1.Log data

Armazenamos uma grande quantidade de informações de segurança em arquivos de log, presentes em servidores, dispositivos e outros componentes da rede. Esses logs contém dados sobre tráfego bloqueado e permitido, tentativas de exploração de vulnerabilidades, categorias de URLs acessadas e tráfego de DNS sinkhole, que pode indicar processos maliciosos dentro da rede. Isso nos permite documentar o fluxo de tráfego e correlacionar eventos de segurança em diferentes dispositivos.

Os **firewalls** são fontes valiosas de logs, registrando tráfego de entrada e saída, endereços IP de origem e destino, portas utilizadas e decisões sobre o bloqueio ou permissão de conexões. Firewalls de próxima geração (*Next Generation Firewalls* - NGFW) oferecem ainda mais detalhes, incluindo aplicações utilizadas, categorias de URLs acessadas e padrões de comportamento suspeitos.

Além dos firewalls, aplicações e sistemas operacionais também geram logs importantes. **No Windows, o Event Viewer registra eventos críticos, enquanto no Linux e macOS, esses logs estão no diretório /var/log**. Essas informações são geralmente consolidadas em sistemas de **Gerenciamento de Informações e Eventos de Segurança** (*Security Information and Event Management* - SIEM), permitindo análise centralizada e filtragem de eventos relevantes.

Os **dispositivos de endpoint**, como laptops, desktops e celulares, registram uma série de eventos, incluindo tentativas de login, mudanças de senha, bloqueios de conta e execução de processos. Esses logs podem ser enviados para um SIEM, permitindo a correlação entre eventos no endpoint, na rede e em outros dispositivos de segurança.

Sistemas de **Detecção e Prevenção de Intrusões** (*IDS/IPS*) também fornecem registros valiosos. Eles identificam ataques conhecidos e vulnerabilidades exploradas. Logs de IDS/IPS detalham eventos como ataques de negação de serviço (*DoS*), tentativas de exploração de portas e varreduras maliciosas. Esses eventos podem ser correlacionados no SIEM para uma visão mais abrangente da ameaça.

A **infraestrutura de rede**, incluindo switches, roteadores e pontos de acesso Wi-Fi, também gera registros importantes. Logs de roteadores podem indicar mudanças suspeitas nas tabelas de roteamento, enquanto switches podem registrar tentativas de acesso não autorizado. Firewalls e VPNs frequentemente identificam tráfego anômalo e podem bloquear atividades maliciosas automaticamente.

Além disso, **metadados** embutidos em documentos e e-mails podem revelar informações ocultas. E-mails contêm cabeçalhos que registram os servidores pelos quais passaram, enquanto imagens podem armazenar dados de GPS e informações sobre o dispositivo usado para capturá-las. Documentos de texto e planilhas muitas

vezes registram o autor do arquivo, datas de modificação e outras informações úteis em investigações.

As **varreduras de vulnerabilidades** geram uma grande quantidade de logs, ajudando a identificar dispositivos desprotegidos, configurações incorretas e softwares desatualizados. Um relatório de varredura pode indicar, por exemplo, que um sistema não possui um firewall ativado ou que contas de convidado estão habilitadas indevidamente.

Os **SIEMs** facilitam a análise dessa grande quantidade de dados, consolidando logs de diversas fontes. Para otimizar o processamento, é importante definir quais eventos são relevantes para a segurança da organização. Além disso, dashboards personalizados permitem visualizar rapidamente a situação da rede, sem necessidade de analisar cada log individualmente.

Outra ferramenta essencial para a investigação de tráfego é a análise de **pacotes de rede**, feita com softwares como Wireshark. A captura de pacotes permite examinar cada detalhe das comunicações, incluindo endereços IP, protocolos utilizados e até o conteúdo de mensagens trocadas. Firewalls e switches modernos podem realizar capturas diretamente, permitindo inspeções detalhadas sem necessidade de equipamentos adicionais.

O gerenciamento adequado dos logs e a correlação entre diferentes fontes de dados são fundamentais para identificar ameaças e responder rapidamente a incidentes de segurança. O uso de ferramentas como SIEMs, firewalls de próxima geração e análise de tráfego de rede permite um monitoramento mais eficiente e proativo contra ataques cibernéticos.