

H-CYBER ASSET

(SERVIÇO DE SUPORTE PARA PROTEÇÃO A ENDPOINTS (CIS))

CYBER EFFECT - NÍVEL 0 - BÁSICO



DESCRIÇÃO

h.cyber ASSET

Fornecimento de serviços especializados para a implementação, configuração e gestão de software de segurança no endpoint do cliente. Estes serviços destinam-se a proteger os endpoints do cliente contra ataques e possíveis comprometimentos.

O serviço para proteção dos endpoints, consiste na execução dos seguintes controlos obrigatórios/opcionais:

- » Anti-malware.
- » Prevenção de Intrusão Host-based (HIPS).
- » Navegação segura na web.
- » Firewall.
- » Gestão e controlo de forma centralizada dos endpoints.
- » Proteção de equipamentos de media removíveis.
- » Prevenção de fugas de dados (DLP).
- » Encriptação.
- » Proteção contra malware e configuração de protocolos de segurança (SPF, DKIM, DMARC,...) para o serviço de email.
- » Gestão de atualizações dos ativos ligados na rede de dados.
- » Endpoint Detection and Response.



H-CYBER ASSET

(SERVIÇO DE SUPORTE PARA PROTEÇÃO A ENDPOINTS (CIS))

CYBER EFFECT - NÍVEL 0 - BÁSICO

» Medidas de segurança que impedem a utilização de suportes amovíveis não autorizados para armazenamento de informação.

» Diretrizes de configuração para o hardening com base em boas práticas de segurança (standards, frameworks e guidelines dos fabricantes).



PROPOSTA DE VALOR

O serviço para Proteção de Endpoints (CIS) permite a implementação coerente da segurança em toda a organização, alinhado com as políticas e requisitos técnicos de segurança, de forma a fortalecer a proteção contra ataques informáticos realizados internamente/externamente.



CARACTERÍSTICAS DO SERVIÇO

Utilização de conhecimentos aprofundados na implementação, configuração e gestão do software no Endpoint do cliente. Inclui:

- ▶ Gestão do ciclo de vida completo com base nos controlos de segurança, assegurando a atualização dos ativos.
- ▶ Revisão e adaptação da configuração e orientação recomendadas para cada release/versão dos fabricantes.
- ▶ Fornecimento de suporte técnico de segundo e terceiro nível.
- ▶ Suporte na correção de vulnerabilidades, complementando através da análise de vulnerabilidades, se aplicável.



H-CYBER ASSET

(SERVIÇO DE SUPORTE PARA PROTEÇÃO A ENDPOINTS (CIS))

CYBER EFFECT - NÍVEL 0 - BÁSICO



VALOR ACRESCENTADO

O nosso foco é:

» Poupar dinheiro a longo prazo

Quanto menos hardware e software estiver instalado no endpoint, menos dinheiro o cliente terá de gastar em atualizações e em despesas para remover malware. O hardening no endpoint liberta mais espaço no computador, o que significa que o cliente não tem de comprar mais memória e/ou capacidade de disco.

» Eliminar pontos de acesso

A remoção de ficheiros desnecessários, serviços, software e partilha de ficheiros reduz o número de pontos de acesso, aos quais um hacker poderá aceder.

» Reduzir falhas de segurança

O hardening contribui, em vários níveis de segurança, para proteger os utilizadores e a sua informação. O hardening também remove ficheiros e programas desnecessários, que são frequentemente esquecidos, e que proporcionam aos hackers acesso “camuflado” ao sistema.

» **Instalação, configuração e manutenção de EDR (Endpoint Detection and Response) e IDS**, de forma a garantir uma completa visibilidade no endpoint e na rede de dados do cliente.



H-CYBER ASSET

(SERVIÇO DE SUPORTE PARA PROTEÇÃO A ENDPOINTS (CIS))

CYBER EFFECT - NÍVEL 0 - BÁSICO



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 Suporte para Proteção a Endpoints (CIS)”
(disponibilizado na página do serviço no website)



Comercial da Hardsecure:

(+351) 218 278 126

geral@hardsecure.com



Website:

www.hardsecure.com (Formulário “Solicitar Proposta”)

