
mindthesec
2021

mindthesec 2021

José Lopes

Trabalha com segurança da informação desde 2013, na Companhia Energética de Minas Gerais (Cemig).

Foi responsável por estruturar o CSIRT Cemig e tornou-se coordenador do SOC Cemig em 2017, cargo que ocupa até a atualidade.

Formado em Ciência da Computação, tem algumas certificações relevantes na área de segurança: CISSP, Security+, AWS Security Specialist.

mindthesec 2021

Visibilidade de Rede

Tratar incidentes adequadamente requer **conhecimento da rede** e dos sistemas que a compõem, mas para fazer isso de forma realmente eficaz é necessário ter visão de quem faz o quê no perímetro.

Esta palestra apresenta algumas ideias nesse sentido, visando reduzir a dedução e aumentar a quantidade de fatos para **tratar incidentes** de forma mais assertiva.

mindthesec 2021

Conteúdo da apresentação

01 Introdução

02 Caçando Fantasmas

03 Tratando Incidentes

04 Conclusão

Introdução

- **Incidentes** podem acontecer a qualquer momento na rede.
- Para **responder** adequadamente é importante ter:
  - pessoas capacitadas
  - processos definidos e comunicados
  - tecnologias configuradas
- Mas mesmo com tudo isso, pode não ser possível identificar a **causa raiz**, se os times não tiverem a devida visão sobre o que ocorre na rede.
- Nesta palestra, teremos alguns ***insights*** de como aumentar a visibilidade e como isso poderá ajudar a evitar/tratar incidentes e garantir o correto funcionamento da rede.

Caçando Fantasmas

- Tratar incidentes **sem dados** suficientes pode parecer como caçar de fantasmas nos filmes de Hollywood.

- Durante o tratamento de um incidente, algumas **perguntas** costumam aparecer, como:
  - Qual o usuário associado?
  - Quais as máquinas relacionadas (*source*, *destination*)?
  - Quando começou?
  - Por onde passou?

- Caso não se tenha sistemas capazes de **monitorar** eventos, algumas dessas perguntas podem ficar sem resposta ou serem parcialmente respondidas, comprometendo o tratamento.

Caçando Fantasmas

- No **pior cenário**, os times não têm qualquer informação sobre o ambiente e se sentem assombrados, sem saber quem e onde está o fantasma.
  - Não existe monitoramento

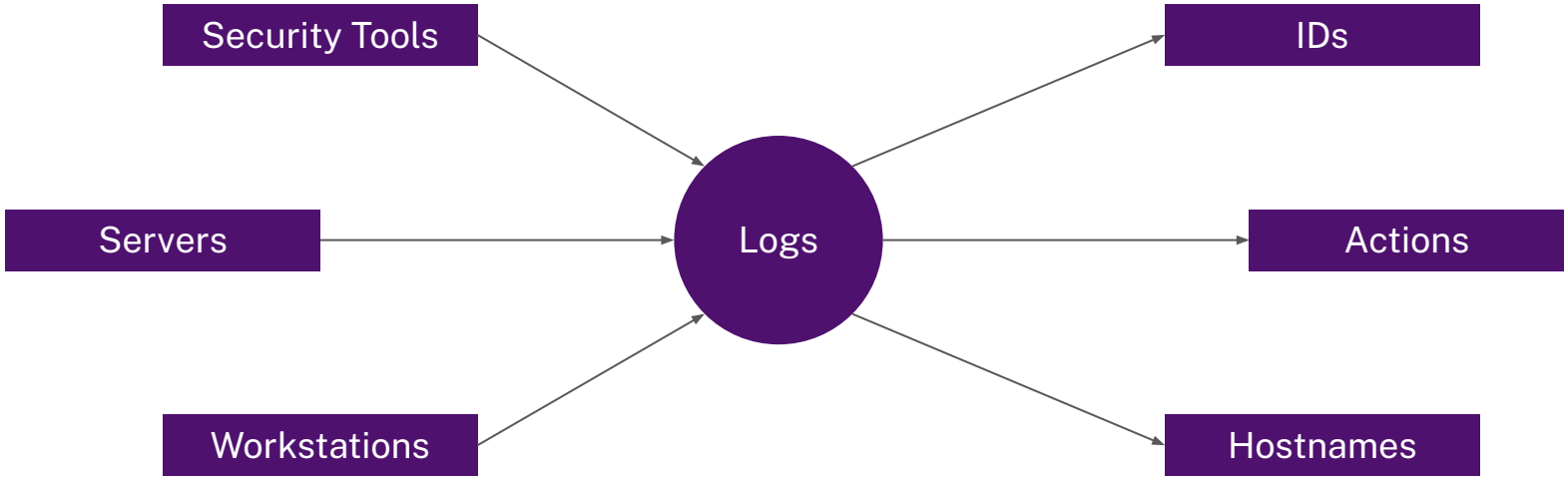
- Em um cenário **mais comum**, é possível que os times tenham alguma ideia da rede e consigam enxergar *flashes* de atividades maliciosas.
  - Apenas **alguns sistemas** são monitorados
  - Só se tem visão quando o **ator de ameaças** interage com tais sistemas

Tratando Incidentes

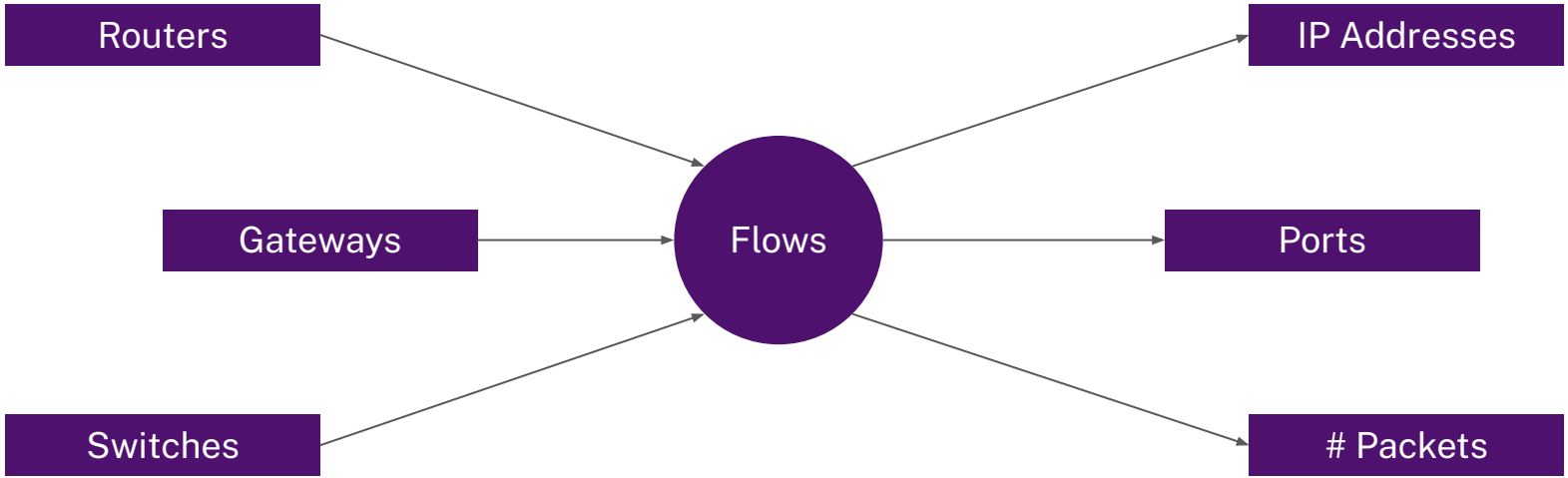
- No **cenário ideal**, os times têm dados de diversos sistemas e sabem o que se passa na rede, deixando de "caçar fantasmas" e passando a tratar incidentes de forma eficaz.

- Mas que dados são esses?
  - **Logs** de sistemas
  - **Flows** de rede
  - **Feeds** de ameaças

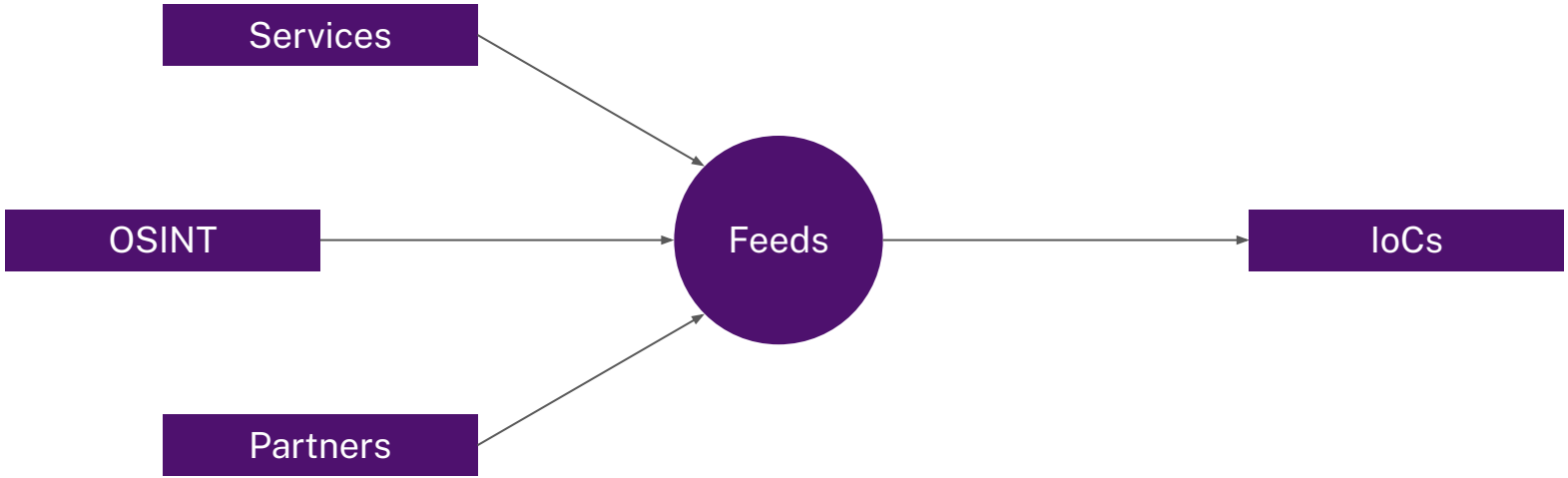
Tratando Incidentes



Tratando Incidentes



Tratando Incidentes



Tratando Incidentes

- Como é difícil ter recursos suficientes para receber todos os logs, flows e feeds, é importante que os times consigam "**pinçar**" dados:
  - Logs:
    - Definir sistemas **críticos** ou com alto potencial de detecção de atores de ameaças: firewalls, DCs, servidores importantes, antimalware, IPS...
    - **Filtrar** *facilities*/*severities* ou *event IDs*, para receber o que é mais importante
  - Flows:
    - Definir ativos que são "**chave**" na rede, por onde o ator de ameaças passaria: routers de borda, switches de redes críticas, switches de DMZ...
    - Definir **taxas de amostragem**, em vez de receber flows 1:1
  - Feeds:
    - Definir feeds de ameaças **relevantes** e filtrar IoCs que sejam pertinentes ao ambiente, à empresa ou ao nicho de mercado em que se está inserido

Tratando Incidentes

- O **tempo** é fundamental! É de suma importância que todos os relógios estejam sincronizados, para montar a linha temporal.
  - Idealmente, os tempos deveriam ser acompanhados da *time zone*.
- Logs não têm **padrão**: conhecimento em expressões regulares é fundamental para extrair os dados.
- Flows têm campos **padronizados** e são unidirecionais.
  - Fáceis de se configurar, desde que o agregador conheça o protocolo (sFlow, jFlow, IPFix, NetFlow v5...).
- Feeds precisam ser filtrados e idealmente devem ser acompanhados de **contexto**.

Conclusão

- Computação é uma ciência exata e por isso, os profissionais devem se embasar mais em **dados** e menos em suposições para tratar incidentes em computadores.
  - Por isso, a **visibilidade de rede** é fundamental no tratamento de incidentes

- O ***feeling* do analista** é importante, mas requer dados suficientes para definir ações relevantes para o tratamento.
  - Entradas erradas, tendem a gerar saídas erradas

Conclusão

- Logs e flows são fontes ricas de dados para prover visão da rede e são gerados **gratuitamente** pelas ferramentas e sistemas do parque.
- Feeds têm potencial para ajudar na **prevenção** de incidentes.
- Logs **variam** muito entre aplicação, sistema operacional e ativos de rede: saiba o que cada um pode te entregar.
- Desenvolvedores: criem aplicações que gerem logs **relevantes**!

mindthesec 2021

Obrigado


joselopes@cemig.com.br


https://www.linkedin.com/in/jlopesjr/