

H-CYBER MONITOR

(SERVIÇO DE MONITORIZAÇÃO DE CIBERSEGURANÇA)

CYBER EFFECT - NÍVEL 1 - REATIVO

Esta datasheet apresenta de forma genérica o nosso serviço. O âmbito efetivo e condições da prestação do serviço, terão de ser refletidas em proposta técnica e comercial.



DESCRIÇÃO



O Serviço de Monitorização de Incidentes de Segurança, fornece a monitorização de todos os ativos (internos ou externos), que estejam dentro do âmbito que venha a ser definido, para detetar e identificar ameaças e Indicadores de compromisso (IoC), a fim de assegurar a monitorização da segurança no ambiente da organização em tempo real.



PROPOSTA DE VALOR

Este serviço foi concebido para detetar incidentes, como pré-requisito para a resposta a incidentes. Ao monitorizar diariamente milhões de eventos, o Serviço proporciona uma visibilidade ao cliente, garantindo:

- » A identificação de *Data Leaks* que são detetadas e/ou exfiltradas.
- » Serviços de monitorização de segurança aos serviços, portas, protocolos, aplicações publicadas para fora da organização (sites, aplicações, serviços...).
- » A identificação de malware que esteja em execução (*ransomware, bots, trojans,...*).
- » A identificação de IPs internos que estejam a efetuar pedidos de sessão a domínios externos identificados como *blacklists* e que possam comprometer a organização.
- » Os eventos são correlacionados e analisados por analistas de segurança qualificados e experientes, para ações apropriadas, conforme o tipo de incidente.



H-CYBER MONITOR

(SERVIÇO DE MONITORIZAÇÃO DE CIBERSEGURANÇA)

CYBER EFFECT - NÍVEL 1 - REATIVO

Esta datasheet apresenta de forma genérica o nosso serviço. O âmbito efetivo e condições da prestação do serviço, terão de ser refletidas em proposta técnica e comercial.

- » A correlação feita a partir de várias *sources* (AD, *firewalls*, antivírus, servidores, routers,...) que permite criar uma imagem e *tracking* de ações.
- » A monitorização comportamental dos ficheiros (FIM – *File Integrity Monitor*), através da monitorização de ficheiros e alerta de alterações (edição, eliminação, *upload*,...).
- » Da monitorização das políticas de segurança e da sua conformidade, de acordo com o ciclo de vida do *software* e *hardware*.



CARACTERÍSTICAS DO SERVIÇO

Este serviço é definido pelos seguintes elementos:

- ▶ **Fornecimento da capacidade para verificar todo o tráfego de entrada/saída**, para assegurar a conformidade com as normas de segurança e as políticas de segurança aplicáveis aos clientes; tais verificações incluem código malicioso, conteúdo executável, conteúdo encriptado, SPAM, conteúdo de dados classificados.
- ▶ **Monitorização do serviço de saída de correio eletrónico**, quer centralmente pela Equipa de Resposta a Incidentes, quer localmente pelas equipas de TI do cliente.
- ▶ **Monitorização dos sites, aplicações e serviços do cliente na Internet**, para alterações não autorizadas e para tomar as medidas apropriadas de comunicação/remediação.
- ▶ **Serviços de Monitorização, Detecção e Prevenção na intrusão na rede e nos endpoints**, geridos e monitorizados centralmente.



H-CYBER MONITOR

(SERVIÇO DE MONITORIZAÇÃO DE CIBERSEGURANÇA)

CYBER EFFECT - NÍVEL 1 - REATIVO

Esta datasheet apresenta de forma genérica o nosso serviço. O âmbito efetivo e condições da prestação do serviço, terão de ser refletidas em proposta técnica e comercial.



VALOR ACRESCENTADO

- » Redução do tempo de exposição face a ataques informáticos.
- » Este serviço atua de forma preventiva, atuando sob a forma de aprendizagem do tráfego da rede e do comportamento dos *endpoints*, permitindo executar ações de melhoria nas configurações da rede e dos *endpoints* dos clientes (IT, IoT & OT), minimizando a possibilidade de paragens de serviços, que podem resultar em custos financeiros significativos para os clientes.
- » Diminuição de danos face a ciberataques. Os ataques informáticos podem degradar a reputação de qualquer negócio/instituição e podem também causar violações/perdas significativas de informação. Muitas destas ciberameaças concentram-se na intrusão na rede para roubo de informação valiosa.
- » Detecção automática de atividades invulgares/irregulares dentro da rede de dados dos clientes, evitando que ciberameaças se propaguem a outras áreas da instituição que possam causar danos generalizados.



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 Monitorização de Cibersegurança” (disponibilizado na página do serviço no website)



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



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

A **Hardsecure** é uma empresa portuguesa, fundada em 2011, conta com uma equipa altamente especializada que **presta serviços** e implementa **soluções inovadoras** exclusivamente nas áreas de **Segurança em Sistemas de Informação e Cibersegurança**.



Rua Acácio de Paiva 16
 1º Dto - 1700-006 Lisboa



www.hardsecure.com



(+351) 218 278 126

@ geral@hardsecure.com