SIEM
SECURITY INFORMATION AND EVENT MANAGEMENT

Erivan M. da Silva

Trainner de Segurança da Informação

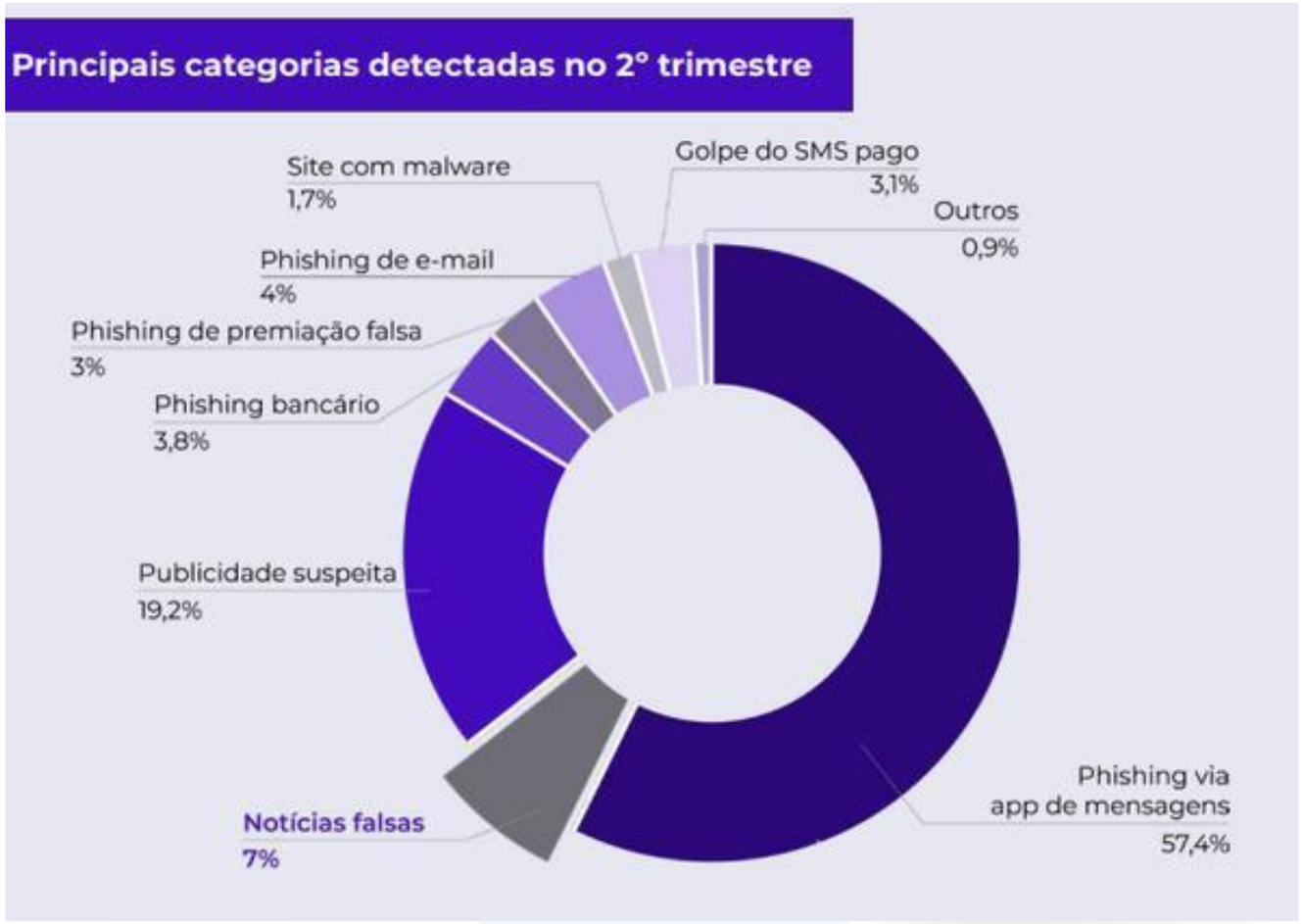
Conformidade com a LGPD

QUAIS SÃO AS CONSEQUÊNCIAS DO VAZAMENTO DE DADOS?

- Gera penalidades ligadas à LGPD;
- Compromete a imagem da empresa;
- Interrompe os seus serviços; e
- Provoca a redução dos lucros;

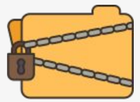
"No mundo da segurança cibernética, a última coisa que você quer é ter um alvo pintado em você."

TIM COOK



https://canaltech.com.br/seguranca/numero-de-ataques-cibernetico s-no-brasil-quase-que-dobrou-em-2018-119600/

PONTOS PARA DISCUSSÃO:

- Confidencialidade 
- Integridade 
- Disponibilidade 

A segurança da informação ajuda a proteger a reputação da empresa.

Conheça a solução

WAZUH!

SIEM: SEGURANÇA DA INFORMAÇÃO E GESTÃO DE EVENTOS.

PaulOOctavio

SIEM WAZUH.

QUAL BENEFÍCIO DE UM SIEM PARA A ORGANIZAÇÃO?

Análise de dados

captura os log e faz uma análise minuciosa.

Monitoramento

E capaz de monitorar a integridade de arquivos.

Detecção de intrusão

Fornece automatizadamente resposta a intrusão.

EM COMPLIANCE COM

PCI DSS, NIST 800-53,GDPR

Segurança de Terminais

Avaliação de Configuração, Detecção e Respostas de incidentes e Monitoramento de integridade de arquivo

Inteligência contra ameaças

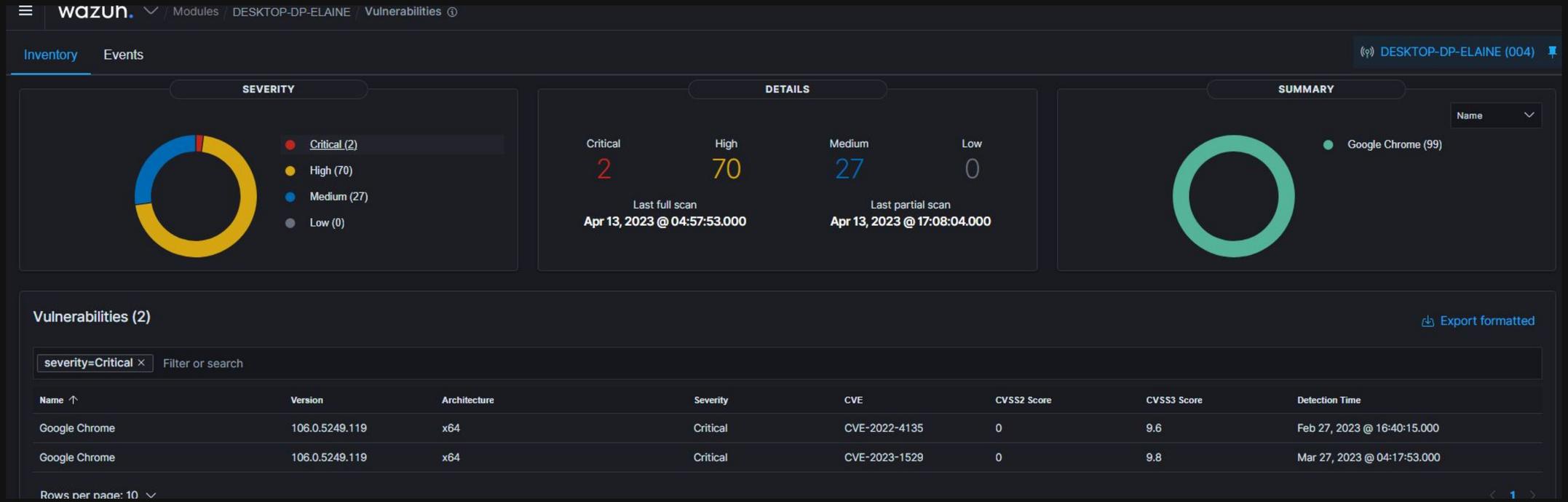
Caça de Ameaças, Higiene de T.I e detecção de vulnerabilidades

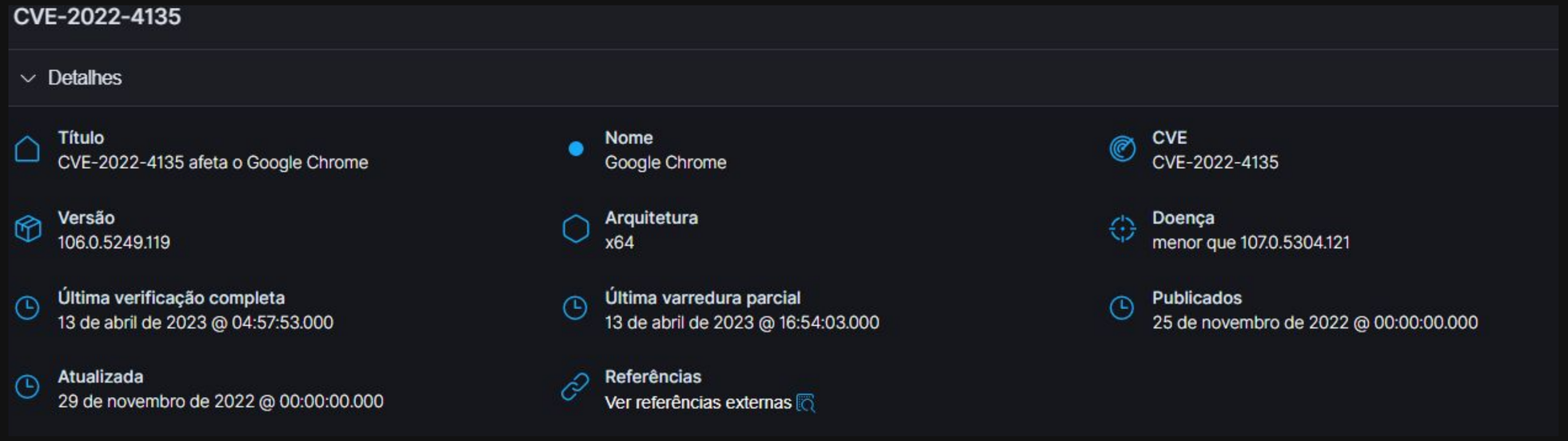
Operações de Segurança

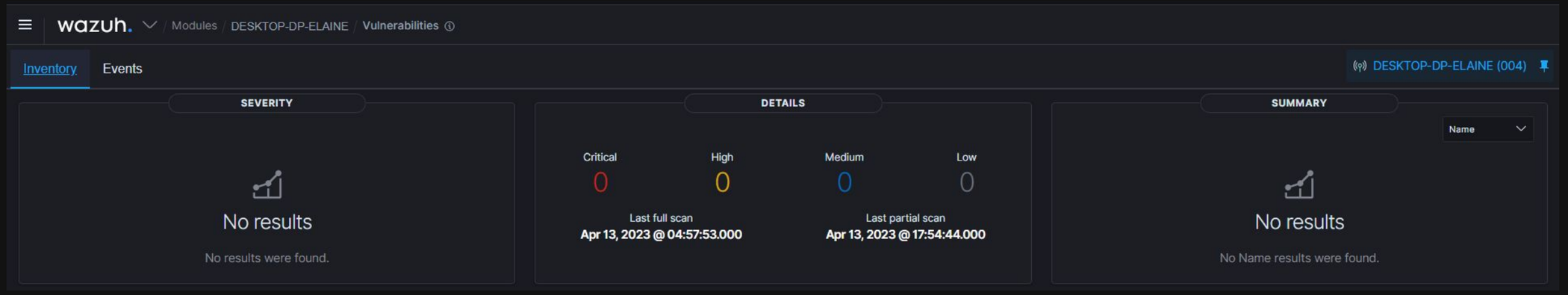
Autoridade, Compliance e Conformidade, Análise de Dados e Registros e Detecção de Malware

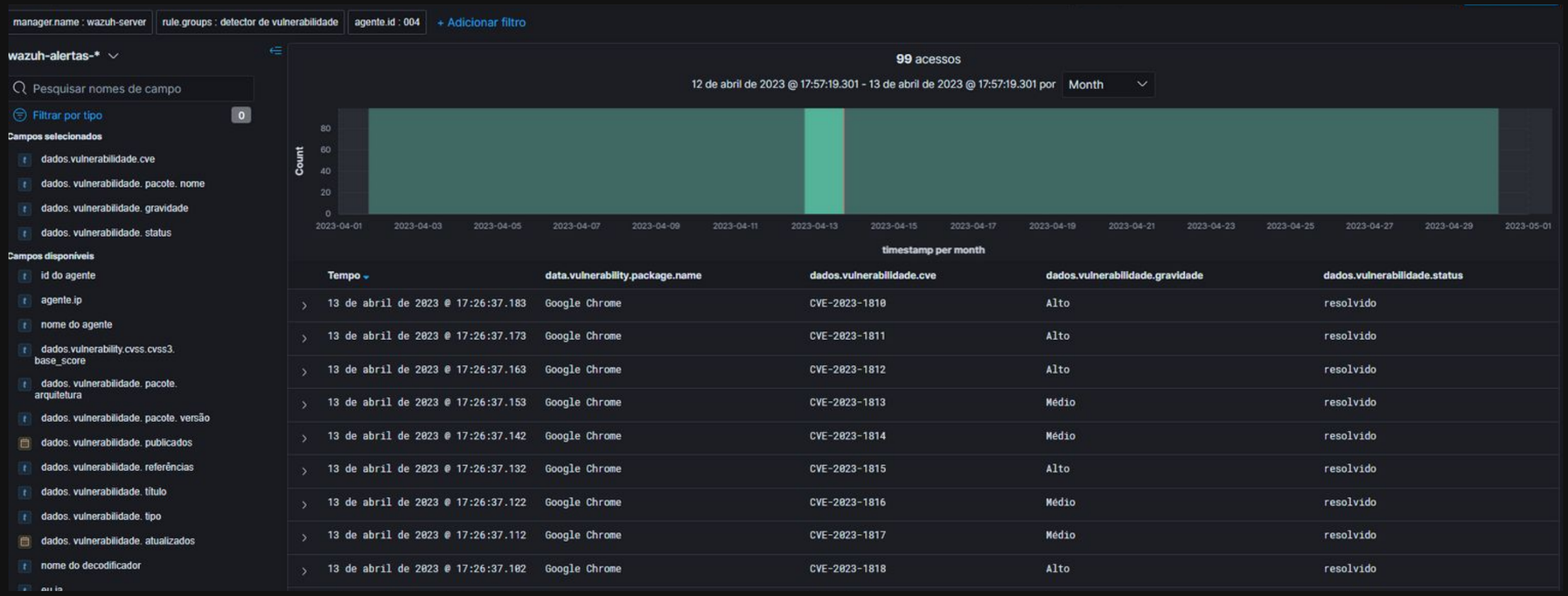
Melhor Custo-Benefício

Solução open source based, você só paga pelos recursos utilizados em Cloud


wazuh.
Modules / DESKTOP-DP-ELAINE / Vulnerabilities
Inventory
Events
DESKTOP-DP-ELAINE (004)
SEVERITY
Critical (2)
High (70)
Medium (27)
Low (0)
DETAILS
Critical
2
High
70
Medium
27
Low
0
Last full scan
Apr 13, 2023 @ 04:57:53.000
Last partial scan
Apr 13, 2023 @ 17:08:04.000
SUMMARY
Name
Google Chrome (99)
Vulnerabilities (2)
Export formatted
severity=Critical
Filter or search
Name
Version
Architecture
Severity
CVE
CVSS2 Score
CVSS3 Score
Detection Time
Google Chrome
106.0.5249.119
x64
Critical
CVE-2022-4135
0
9.6
Feb 27, 2023 @ 16:40:15.000
Google Chrome
106.0.5249.119
x64
Critical
CVE-2023-1529
0
9.8
Mar 27, 2023 @ 04:17:53.000
Rows per page: 10
1


CVE-2022-4135
Detalhes
Título
CVE-2022-4135 afeta o Google Chrome
Nome
Google Chrome
CVE
CVE-2022-4135
Versão
106.0.5249.119
Arquitetura
x64
Doença
menor que 107.0.5304.121
Última verificação completa
13 de abril de 2023 @ 04:57:53.000
Última varredura parcial
13 de abril de 2023 @ 16:54:03.000
Publicados
25 de novembro de 2022 @ 00:00:00.000
Atualizada
29 de novembro de 2022 @ 00:00:00.000
Referências
Ver referências externas


wazuh.
Modules / DESKTOP-DP-ELAINE / Vulnerabilities
Inventory
Events
DESKTOP-DP-ELAINE (004)
SEVERITY
No results
No results were found.
DETAILS
Critical
0
High
0
Medium
0
Low
0
Last full scan
Apr 13, 2023 @ 04:57:53.000
Last partial scan
Apr 13, 2023 @ 17:54:44.000
SUMMARY
Name
No results
No Name results were found.


manager.name : wazuh-server
rule.groups : detector de vulnerabilidade
agente.id : 004
+ Adicionar filtro
wazuh-alertas-*
Pesquisar nomes de campo
Filtrar por tipo
0
Campos selecionados
dados.vulnerabilidade.cve
dados. vulnerabilidade. pacote. nome
dados. vulnerabilidade. gravidade
dados. vulnerabilidade. status
Campos disponíveis
id do agente
agente.ip
nome do agente
dados.vulnerability.cvss.cvss3. base_score
dados. vulnerabilidade. pacote. arquitetura
dados. vulnerabilidade. pacote. versão
dados. vulnerabilidade. publicados
dados. vulnerabilidade. referências
dados. vulnerabilidade. título
dados. vulnerabilidade. tipo
dados. vulnerabilidade. atualizados
nome do decodificador
99 acessos
12 de abril de 2023 @ 17:57:19.301 - 13 de abril de 2023 @ 17:57:19.301 por Month
Count
timestamp per month
Tempo
data.vulnerability.package.name
dados.vulnerabilidade.cve
dados.vulnerabilidade.gravidade
dados.vulnerabilidade.status
13 de abril de 2023 @ 17:26:37.183 Google Chrome CVE-2023-1810 Alto resolvido
13 de abril de 2023 @ 17:26:37.173 Google Chrome CVE-2023-1811 Alto resolvido
13 de abril de 2023 @ 17:26:37.163 Google Chrome CVE-2023-1812 Alto resolvido
13 de abril de 2023 @ 17:26:37.153 Google Chrome CVE-2023-1813 Médio resolvido
13 de abril de 2023 @ 17:26:37.142 Google Chrome CVE-2023-1814 Médio resolvido
13 de abril de 2023 @ 17:26:37.132 Google Chrome CVE-2023-1815 Alto resolvido
13 de abril de 2023 @ 17:26:37.122 Google Chrome CVE-2023-1816 Médio resolvido
13 de abril de 2023 @ 17:26:37.112 Google Chrome CVE-2023-1817 Médio resolvido
13 de abril de 2023 @ 17:26:37.102 Google Chrome CVE-2023-1818 Alto resolvido

Situação Problema

Antes da ferramenta, a segurança da informação era gerenciada de forma manual.

Qual é o problema?

O não uso de um SIEM pode trazer vários problemas para a segurança de uma organização, como:

- Falta de visibilidade;
- Aumento do tempo de resposta;
- Dificuldade na análise de dados; e
- Maior risco de violação de dados.

Solução para o problema !

O primeiro passo para implementar um SIEM é realizar um planejamento adequado, como:

- Definir os objetivos da implementação do SIEM;
- Avaliar a infraestrutura existente;
- Definir as políticas de segurança;
- Realizar a implementação; e
- Testar e ajustar.

Como vamos saber quando o problema estiver resolvido?

Com ajuda da ferramenta SIEM, as ameaças será interrompida antes que causem danos.

- Na Confidencialidade;
- Integridade; e
- Disponibilidade;