Como configurar seu SOC visando o sucesso

Pensando em configurar ou reconfigurar seu centro de operações de segurança (SOC) para eficiência ideal?

Um SOC bem projetado é fundamental para proteger sua organização contra ameaças emergentes de segurança física e cibernética. Aqui, dividimos as principais considerações em sete categorias essenciais: configuração, colaboração, contexto, clareza, coordenação, compliance e cybersecurity.

Configuração: Amplie alcance e flexibilidade

- **Otimize o layout do hub**: Organize o SOC, criando espaços de trabalho colaborativos e otimizando a visibilidade do monitor.
- **Evite janelas**: A sala deve ser sem janelas e com acesso limitado para garantir a segurança e minimizar distrações.
- **Considere sua infraestrutura de TI**: Que tipo de infraestrutura de TI você possui? In loco, na nuvem ou híbrido? Como isso afeta a eficiência do seu SOC?

Colaboração: aprimore o trabalho em equipe dentro e fora do seu SOC

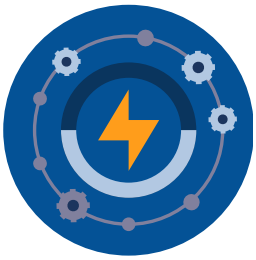
- **Instale paredes de vídeo**: implemente paredes de vídeo para exibir feeds em tempo real e melhorar a visibilidade geral.
- **Invista em ferramentas de comunicação**: Use ferramentas de gerenciamento de comunicação SIP, como o Sipelia™, para transmitir informações e comunicar-se com outras pessoas.
- **Configure um endereço de e-mail dedicado**: Melhore as comunicações com e-mail dedicado para todas as solicitações.
- **Despache e atribua tarefas**: Considere a implementação de sistemas colaborativos de gerenciamento de decisões, como o Mission Control™, para uma atribuição eficiente de tarefas.

Contexto: obtenha uma visão unificada

- **Aproveite recursos avançados de mapeamento**: Utilize ferramentas de mapeamento em seu SOC para visualizar e compreender facilmente eventos em todas as instalações.
- **Conecte dispositivos IIoT**: Melhore a consciência contextual conectando dispositivos IIoT e agregando dados em uma única plataforma unificada.
- **Adicione janelas do navegador aos painéis**: Integre feeds de notícias e atualizações de mídia social para eventos externos.

Clareza: digitalize informações para obter insights acionáveis

- **Crie regras**: Estabeleça regras fáceis de usar que eliminem alarmes falsos e reduzam a sobrecarga do operador.
- **Automatize tarefas**: crie fluxos de trabalho automatizados que os operadores possam seguir durante momentos críticos para garantir que as notificações sejam tratadas de acordo com os procedimentos de segurança visando compliance.
- **Filtre dados**: Ferramentas de automação para filtrar dados, permitindo resolver rapidamente possíveis ameaças.



Coordenação: Escale e responda a eventos de forma eficiente

- **Configure procedimentos operacionais dinâmicos**: Introduza procedimentos operacionais dinâmicos com o Mission Control para respostas customizadas às diferentes fases do incidente.
- **Considere direitos de escalonamento para workstation**: atribua direitos de escalonamento baseados em workstation para providências mais rápidas e eficientes durante emergências.

Compliance: Cumpra as regulamentações

- **Atribua privilégios de usuário**: Ajuste os privilégios do usuário para garantir compliance regulatório.
- **Configure relatórios**: Facilite investigações forenses através da elaboração de relatórios abrangentes de incidentes.

Cybersecurity: fique à frente das ameaças

- **Automatize atualizações de manutenção**: configure tarefas automatizadas para receber notificações com atualizações de manutenção do dispositivo e status de integridade do sistema.
- **Mantenha uma trilha de auditoria**: Escolha um software que facilite a exportação em formato nativo e o compartilhamento de arquivos, mantendo junto uma trilha de auditoria robusta.

Otimize seu centro de operações de segurança com a ajuda de um sistema colaborativo de gerenciamento de decisão

Saiba mais sobre o Mission Control

Genetec Inc.
genetec.com/br
info@genetec.com
@genetec

ATUALIZADO: 12-03-2024