H-CYBER INTELLIGENCE

(SERVIÇO DE ANÁLISE E INTELIGÊNCIA DE AMEAÇAS CYBER)

CYBER EFFECT - NÍVEL 3 - PRODUTIVO

h·cyber INTELLIGENCE

DESCRIÇÃO

A equipa do Serviço de Análise e Inteligência de Ameaças Cyber (CTI) fornece aos clientes informações sobre ameaças e ATP's, que ajudam a mitigar ações externas contra os nossos clientes. As fontes de inteligência de ameaças cyber incluem inteligência via OSINT, intel via meios de comunicação social, intel humana, intel técnica ou intel via deep e dark web, redes Tor, Freenet, I2P, Riffle e outras.

PROPOSTA DE VALOR

O Serviço de Análise de Inteligência de Ameaças Cyber entrega dados transformados, recolhidos por métodos tradicionais de inteligência a partir das plataformas partilhadas por ATP's, num relatório integrado para o cliente. Os métodos tradicionais de inteligência podem incluir seguimentos passivos, ou criar 'persona' ativa, para descobrir o que os atacantes estão a discutir/planear, os seus novos métodos, as suas informações coletadas do nosso cliente alvo e todos os outros detalhes operacionais. Certamente que estes métodos requerem um elevado nível de conhecimento e experiência, de forma a permitir aos clientes tomar decisões proactivas na sua infraestrutura de TI. Os agentes de ameaças operam em "matriz", espalhados por diferentes locais, sendo difícil localizá-los através de informações anteriormente recolhidas sobre esta mesma "matriz".

CARACTERÍSTICAS DO SERVIÇO

O Serviço Análise e Inteligência de Ameaças Cyber é composto pelos seguintes elementos:

- **Cyber Bits:** breves noticias de inteligência sobre temas relacionados com o ciberespaço.
- Open Source Intelligence (OSINT), que visa captar os eventos públicos mais importantes da semana, que ocorreram num domínio cibernético amplamente compreendido.

Rua Acácio de Paiva 16
1ºD - 1700-006 Lisboa
www.hardsecure.com
(+351) 218 278 126
geral@hardsecure.com

H-CYBER INTELLIGENCE

(SERVIÇO DE ANÁLISE E INTELIGÊNCIA DE AMEAÇAS CYBER)

CYBER EFFECT - NÍVEL 3 - PRODUTIVO

- Atualização de URLs maliciosos de código aberto e pacotes de exploração.
- Fóruns em linha com as recentes descobertas, redes sociais, monitorização de blogs.
- Ligação com outros membros e organizações de segurança.
- Taxonomia Comum para as Redes Nacionais de Equipas de Resposta a Incidentes de Segurança Informática (CSIRTs).
- **Tendências:** atualizações sobre padrões emergentes e sobre novos modus operandi, ferramentas e técnicas que os cibercriminosos utilizam.
- **Conhecimento:** orientação sobre diferentes aspetos do cibercrime, tais como infraestruturas, ferramentas e modus operandi.

VALOR ACRESCENTADO

O CTI é uma capacidade essencial no programa de segurança de uma organização. Utilizado corretamente, o CTI pode permitir uma melhoria da segurança e decisões comerciais mais bem informadas e, em última análise, permitir que os clientes tomem medidas decisivas para proteger os seus utilizadores, dados e reputação contra elementos desconhecidos de forma proativa (ou seja, com prévio acesso a informação que diz respeito à sua instituição).

O CTI inclui frequentemente a assinatura, reputação e alimentação de dados sobre ameaças, mas vai além destes, em quase todos os sentidos. As nossas atividades típicas envolvem:

- Recolha constante de informação humana e técnica à escala global.
- Fornecimento de dados contextualizados, ricos e virados para o adversário.
- Personalização para os nossos parceiros e clientes.

O CTI permite aos nossos clientes serem proactivos e prepararem-se para os adversários e ameaças do amanhã, em vez de reagirem aos ataques de ontem. Sem a capacidade de considerar todos os riscos e opções à sua disposição, os profissionais de Cibersegurança não poderão tomar as melhores decisões de segurança possíveis para a sua organização.

Rua Acácio de Paiva 16
1ºD - 1700-006 Lisboa
www.hardsecure.com
(+351) 218 278 126
geral@hardsecure.com

H-CYBER INTELLIGENCE

(SERVIÇO DE ANÁLISE E INTELIGÊNCIA DE AMEAÇAS CYBER)

CYBER EFFECT - NÍVEL 3 - PRODUTIVO

Aqui estão alguns dos benefícios do nosso Serviço de Análise e Inteligência de Ameaças Cyber:

» Perceção e contexto valiosos: Informação detalhada sobre quais as ameaças mais suscetíveis de afetar uma organização ou indústria, e indicadores para ajudar a prevenir e detetar ataques.

» Períodos de resposta a incidentes melhorados: Priorização de alertas, o que permite a uma organização responder mais rapidamente a ameaças reais e reduzir o risco de graves consequências de violação de dados.

» Melhorar a comunicação, planeamento e investimento: As equipas de segurança podem comunicar riscos reais ao negócio e concentrar-se na proteção de alvos de alto risco contra ameaças reais, através de investimento e planeamento de segurança adicionais.

PEDIDOS DE PROPOSTA / INFORMAÇÃO

Para informações adicionais ou mais esclarecimentos, por favor entre em contato através de um dos seguintes meios:

Formulário "Hardsecure – Serviço de Análise de Inteligência de Ameaças Cyber" (disponibilizado na página do serviço no website)

Comercial da Hardsecure:
(+351) 218 278 126
geral@hardsecure.com

Website:
www.hardsecure.com (Formulário **"Solicitar Proposta"**)