



Cyberdefence Security Operations Center SOC as a Service

No contexto actual em que cada organização é cada vez mais digital, e em que a informação é considerada um dos activos mais valiosos, assistimos a um preocupante aumento de ciberataques que colocam em risco os colaboradores, o negócio e a reputação das marcas.

A conformidade com os novos regulamentos, as directivas e a legislação decorrente, a escassez de recursos especializados em cibersegurança, aliados aos investimentos avultados por estes exigidos, fazem com que as organizações reconheçam ser um grande desafio proteger o seu negócio sem apoio especializado.

A Claranet Security, através do seu Security Operation Center nacional (SOC) 24X7, conta com uma equipa de especialistas em cibersegurança que, actuando como uma extensão das suas equipas técnicas, fornece os recursos, o *know-how* e a cobertura necessários para aumentar a postura de cibersegurança e a resiliência contra estas novas ciberameaças.

CLARANET SECURITY OPERATIONS CENTRE



Os serviços oferecidos pelo SOC 24X7 englobam:

Detecção de tentativas de intrusão e outros eventos de segurança relevantes através da integração da monitorização dos activos e informação de *Threat Intelligence* em plataformas *Security Information and Event Management* (SIEM).

Gestão de soluções de segurança, incluindo Anti-virus inteligentes, *Firewalls* comportamentais, DNS *Firewalls*, soluções avançadas de *sandboxing*, entre outras soluções de prevenção e detecção de nova geração.

Gestão de vulnerabilidades, através da coordenação das fases do ciclo de vida das vulnerabilidades, desde a sua identificação até gestão da implementação de actualizações e patches e outras actividades de mitigação.

Monitorização contínua e detecção de ciberameaças em novos espaços de risco, como a web e *deep & dark web*, detecção de *data breaches* - incluindo credenciais expostas, perfis falsos de executivos, cópias de sites para *phishing*, abuso de marca, entre outros.

O Claranet SOC fornece um serviço especializado *end-to-end*, desde a monitorização contínua a activos enriquecida com informação de *Threat Intelligence*, até à análise forense decorrente durante e após a resolução dos incidentes de segurança.



Proactive protection



Early detection



Immediate response

O serviço é prestado num ciclo bem determinado e permitindo, a todo o momento, garantir o mais célere encaminhamento da informação necessária e enriquecida por forma a levar à rápida resolução ou mitigação dos incidentes de segurança.

Porquê a Claranet?

- Membro da Rede Nacional de CSIRTs (*Computer Security Incident Response Team*) desde 2009
- Colaboração activa com organizações de referência como o APWG.eu Anti-phishing Working Group, e o projecto "No More Ransom" da Europol European CyberCrime Center (EC3).
- Nos últimos 5 anos, membros da equipa da Claranet trabalharam com CERTs (*Computer Emergency Response Teams*) nacionais de dezenas de países, facilitando a agilidade necessária em processos de takedown.

A Claranet em números

- Fundada em 1996
- 360M€ de facturação anual
- Mais de 6.500 Clientes empresariais
- Operações em 8 países
- Mais de 1.800 colaboradores em 24 escritórios
- 43 Datacenters na Europa, dos quais 5 em Portugal
- Microsoft Cloud OS Partner of the Year 2014 e 2015
- Líder no Quadrante Mágico da Gartner de Managed Hybrid Cloud Hosting