Sistema de Comunicação Crítica

Problema

Os sistemas críticos têm muito emprego na área de defesa e sempre exigiram características como robustez, interoperabilidade e flexibilidade. Nestes sistemas, as questões relativas à segurança cibernética requerem vigilância constante e investimento em tecnologias e práticas de segurança de última geração, de forma a garantir a integridade, confidencialidade e disponibilidade destes sistemas.

Tais sistemas são considerados sensíveis, pois uma falha leva, inevitavelmente, ao não cumprimento do objetivo de uma determinada missão. O sistema deve ser confiável, ou seja, a confiança dos usuários têm de que o sistema não irá falhar. Destacam-se quatro importantes dimensões para o estabelecimento da confiança, que são:

- **Disponibilidade**, pode ser utilizado a todo momento.
- **Confiabilidade**, fornece todos os serviços esperados.
- **Segurança**, seguro com disponibilidade, integridade, confiabilidade e autenticação.
- **Proteção**, não permite que ocorra invasão acidental e/ou intencional.

Sistema Crítico de comunicação, alvo de ataques cibernéticos

Monitoramento sistema crítico

Para a implantação de um sistema crítico, com função principal de viabilizar a comunicação entre vários outros sistemas, a capacidade de segurança cibernética é fundamental. A ausência de uma solução robusta e escalável de cibersegurança, integrada a um ambiente de gestão de segurança, por exemplo, um Centro de Operações de Segurança (SOC), eleva sensivelmente o risco de que as ameaças cibernéticas sejam bem sucedidas. Os prejuízos, em decorrência do sucesso das ameaças, podem ser financeiros, técnicos, ambientais e até perda da vida humana.

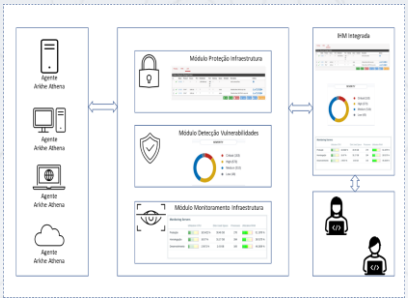
Solução

O uso do Arkhe Athena como solução de cibersegurança, integrada ao Centro de Operações de Segurança (SOC), possibilita o estabelecimento de um alto nível de proteção da infraestrutura do ambiente em que o novo sistema de comunicação crítica é implementado. Os recursos disponíveis no Athena promovem proteção sólida e avançada contra acessos não autorizados. Utilizando uma arquitetura com o Athena integrado ao Centro de Operações de Segurança (SOC), o analista de segurança tem as condições técnicas para responder de forma imediata aos possíveis incidentes e ameaças cibernéticas. O Athena oferece capacidades e recursos avançados de monitoramento e uma visibilidade detalhada da infraestrutura, tudo em tempo real. Isso permite que os analistas de segurança acompanhem o estado e o desempenho do ambiente de forma eficaz, condição importante para possibilitar o funcionamento adequado dos sistemas existentes, em especial, o sistema de comunicação crítica. A funcionalidade de monitoração e controle das vulnerabilidades presente no Arkhe Athena, com identificação e propostas de correções, possibilita que o analista realize as atualizações e ajustes necessários, visando diminuir os riscos provenientes das ameaças cibernéticas. Essa capacidade é crucial para garantir o funcionamento adequado de todos os sistemas, especialmente o sistema de comunicação crítica.

Benefícios

A integração do Arkhe Athena com Centros de Operações de Segurança (SOC) fortalece a capacidade de resposta a incidentes e a coordenação eficaz das ações com os sistemas de segurança. A abordagem modular do Arkhe Athena possibilita fácil e rápida expansão, visando a proteção de futuros projetos e novos sistemas, mantendo a consciência e as práticas de segurança. A visibilidade e monitoramento contínuo da infraestrutura, através do Athena, permite a pronta identificação de anomalias e ameaças. O analista de segurança tem condições de tomar ações de resposta, forma ágil e eficiente. Ao implementar as medidas proativas para a proteção do sistema de comunicação crítica, os riscos de comprometimento da segurança são minimizados, proporcionando uma melhoria na resiliência cibernética.

Arkhe Athena, capacidade de resposta a incidentes



Monitoramento contínuo, integrado e escalável

contato@atech.com.br | Tel.: 55 (11) 3103-4600
Rua do Rocio, 313 - 5° andar
Vila Olímpia - São Paulo - SP