recurso_28_junho_2023

Ex. 5

Question: Proponha um sistema SIEM, incluindo o processo de coleta de dados e a definição de regras de alerta, capaz de alertar para:

Ex. 5.a)

Question: Tentativas de uso ilegítimo dos servidores DNS da empresa, para exfiltração ou C&C. (2.0 valores)
Answer:

SIEM Proposal:

1. Coleta de Dados:

- **Logs de Servidores DNS**: Coletar logs detalhados de consultas e respostas DNS dos servidores DNS internos.
- **NetFlow/SFlow**: Monitorar o tráfego de rede para identificar padrões anômalos de uso de DNS.
- **Logs de Firewall e IDS/IPS**: Coletar logs de firewalls e sistemas de detecção/prevenção de intrusões para monitorar tráfego DNS suspeito.

2. Regras de Alerta:

- **Alta Frequência de Consultas DNS**: Definir alertas para um número elevado de consultas DNS feitas por um único host em um curto período de tempo.
  - *Regra*: Se um host realizar mais de 100 consultas DNS por minuto, gerar um alerta.
- **Consultas para Domínios Suspeitos**: Alerta para consultas DNS para domínios conhecidos por serem associados a atividades maliciosas ou recém-criados.
  - *Regra*: Se um domínio consultado estiver na lista de domínios suspeitos ou for um domínio recém-criado, gerar um alerta.
- **Padrões Incomuns de Resolução**: Identificar padrões de consulta/resolução que não seguem o comportamento típico de uso.
  - *Regra*: Se um host realizar consultas para domínios com respostas de IPs internos ou respostas repetitivas, gerar um alerta.

Ex. 5.b)

Question: Possível comunicação IPv4 de C&C usando um serviço legitimo e autorizado (por exemplo o Twitter). (2.0 valores)
Answer:

SIEM Proposal:
1. Coleta de Dados:

- **Logs de Proxy Web**: Coletar logs de proxy web para monitorar acesso a serviços legítimos como Twitter.
- **Logs de Firewalls**: Monitorar logs de firewalls para tráfego HTTP/HTTPS específico para endereços IP de serviços autorizados.
- **Logs de Aplicações**: Coletar logs de aplicações que utilizam APIs de serviços legítimos.

2. Regras de Alerta:

- **Análise de Padrões de Comunicação**: Identificar padrões anômalos no uso de serviços legítimos, como uso fora do horário de trabalho ou picos de comunicação.
  - *Regra*: Se um host se comunicar com Twitter API mais de 50 vezes em uma hora fora do horário de trabalho, gerar um alerta.
- **Detectar Comandos Específicos**: Monitorar e analisar mensagens ou payloads específicos nas comunicações para identificar comandos C&C.
  - *Regra*: Se forem detectadas mensagens ou padrões de comunicação suspeitos que correspondam a comandos conhecidos de C&C, gerar um alerta.
- **Listas de Reputação e Contexto**: Usar listas de reputação para identificar endereços IP ou contas Twitter associados a atividades maliciosas.
  - *Regra*: Se uma comunicação for estabelecida com um IP ou conta Twitter de reputação suspeita, gerar um alerta.

Rácio de Upload/Download do serviço, na rede começa a ser alterado, então é uma coisa que pode ser normal. Normalmente, o uso do twitter é mete 2 ou 3 tweets e dps vê mais. Num cenário de Command & Control, é provável que comece a criar 1 tweet e ver 1 tweet...

Ex. 5.c)

Question: Possível exfiltração de dados por HTTPS de terminais da administração da empresa. (1.5 valores)
Answer:

SIEM Proposal:

1. Coleta de Dados:

- **Logs de Proxy Web**: Coletar logs de proxy web para monitorar acessos HTTPS.
- **NetFlow/SFlow**: Monitorar padrões de tráfego de rede, focando em conexões HTTPS.
- **Logs de Endpoints**: Coletar logs de atividades dos terminais, incluindo acessos a arquivos e movimentos de dados.

2. Regras de Alerta:

- **Análise de Volume de Dados**: Detectar grandes volumes de dados sendo transferidos via HTTPS fora dos padrões normais.
  - *Regra*: Se um terminal da administração transferir mais de 500 MB de dados via HTTPS em uma hora, gerar um alerta.
- **Acessos HTTPS Não Usuais**: Identificar acessos a domínios HTTPS que não são comumente acessados pelos terminais da administração.
  - *Regra*: Se um terminal acessar um domínio HTTPS que não esteja na lista de domínios permitidos ou habituais, gerar um alerta.
- **Padrões de Horário**: Monitorar transferências de dados HTTPS fora do horário normal de trabalho.
  - *Regra*: Se um terminal da administração transferir dados via HTTPS entre 22h e 6h, gerar um alerta.

terminais da empresa-> não é possível obter os logs. Então só é possível usar o netflow (routers) ou rsyslog (firewall), apenas podendo analisar os fluxos. Cuidado para não ficar pesado, analisar tudo e toda a gente. O ideal é ter um serviço leve que analise a rede, com regras básicas e após ser detetado, então sim, pode ser analisado mais os logs e outros métodos para saber exatamente. Propor soluções multi-stack é uma boa opção. Modelos com utilizadores podem ser definidos, para melhor aplicar regras e politicas