Emas Security Operations Manager

Um passo à frente de um SIEM

Aspetos destacáveis

- **Proporciona capacidades de análise em tempo real**
- **Incrementa a agilidade das organizações**
- **Fomenta a colaboração interdepartamental**
- **Ajuda a homogeneizar a atenção aos clientes**
- **Simplifica a interação com os sistemas**
- **Agrupa efeitos e localiza as causas**
- **Permite reduzir os tempos de resposta**
- **Melhora a rastreabilidade das ações**
- **Oferece suporte aos sistemas de gestão**
- **Prioriza a atenção dos utilizadores**

Mediante um ambiente plenamente integrado o **emas Security Operations Manager**, articula-se em redor a uma CMDB (ISO 20000 ou ITIL compliant) que dispõe de capacidades de monitorização de segurança e recolha.

Dispõe de uma orientação flexível para a vigilância do mundo IP, incluindo Internet das coisas (IoT) e o mundo OT em geral, incorporando inteligência avançada mediante a utilização de técnicas de correlação complexa de eventos ou análise de padrões para a identificação de anomalias.

Adicionalmente, permite a gestão dos processos ligados ao Serviço, incluindo o processo de gestão de incidentes (Incident Handling), da Qualidade de Serviço, da configuração ou da gestão de conhecimento.

Detete a presença de indicadores chave de padrões de ataque

Priorize a atuação para agilizar a resposta a ameaças

Relacione informação de diferentes origens para enriquecer os dados

Administre a sua informação de forma centralizada

O que é e como funciona?

O **emas SOM** está composto por um conjunto de módulos que proporcionam as funcionalidades de operação integral do centro de serviços:

O **argos** é o módulo de monitorização e recolha de eventos de Segurança, a sua missão é a monitorização da segurança em âmbito tanto de IT como de OT, assim como a recolha, modelação e centralização dos registos de atividade dos mesmos (logs) para a sua posterior análise, incluindo capacidades de análise forense. A partir da informação que recolhe, o argos proporciona um potente módulo de visualização de dados, que permite uma análise visual pormenorizada das diferentes origens de dados (IDS, Firewalls, registos DNS, DHCP, redes sociais, emails, etc.).

O **tritón** é o módulo de inteligência que, mediante a utilização de técnicas de correlação complexa de eventos, serve como base para o desenvolvimento e parametrização de correlacionadores de eventos especializados, e sua aplicação em diferentes domínios da deteção e proteção. O Tritón dispõe de um potente conjunto de regras de correlação pré desenhadas que podem ser ajustadas e estendidas para adaptarem-se às particularidades de determinado ambiente e das ameaças do organismo que protege, mediante uma linguagem próxima ao interlocutor (DSL). A inteligência proporcionada pelo Tritón, não só facilita a deteção de ameaças complexas como também permite a automatização parcial do processo de remediação, lançando ordens de ações sobre o ambiente (bloqueio de IPs, ordens ao NAC, etc).

O **carmen** é o módulo de Advanced Threat Protection cujo objetivo é suportar o processo de investigação (Threat Hunting) para a identificação de comprometimentos por APTs. Exerce um mecanismo de proteção na deteção na fase de intrusão (Breach Detection) aplicando técnicas avançadas de Sandboxing ao tráfego de entrada.

Por outro lado, considerando que a organização já tenha sido comprometida, o carmen focaliza-se na adquisição, processamento e análise de trafego de saída da rede em protocolos como HTTP, DNS ou SMTP (os mais habituais para este tipo de comunicações), assim como, mecanismos habituais para a aquisição de persistência no roubo de informação na rede corporativa (psexec, rdp, named pipes…)

O **emas** é o módulo de Gestão do Serviço e atua como núcleo de gestão da plataforma sendo a consola que recolhe todas as incidências ou alertas automáticos gerados pelo sistema de correlação ou manuais cujo origem seja o processo de suporte a utilizadores. O emas suporta a gestão do ciclo de vida do incidente (Incident Handling) desde a sua criação até a sua resolução apoiando-se por uma base de dados de activos (CMDB) que recolhe os activos a proteger, e numa definição do catálogo de serviços de suporte para assegurar uma resposta procedimentada.

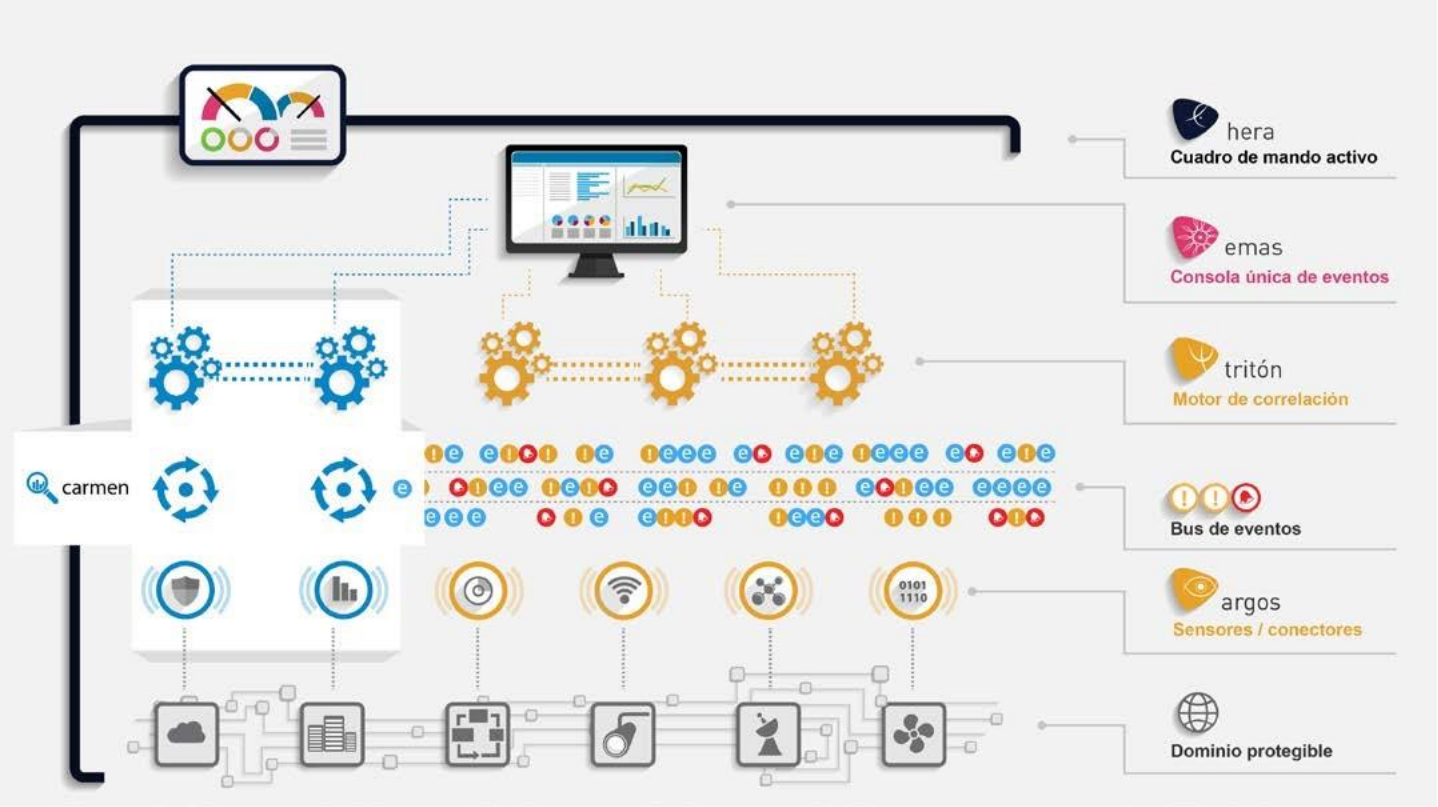
A gestão dos incidentes é realizada vigiando os objetivos de Acordos de Níveis de Serviço (SLA) apoiando-se numa base de dados de conhecimento que é retroalimentada.

O **hera** é o módulo de Dashboarding que oferece distintas visões da evolução do serviço prestado: por um lado oferece a visão interna, tanto em tempo real, como históricos dos indicadores chave de eficiência, eficácia, risco e carga do sistema. Por outro, é capaz de exportar aos seus clientes um quadro de comando personalizado que lhes permite seguir, em tempo real, a evolução do serviço prestado.

Funcionalidades

- Centralização e análise de Logs
- Análise de Vulnerabilidades
- Deteção de intrusões (Network IDS)
- Controlo da integridade de ficheiros (Host IDS)
- Autodescoberta de activos
- Monitorização de disponibilidade sistemas e aplicações
- Monitorização da rede
- Correlação de eventos
- Gestão de eventos
- Multiplicidade de Relatórios

Arquitetura



O volume da informação que deve processar qualquer organização hoje em dia é impossível gerir sem uma ferramenta que ajude a sua recolha, normalização, armazenamento, análise e correlação, que leve a uma redução muito significativa do volume de informação a tratar finalmente pelo pessoal técnico.

O emas-Security Operations Manager suporta um modelo de processamento baseado na análise e extração da Tras realizar uma identificação das fontes de informação, argos realiza uma seleção da informação relevante suscetível de ser analisada. Posteriormente realiza-se a análise e correlação, em o tritón aplica a sua inteligência e c

O carmen realiza uma análise automática e manual. Após isso produz-se a ação, derivada da gestão dos alertas que produzem-se na consola de gestão (emas).

Por último, o módulo de Dashboarding (hera) proporciona informação mediante indicadores específicos de segurança.

Tem a capacidade de funcionar com um modelo clássico centralizado, no qual existe uma ou várias sondas que recolhem informação e um nó central que armazena os registos, e sobre este volume total de informação, realiza-se a atividade de correlação.

Adicionalmente, pode suportar um modelo de correlação distribuído, em que os eventos podem ser recolhidos e correlacionados na origem, descarregando assim posteriormente ao nó central, e realizando neste, uma correlação de segundo nível, utilizando apenas alertas previamente correlacionados para identificar ameaças que afetem de forma coordenada a várias fontes.

Solicite-nos uma demonstração

Para saber mais sobre como o **emas SOM** pode ajudar a proteger a sua organização, ou solicitar uma demo, contacte-nos.

+351 21 7923729
info@s2grupo.com
www.s2grupo.com

Antecipando um mundo
ciberseguro

S2 GRUPO