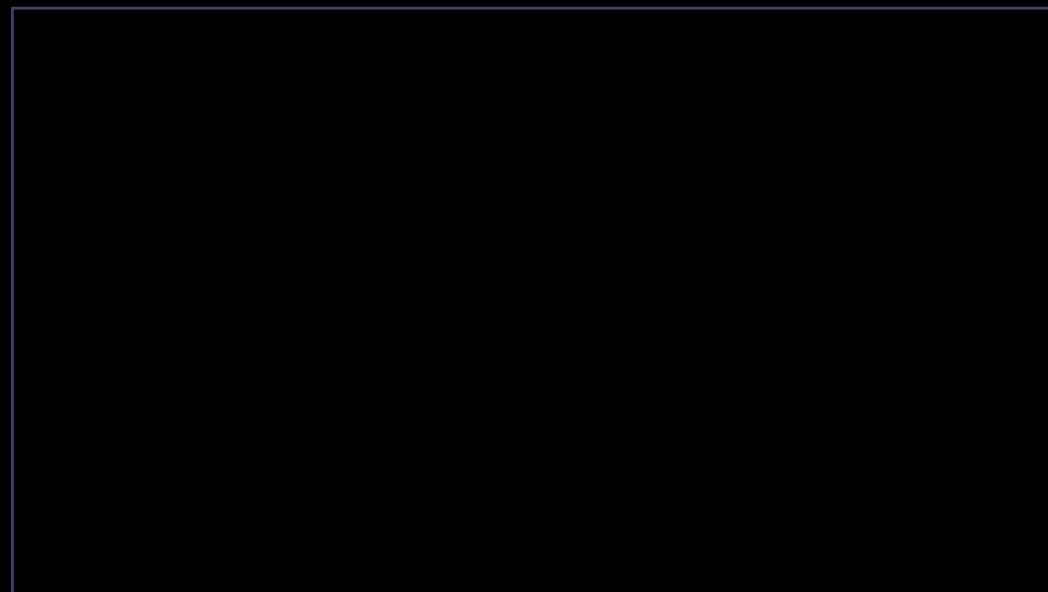




Prime

CCS-A

Avaliações de Segurança –
Syslog e SIEM



Syslog / SIEM

► Syslog – System Logging Protocol



Protocolo padrão para sistemas Linux.



Sistema de relatórios de erros fica separado do ativo monitorado.



Padrão para registrar remotamente.

► Security Information and Event Management (SIEM)



Coleta;



Agrega;

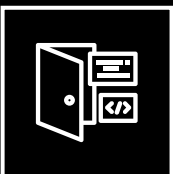


Aplica correspondência para se tornar legível.

Revisão de Relatórios



Relatórios ou alertas são os principais meios de fornecer saída de um SIEM.



Como qualquer ferramenta de monitoramento, certifique-se de revisar os relatórios do tipo de atividade no seu ambiente.



Podem ser revisados para determinar se um incidente é real.

Captura de Pacotes

- ▶ Elemento básico para engenheiros de rede.

- ▶ Diagnóstico e entendimento de problemas de comunicação de rede.

- ▶ Uso do SIEM:



Quando uma regra é acionada, o **appliance de captura** coleta e envia uma quantidade de tráfego para análise.

- ▶ Pode ser feito com hardware comum:



Custo relativamente baixo de armazenamento;



Caso seja posicionado adequadamente.

Entradas de Dados

- ▶ Deve haver muitas entradas de dados para o SIEM.
- ▶ Sobre o SIEM:
 -  O importante é determinar quais informações são necessárias;
 -  Definir as saídas desejadas também é fundamental;
 -  Rastreia entradas necessárias de firewall, sistemas, dispositivos de rede e servidores.
- ▶ SIEM é ajustado para responder às perguntas sobre o ambiente e seus riscos.

Análise do Comportamento do Usuário

- ▶ Avanços na análise comportamental proporcionaram outro uso para o SIEM.



Muitos SIEMs têm módulos para análise do comportamento do usuário final.

- ▶ O SIEM deve monitorar o comportamento do usuário para ajudar a detectar o potencial de ameaças internas.



Mostra padrões de atividade.

Análise de Sentimentos

- ▶ Correspondência de padrões = Sentimentos específicos.
- ▶ Podem determinar entradas como (em conjunto com a IA):



E-mails;



Bate-papos;



Mecanismos de coleta de feedback;



Comunicações de mídia social.

- ▶ Usada para rastrear padrões nas emoções: "feliz", "triste", "bravo" ou "frustrado".

Monitoramento de Segurança

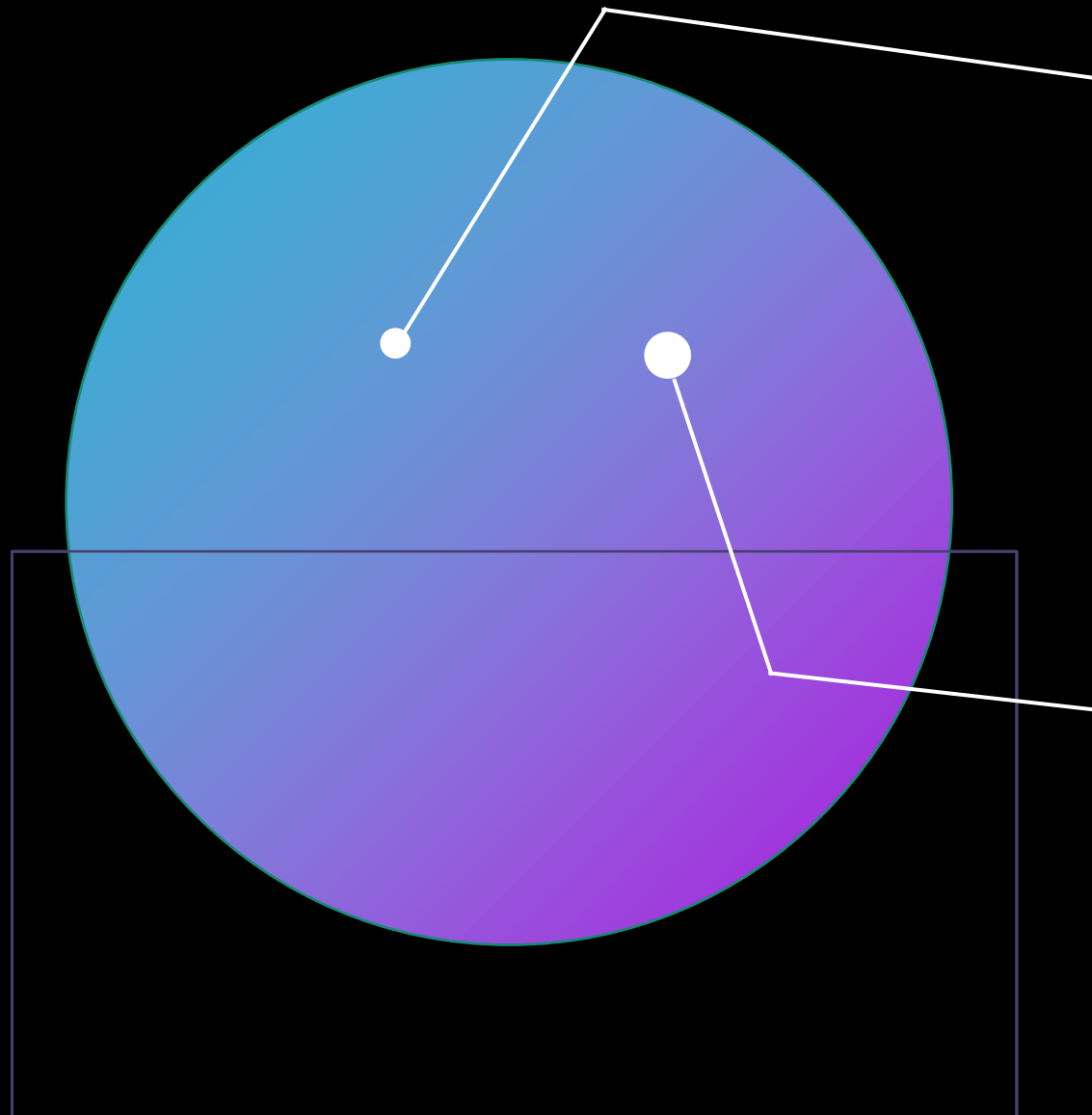
- ▶ Processo de coleta e análise de informações.
 - ▶ Detecta comportamentos suspeitos ou alterações não autorizadas.
- ▶ SIEMs – Gerenciamento dos dados de eventos associados aos eventos detectados.
- ▶ SIEM e SOAR – Essenciais para o monitoramento de segurança.
- ▶ SOAR: Automatizar as operações com foco em:
 - Gerenciamento de ameaças e vulnerabilidades;
 - Resposta a incidentes de segurança;
 - Automação de operações de segurança.

Agregação de Logs

- ▶ Processo de combinação de logs.
 - ▶ Permite formatos diferentes de diferentes sistemas.
 - ▶ Permite juntá-los para fazer uma análise completa.
- ▶ Durante o processo de agregação, os logs podem ser:
 -  | Analisados;
 -  | Modificados;
 -  | Campos-chave extraídos ou modificados com base em pesquisas e regras.
- ▶ Condiciona dados em um formato pesquisável e utilizável no SIEM.

Coletores de Log

- ▶ Softwares que funcionam para coletar dados de fontes independentes.
- ▶  Para alimentar um SIEM.
- ▶ Podem ter formatos diferentes de diferentes dispositivos.
- ▶ Podem harmonizar esses diferentes elementos em um fluxo de dados.



Orquestração, Automação e Resposta de Segurança (SOAR)

- ▶ É muito mais do que uma ferramenta de monitoramento.
- ▶ Dados geralmente são alimentados por SIEM, mas o SOAR é uma integração completa.
 -  Os sistemas de orquestração, automação e resposta de segurança (SOAR) pegam dados SIEM.
- ▶ Caçadores de ameaças usam essas informações.
 -  Para automatizar e responder a incidentes de segurança, facilitando a identificação de métodos de acesso e ataque.
- ▶ SOAR combinam:
 -  Dados;
 -  Alarmes de plataformas integradas.

OBRIGADO!

AVALIAÇÕES DE SEGURANÇA -
SYSLOG/INFORMAÇÕES DE SEGURANÇA E
GERENCIAMENTO DE EVENTOS (SIEM)