1.Monitoramento de segurança

Os invasores estão constantemente tentando obter acesso a sistemas e serviços, o que torna essencial o monitoramento contínuo das redes. Há uma grande quantidade de informações que precisam ser acompanhadas, incluindo autenticações, acessos remotos, uso de serviços e atividades suspeitas. O monitoramento em tempo real permite reagir rapidamente a eventos de segurança, verificando acessos a contas, regras de firewall e tráfego de rede. Muitas empresas utilizam painéis de controle para consolidar esses dados e fornecer uma visão geral da postura de segurança da organização.

Um dos principais pontos de monitoramento são os dispositivos de computação, onde é possível acompanhar autenticações e identificar a origem dos acessos. Caso haja um grande número de logins vindos de um país onde a empresa não possui funcionários, isso pode indicar uma tentativa de invasão. Além disso, é importante monitorar os serviços em execução nos dispositivos, como backups, versões de software e a necessidade de aplicação de patches. O acompanhamento do uso de aplicativos também é essencial para garantir a disponibilidade dos sistemas e identificar atividades anômalas.

O monitoramento do tráfego de rede pode ajudar a detectar incidentes de segurança, como exfiltração de dados. Se uma quantidade incomum de dados for transferida repentinamente, isso pode indicar que um atacante está roubando informações. Manter contato com os desenvolvedores dos aplicativos utilizados na empresa é uma prática recomendada, pois permite receber notificações sobre falhas de segurança e atualizações críticas.

Outro aspecto importante do monitoramento é a análise dos acessos remotos à rede corporativa. As empresas precisam identificar quantos usuários estão conectados via VPN, distinguindo entre funcionários, fornecedores e visitantes. O monitoramento de firewalls e sistemas de prevenção de intrusão pode revelar tentativas de ataques, permitindo ações preventivas antes que uma invasão ocorra.

Monitorar diversos sistemas diferentes pode ser um desafio, pois cada um gera logs em formatos variados e coleta informações distintas. Para resolver isso, muitas organizações utilizam **SIEMs (Security Information and Event Management)**, **que consolidam logs de dispositivos como firewalls, switches, servidores e roteadores em um único banco de dados**. Isso facilita a correlação de eventos e a criação de relatórios detalhados sobre atividades suspeitas.

Com um SIEM, é possível comparar informações de autenticação em VPNs e correlacioná-las com acessos a aplicativos internos. Também é possível monitorar o volume de dados transferidos na rede, estabelecendo padrões normais e emitindo alertas caso ocorram variações inesperadas. Além disso, relatórios podem ser gerados

para identificar usuários com permissões excessivas ou processos de acesso não autorizados.

Todos os dias, novas vulnerabilidades são descobertas, e é crucial saber quais sistemas estão suscetíveis a essas falhas. O desafio aumenta devido à mobilidade dos dispositivos, como laptops e smartphones, que estão em constante movimento. Para lidar com isso, muitas empresas adotam ferramentas que realizam varreduras automáticas em todos os dispositivos da rede, coletando informações sobre versões de sistemas operacionais, drivers e aplicativos instalados.

Essas varreduras geram grandes volumes de dados, armazenados em bancos de dados para análise posterior. Relatórios detalhados podem ser criados para avaliar o nível de conformidade dos dispositivos e determinar quais precisam de atualizações. Um dos relatórios mais importantes é o que mostra quais dispositivos não estão em conformidade com as políticas de segurança e quais ações devem ser tomadas para corrigir isso.

Além de relatórios de conformidade, empresas também realizam análises hipotéticas, chamadas de relatórios ad hoc, para prever impactos de mudanças futuras. Por exemplo, um relatório pode ser gerado para avaliar quantos dispositivos serão afetados quando um sistema operacional atingir o fim do suporte dentro de seis meses.

Diferente do que é mostrado em filmes, onde invasores são rapidamente detectados, a realidade é bem diferente. Um relatório da IBM de 2022 revelou que, em média, as empresas levam cerca de nove meses para identificar e conter uma violação de segurança. Durante esse tempo, os invasores podem explorar sistemas, obter acesso a dados e se estabelecer dentro da rede sem serem notados. Isso destaca a importância de ter uma estratégia de backup de longo prazo, pois um ataque pode permanecer oculto por meses ou até anos antes de ser descoberto.

Em algumas organizações, leis estaduais ou federais exigem a retenção de dados por períodos específicos. Esses registros não são apenas úteis para fins operacionais, mas também ajudam a entender atividades maliciosas dentro da rede.

Alertas em tempo real são essenciais para detectar ataques rapidamente. Um aumento inesperado nos erros de autenticação pode indicar uma tentativa de ataque por força bruta. Da mesma forma, um grande volume de dados sendo transferido para um servidor externo pode indicar um vazamento de informações. Ter um sistema de alerta eficiente permite que a equipe de segurança reaja imediatamente a essas ameaças.

Ao invés de esperar que alguém veja um relatório na manhã seguinte, um sistema de segurança pode enviar mensagens de texto ou e-mails para notificar os responsáveis assim que uma ameaça for detectada. Em centros de operações de

segurança (SOC), alarmes são configurados para alertar a equipe sobre incidentes críticos.

Quando um ataque é identificado, uma resposta comum é **isolar** o dispositivo comprometido da rede para impedir que o invasor se movimente lateralmente e comprometa outros sistemas. No entanto, é crucial garantir que os alertas sejam precisos, pois falsos positivos podem levar a interrupções desnecessárias.

Ajustar corretamente os alertas é um processo contínuo, buscando um equilíbrio entre detectar ameaças reais e evitar notificações excessivas. O maior perigo ocorre quando um evento crítico não gera um alerta, o que é conhecido como **falso negativo**. Esse ajuste fino é fundamental para garantir que as equipes de segurança possam tomar decisões rápidas e informadas com base nos alarmes recebidos.