

H- CYBER INCIDENT RESPONSE

(SERVIÇO DE GESTÃO DE INCIDENTES DE SEGURANÇA E CIBERSEGURANÇA)

CYBER EFFECT - NÍVEL 2 - PROATIVO



DESCRIÇÃO



Este serviço garante uma capacidade em tempo real, a identificação/deteção, contenção, remediação e recuperação de incidentes de segurança que ocorram na organização. O serviço permite uma resposta eficaz e eficiente, atuando no imediato face à ocorrência de problemas de segurança detetados e/ou reportados na organização, garantindo um acompanhamento adequado do incidente de segurança.



PROPOSTA DE VALOR

Este serviço fornece um tratamento centralizado dos incidentes de segurança. A gestão experiente, eficaz e eficiente dos incidentes identificados através da nossa framework de ferramentas customizadas, assegurando o tratamento correto e garantindo uma monitorização do ciclo de vida do incidente, aliado a uma capacidade de integrar no incidente informação coletada a partir de fontes externas (MITRE, CERTs, fabricantes, ...), aumenta a eficácia e produtividade global da organização.



CARACTERÍSTICAS DO SERVIÇO

O serviço é composto por:

- ▶ Triagem dos Incidentes;
- ▶ Correlação de Eventos;
- ▶ Tratamento e Resposta a Incidentes;
- ▶ Alerta, Comunicação e Suporte na Recuperação;
- ▶ Análise e Acompanhamento dos Incidentes;



H- CYBER INCIDENT RESPONSE

(SERVIÇO DE GESTÃO DE INCIDENTES DE SEGURANÇA E CIBERSEGURANÇA)

CYBER EFFECT - NÍVEL 2 - PROATIVO

- ▶ Monitorização, Avaliação e Recuperação de Incidentes de Segurança ao nível de comunicações e sistemas de informação;
- ▶ Possui capacidades para deteção de malware conhecido e zero-day/zero-hour, ir além dos alertas individuais para identificar e priorizar potenciais incidentes, possuindo funcionalidades ao nível de IA, para acelerar os processos de investigação.

É instalado o core de funcionamento através do SIEM, que pode ser on-prem & cloud, com escalabilidade e menor TCO.

O nosso serviço fornece um conjunto de ferramentas, soluções e recursos para automatizar vários processos, e/ou para fornecer aos nossos clientes as ferramentas necessárias para encontrar e resolver falhas de segurança.



VALOR ACRESCENTADO

- » A Hardsecure possui uma framework, que integra Inteligência de Ameaças, SIEM, Análise de Malware, Segurança de Redes, CTI (Cyber Threat Intelligence), sistema de ticketing, File Integrity Management (FIM) segurança de endpoints (Endpoint Detection and Response). Esta framework faz parte de um processo que realiza investigação, procura de ameaças, deteção, triagem, gestão de incidentes, resposta, documentação e relatórios, com KPIs aplicados para cada incidente.
- » Integramos na nossa framework: CTI (Cyber Threat Intelligence) e Pentest as a Service (interno e externo), onde todas as vulnerabilidades são validadas de modo a evitar falsos positivos.
- » Podemos integrar serviços de Gestão de Incidentes de Segurança com Serviços de Gestão de Cibersegurança, a fim de realizar consultoria para apoiar os nossos clientes em:
 - Identificar vulnerabilidades e suporte para as mitigar/bloquear;
 - Awareness e formação a todos os utilizadores;
 - Mitigar & bloquear ataques, com base nos incidentes de segurança, no menor tempo possível (sempre em coordenação com a equipa de TI & segurança da organização).



H- CYBER INCIDENT RESPONSE

(SERVIÇO DE GESTÃO DE INCIDENTES DE SEGURANÇA E CIBERSEGURANÇA)

CYBER EFFECT - NÍVEL 2 - PROATIVO



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 Gestão de Incidentes de Segurança e 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”)

