Jolera®

Your Partner in IT

Grupo MICROSEGUR

Dream the future, we protect the present

Quem é a Jolera?

A Jolera desenvolve soluções geridas de TI.
Oferecemos soluções chave-na-mão de próxima geração, permitindo aos nossos parceiros criar experiências de topo para os seus clientes.

Grupo MICROSEGUR
Dream the future. we protect the present

Jolera®
Your Partner in IT

O que fazemos

Competências globais e portefólio completo

ESTRATÉGIA TI

Planeamento e mapeamento do TI da empresa, e serviço de vCIO.

ARMAZENAMENTO FÍSICO E NA CLOUD

Avaliação, design, gestão e suporte a migrações para a Cloud.

REDE / INFRAESTRUTURA / SEGURANÇA

Avaliação, desenvolvimento, implementação, gestão e suporte à integração SOC/SIEM líder de mercado.

GESTÃO DE SISTEMAS

NSOC (Network And Security Operations Center) disponível 24/7/365, fornecendo patching e suporte à gestão de sistemas.

USER SUPPORT

Service Desk multilingua disponível 24/7/365, com mais de 200 profissionais de apoio nos 3 Tiers.

Grupo MICROSEGUR Dream the future. we protect the present

Jolera

REDUZA CUSTOS

CUSTO MÉDIO DE VIOLAÇÃO DE DADOS EM 2022: O MAIOR DE SEMPRE

€4.24M

Source: IBM Security - Cost of a Data Breach Report 2022

Grupo MICROSEGUR
Dream the future. we protect the present

Jolera

PERMANEÇA PROTEGIDO

83%

DAS EMPRESAS SOFRERAM MAIS DO QUE UMA VIOLAÇÃO DE DADOS

Source: IBM Security - Cost of a Data Breach Report 2022

Grupo MICROSEGUR
Dream the future, we protect the present

Jolera®
Your Partner in IT

MENOS PREOCUPAÇÕES

68%

DOS CEOs SENTEM QUE AS AMEAÇAS À CIBERSEGURANÇA ESTÃO A AUMENTAR

POUPE TEMPO

277 DIAS

TEMPO MÉDIO PARA INDENTIFICAR E CONTER UMA VIOLAÇÃO

Source: IBM Security - Cost of a Data Breach Report 2022

Grupo MICROSEGUR
Dream the future, we protect the present

Jolera®
Your Partner in IT

Secure IT

Plataforma de Segurança Completa

Grupo MICROSEGUR Dream the future we protect the present

Jolera

SEGURANÇA DE FIREWALL

- Serviços geridos e implementação de firewall.
- Conectividade site-a-site otimizada, regras específicas de aplicação.
- Recursos integrados de SD-Wan e administração central de operações de rede/segurança para sua empresa.
- O Centro de Operações de Segurança (SOC) concentra-se na monitorização 24/7/365 de tendências e na remediação/resposta ativa para os respectivos alertas.

RESPOSTA DA DETEÇÃO DE VULNERABILIDADE (VDR)

- Serviço gerido para monitorizar ativos do sistema e gerar relatórios sobre seu estado de vulnerabilidade.
- Estes relatórios fornecem os passos recomendados de acordo com a gravidade.

DETEÇÃO E RESPOSTA DE ENDPOINT (EDR)

- Agentes autónomos para Windows, Mac, Linux e Kubernetes.
- Suporte para dispositivos físicos, virtuais, VDI, data centers de clientes, data centers híbridos e fornecedores de serviços em nuvem.
- A equipe do Centro de Operações de Segurança (SOC) concentra-se em lidar com incidentes de segurança e monitoriza os seus endpoints 24/7/365, corrigindo os seus respectivos alertas.

VULNERABILITY ASSESSMENT

- Revisão única dos ativos do sistema.
- Fornece um relatório detalhando o estado de segurança com recomendações para atender às melhores práticas.
-

EMAIL

- Segurança de E-mail (de entrada e saída: anti-spam, anti-vírus, anti-malware, e-mails anti-phishing, e-mails não entregues, e-mails não seguros)
- Backup de E-mail (Exchange Online, SharePoint Online e OneDrive for Business).
- Arquivamento de E-mail

SIEM

- The Security Information and Event Management (SIEM) recolhe dados dos dispositivos e aplicações dentro da sua rede e comunica com as ferramentas de segurança existentes.
- Correlaciona o comportamento data e reconhece comportamento incomum de vários pontos da sua infraestrutura de TI e notifica as nossas equipas de segurança e operações de rede para reparação.
- Security Operations Center (SOC) centra-se na monitorização 24/7/365 e na resposta remediada/ativa para os respetivos alertas.

SECURITY BASELINE ASSESSMENT (SBA)

- Analise a postura de segurança de uma organização, incluindo endpoints, utilizadores e políticas.
- Fornecer um relatório detalhando o estado de segurança com recomendações para atender às melhores práticas.

DEFESA DO UTILIZADOR

- Teste de phishing para funcionários.
- Recursos para formação e aprendizagem.

SWITCH

- Serviços Geridos & Switch Collocation.
- Melhor conectividade site-to-site, regras específicas da aplicação.
- Capacidades SD-Wan incorporadas e administração central de operações de rede/segurança para o seu negócio.
- Network Operations Center (NOC) centra-se na monitorização 24/7/365 e na resposta remediada/ativa para os respetivos alertas.

PENETRATION TESTING

- Avaliações altamente direcionadas de ativos específicos.
- Ajuda a satisfazer as necessidades da política de segurança, tais como regulamentos do setor.

Centro de Operações de Rede (NOC)

SKU Rápido

Serviço On-Demand

Centro de Operações de Segurança (SOC)

Serviços Geridos

24 horas/dia, 7 dias/semana, 365 dias/ano

SECURE IT™

DETEÇÃO E RESPOSTA ESTENDIDA (XDR)

VISIBILIDADE CONTÍNUA DE AMEAÇAS COM DETEÇÃO E RESPOSTA EM TEMPO REAL

PLATAFORMA INTEGRADA DE DETEÇÃO E RESPOSTA

A nossa plataforma XDR é totalmente gerida e integrada com produtos de segurança líderes do setor, serviços e feeds de dados sobre ameaça, para garantir a proteção dos ambientes pelos melhores.

VERDADEIRA DETEÇÃO E RESPOSTA

Uma verdadeira supervisão de investigação por especialistas em cibersegurança, que analisam dados de ameaças em tempo real através do nosso Centro Global de Resposta a Informação – GIRC.

IA ADAPTÁVEL AVANÇADA + MACHINE LEARNING

Equipar cada dispositivo e carga de trabalho - não importa a sua localização ou conectividade - para responder de forma inteligente contra ameaças cibernéticas com AI e Machine Learning.

THREAT INTELLIGENCE E REMEDIAÇÃO GUIADA

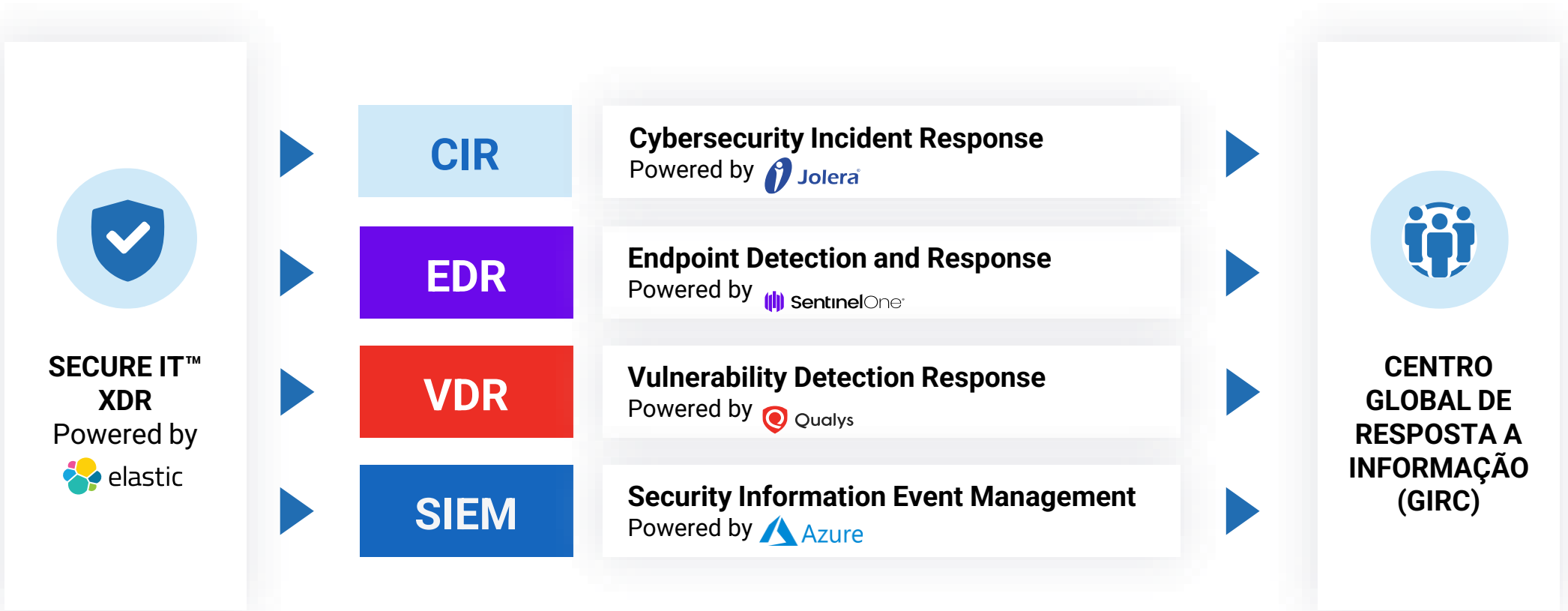
Visibilidade completa da sua superfície de ciberataque com Threat Intelligence, para responder e parar ameaças com a nossa equipa global de especialistas em deteção de ameaças cibernéticas.

Grupo MICROSEGUR Dream the future. we protect the present

Jolera

Plataforma Secure IT™ XDR

Os componentes da nossa plataforma de deteção e resposta alargada são compostos por líderes globais da indústria em cada disciplina de segurança.



NEW: Secure IT™ XDR

elastic

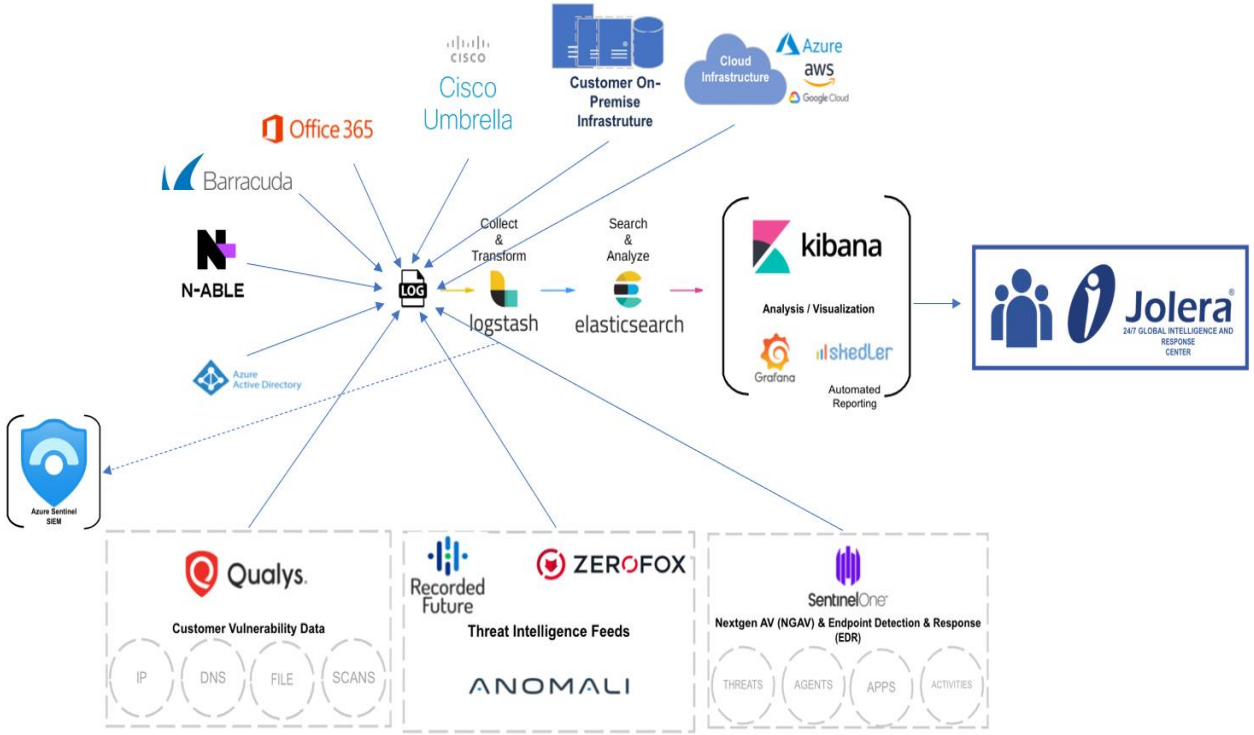
O que é Deteção e Resposta Estendida (XDR)?

Solução proativa para ajudar organizações a prevenir perturbações nas operações comerciais.

Análise de comportamento do utilizador e da entidade (UEBA) melhora a deteção e resposta de ameaças.

Funcionalidades principais da Plataforma:

- Threat Intel and Machine Learning (ML)
- Crescente lista de casos de uso e informação
- Cobertura total em toda infraestrutura de TI
- Monitorização unificada através de relatórios em tempo real.



Grupo MICROSEGUR Dream the future. we protect the present

Jolera

NEW: Secure IT™ XDR

Como pode um cliente beneficiar do Secure IT XDR?

- Permite aos clientes adicionar outra camada de segurança ao seu programa de Cibersegurança.
- Melhorar significativamente o tempo médio para detetar (MTTD) e tempo médio para responder (MTTR) .
- Apoiado pelo nosso Centro Global de Resposta a Informação (GIRC), disponível 24/7/365.
- Cloud native e escalável, permitindo serviços de segurança à escala da nuvem.
- Solução chave-na-mão: Não é necessário comprar hardware ou software para suportar este serviço.
- Proporciona um valor imenso aos clientes que querem alavancar IA e aprendizagem automática para realizar a correlação de eventos em tempo real em toda a sua infraestrutura de T.
- Painel unificado fornece um painel de controlo único para eventos relacionados com a segurança em todos os ativos.

Secure IT™ XDR

Funcionalidades

Secure IT™ XDR Standard e Advanced estão disponíveis para ajudar a sua organização a decidir qual o nível de segurança adequado para uma maior proteção dos ativos das suas propriedades.

SECURE IT – XDR FUNCIONALIDADES E TIERS	STANDARD	ADVANCED
Monitorização sempre disponível (24/7/365)	●	●
Engenheiro de apoio ao vivo à segurança cibernética (24/7/365)	●	●
Allways-on Threat Hunting	●	●
Suporte de contenção e interrupção de ameaças sempre disponível	●	●
I.A. e Machine Learning para detetar/impedir ameaças em segundos	●	●
Deteção rápida e automatizada de anomalias	●	●
Escalável sem a necessidade de comprar hardware ou software	●	●
Deteção de ataques desconhecidos através de analítica comportamental	●	●
Investigações reais e rápidas realizadas por humanos	●	●
Cloud pública e modelos de proteção de ameaças de segurança híbrida	●	●
Escalonamentos detalhados com recomendações de análise e de segurança	●	●
Entregue através de um único painel de controlo através da Jolera SaaS	●	●
Revisões de negócios e planeamento estratégico da melhoria contínua	●	●
Acesso ao Centro Global de Resposta a Informação 24/7	●	●
Plataforma de integração, única e automatizada para uma visibilidade completa	●	●
Resposta a Incidentes Cibernéticos – sem retenção (CIR) *	●	●
Deteção e Resposta de Vulnerabilidade (VDR)	—	●
Deteção e Resposta de Endpoint (EDR)	—	●
Plataforma Secure IT™ Azure Sentinel Accelerator	ADD-ON	ADD-ON

Grupo MICROSEGUR Dream the future. we protect the present

Jolera®

Secure IT™

Processo de adoção de uma framework baseada na Lei 65

OBJETIVO	DESCRIÇÃO
Identificar	Compreensão do contexto da organização, dos ativos que suportam os processos críticos da atividade da organização e dos riscos associados relevantes. Esta compreensão permite à organização definir e priorizar os seus recursos e investimentos, de acordo com os seus objetivos gerais e com a sua estratégia de gestão de risco.
Proteger	Implementação de medidas destinadas a proteger os processos e ativos da organização, independentemente da sua natureza tecnológica. Assim, nesta categoria, são definidas medidas orientadas à proteção da organização nas suas três dimensões: Pessoas, Processos e Tecnologia.
Detetar	Definição e implementação de medidas destinadas a identificar, de forma atempada, os incidentes. Ou seja, a deteção de eventos com um efeito adverso real na segurança das redes e dos sistemas de informação.
Responder	Definição e implementação de medidas de ação apropriadas, em caso de deteção de um incidente. As medidas propostas no âmbito deste objetivo pretendem mitigar o impacto do incidente, ou seja, reduzir os seus potenciais efeitos adversos.
Recuperar	Definição e implementação de atividades, que visam a gestão de planos e medidas de recuperação dos processos e serviços afetados por um incidente de cibersegurança. As medidas pertencentes a este objetivo pretendem assegurar a resiliência da organização nas suas dimensões: Pessoas, Processos e Tecnologia. Assim, no caso de existência de um incidente, a organização tem a capacidade de utilizar as medidas para suporte à recuperação em tempo útil da sua atividade.

Constrangimentos de Mercado

Porque é que as empresas (PMEs e GEs) têm dificuldades/deficiências na implementação de segurança interna?

- Escassez de profissionais qualificados em segurança.
- Especialização elevada dentro da própria área TI.
- Desconhecimento da abrangência do Attack Surface.
- SOC/NOC são dispendiosos.
- Ausência de Framework de Segurança.

Oportunidades

- **Observância da Lei 65**

  - **Público-Alvo:** Operadores de infraestruturas críticas, serviços essenciais dos setores da energia, transportes, banca, infraestruturas do mercado financeiro, saúde, fornecimento e distribuição de agua potável e infraestruturas digitais e prestadores de serviços digitais, assim como as entidades da Administração Pública.
  - **Requisitos:**
    - Avaliação de toda a infraestrutura.
    - Plano de segurança.
    - Análise de risco.
    - Apresentação de relatórios periódicos de segurança.
    - Notificação de incidentes à CNCS.

Consultoria de Segurança

GESTÃO DE VULNERABILIDADES
Gestão proativa para mitigar vulnerabilidades e prevenir explorações.

SCAN DE CONFORMIDADES
Avaliar a adesão às normas políticas definidas e aos quadros de conformidade.

PLANO DE MITIGAÇÃO
Um plano de ação passo a passo com atividades de mitigação detalhadas.

GESTÃO DE PATCHES
Inclui testar e instalar vários patches em sistemas informáticos.

REMEDIAÇÃO
Reparação de alertas de segurança ou problemas pelas nossas equipas de segurança especializadas.

CONSULTA DE CONFORMIDADE
Apoio na implementação de estratégias de conformidade nas políticas empresariais.

Contactos

Grupo MICROSEGUR
Dream the future, we protect the present

Lisboa - Portugal
Rua Reinaldo Ferreira, 48 A
1700-324 Alvalade

Porto - Portugal
Av. Manuel Violas, 476
4410-137, V. N. de Gaia

Luanda – Angola
Rua do Anselmo, 1Q nª 3
Sector F
Morro Bento I – Mun. Da Samba

Jolera®

Europa

Avenida da Boavista, 2099

4100-134 Porto, Portugal

América do Norte

365 Bloor Street East, Suite 200

Toronto, Ontario, Canada M4W 3L4

Jolera®

Your Partner in IT

Grupo MICROSEGUR

Dream the future, we protect the present