquitetura flexível on-prem ou na nuvem

Funciona com segurança, sem impacto na sua rede de produção

Remediação priorizada de falhas de segurança

Valide seus controles de segurança

XM CYBER

CLIQUE ABAIXO PARA ASSISTIR
https://youtu.be/G7SINpADHBY

VEJA COMO A XM CYBER EXPÕE CONTINUAMENTE OS VETORES DE ATAQUE QUE AMEAÇAM SEUS ATIVOS CRÍTICOS E FORNECE REMEDIAÇÃO PRIORIZADA E ATIVA

ENCONTRE LACUNAS QUE NINGUÉM MAIS VÊ

EXCETO OS HACKERS

Hackers exploram todas as aberturas, aguardando mudanças que possam aproximá-los dos ativos críticos da sua organização. A melhor defesa é agir da mesma forma: seja proativo na busca de caminhos de ataque.

Testes manuais não são eficazes porque sua rede muda constantemente. Para entender realmente seu risco, você precisa executar 24/7 em seu ambiente de produção, melhorando constantemente sua postura de segurança.

Testar controles de segurança é importante, mas você também deve ser capaz de detectar todos os caminhos de ataque que escapam às suas soluções de segurança existentes, além de visualizar esse ataque enquanto ele viaja por toda a sua organização, incluindo seus ativos na nuvem.

Ao identificar e priorizar a segurança que protege os dados mais importantes, os clientes da XM Cyber otimizam seus investimentos em segurança e reduzem significativamente os riscos e o impacto de uma brecha.

PENSE COMO UM HACKER PARA PARAR UM HACKER

Confirme que nenhum vetor de ataque permita acesso a ativos críticos

Automatize processos combinados de red team e blue team num purple team automatizado

Melhore a higiene geral de TI e reduza erros de configuração e o efeito do erro humano

Otimize sua equipe de segurança e reduza a dependência de testes manuais

Priorize atividades de segurança para proteger seus dados mais importantes

Acrescente automaticamente as mais recentes técnicas de ataque à sua estratégia de defesa

CASES DE SUCESSO

Desafios de migração para a nuvem. Uma instituição financeira estava migrando aplicativos-chaves para a nuvem. A XM Cyber identificou rapidamente que as regras do ambiente antigo ainda estavam em vigor. Novos dispositivos estavam sendo adicionados sem proteção e vários caminhos de ataque foram expostos.

Questões de higiene de TI. Um gerente de rede estava com pressa. Ele alterou os direitos de administrador em um servidor para atualizar uma nova conexão de rede Wi-Fi, esquecendo de alterá-los de volta. A XM Cyber usou essas credenciais para alcançar o seu servidor financeiro durante uma simulação.

Infraestrutura crítica. A XM Cyber encontra regularmente redes de TI padrão implementadas em redes operacionais com links entre os dois sistemas. Mesmo que hackers e malware não possam afetar esses sistemas operacionais, eles podem bloquear o acesso e desligar efetivamente operações inteiras.

Conexões air-gapped. Até redes air-gapped (fisicamente isoladas) estão suscetíveis a erro. A XM Cyber relevou o uso de USB e conexões de rede conectadas incorretamente, o que levou a redes isoladas, permitindo vetores de ataque.

Conexões de terceiros. Os fornecedores geralmente têm acesso à rede de seus clientes para simplificar a cadeia de suprimentos. As credenciais podem ser roubadas de vários pontos nos portais de fornecedores e clientes. A XM Cyber testa continuamente se essas credenciais e conexões podem chegar aos seus ativos críticos.

Criação de um purple team. Uma companhia de seguros líder de mercado não podia sincronizar os esforços dos seus red team e blue team. Usando a XM Cyber, o cliente unificou as duas equipes, melhorando a produtividade, permitindo uma troca mais rápida de idéias, observações e insights. O resultado foi uma maior visibilidade da superfície de ataque dentro de sua organização.

SOBRE A XM CYBER

A XM Cyber foi fundada por executivos do setor de segurança de elite da Inteligência Israelense. Sua equipe principal é composta por veteranos altamente qualificados e experientes, com expertise em cyber-segurança ofensiva e defensiva. A XM Cyber desenvolveu mais de 15 tecnologias patenteadas baseadas em um conjunto exclusivo de algoritmos que permitem a simulação contínua e automática das técnicas e métodos de um hacker.

XM CYBER

Tel Aviv +972 3 978 6668 New York +1 866 598 6170 Sydney +61 2 8880 0705 London +44 203 322 3031 info@xmcyber.com