1.Resposta a incidentes e proteção de rede

1.1 Monitoramento de redes e redes sem fio

O ***Network Monitor***, também conhecido como analisador de rede ou sniffer, é uma ferramenta utilizada para monitorar e analisar o tráfego de rede. Ele permite capturar pacotes de dados que circulam pela rede, tornando possível examinar em detalhes as comunicações entre dispositivos e os diferentes protocolos que estão sendo utilizados.

Funcionamento:

- **Captura de pacotes:** O Network Monitor captura os pacotes de dados que trafegam na rede. Isso é realizado através de interfaces de rede dedicadas, como placas de rede ou adaptadores, que permitem ao analisador acessar o fluxo de informações que passa por elas.
- **Análise de pacotes:** Após a captura, os pacotes são analisados para extrair informações importantes. O Network Monitor pode decodificar os dados presentes nos pacotes, exibindo detalhes dos cabeçalhos dos protocolos utilizados, endereços IP, portas, informações de controle e carga útil dos pacotes.
- **Filtragem de dados:** Para tornar a análise mais eficiente, o Network Monitor permite aplicar filtros para selecionar pacotes específicos para visualização. Isso é especialmente útil em redes movimentadas, onde a quantidade de dados pode ser significativa. Filtros podem ser baseados em endereços IP, portas, protocolos, entre outros critérios.
- **Visualização e análise de tráfego:** Os pacotes capturados são apresentados ao usuário em uma interface gráfica ou em formato de lista. O Network Monitor possibilita observar o tráfego em tempo real ou examinar capturas prévias. Essa visualização detalhada é fundamental para identificar padrões, detectar problemas e analisar o comportamento da rede.
- **Diagnóstico de problemas:** O Network Monitor é amplamente utilizado por administradores de rede e profissionais de segurança para diagnosticar problemas e investigar atividades suspeitas. Com ele, é possível identificar tráfego não autorizado, anomalias de rede, gargalos de desempenho e outros problemas que podem afetar a operação da rede.
- **Registro e exportação de dados:** O Network Monitor permite gravar as capturas em arquivos de registro para análises futuras. Além disso, os dados capturados podem ser exportados em diferentes formatos para compartilhamento com outros profissionais ou para análises posteriores em outras ferramentas.

1.2 Logs

Logs são registros detalhados de eventos, atividades ou mensagens geradas por sistemas, aplicativos ou dispositivos. Eles têm o propósito de registrar informações relevantes para análise, monitoramento, solução de problemas, auditoria e segurança.

Aspectos e funcionamento:

- **Geração de logs:** Os sistemas e aplicativos geram logs automaticamente conforme eventos ocorrem. Isso pode incluir ações do usuário, erros, atividades de rede, processos iniciados ou encerrados, entre outros eventos importantes.
- **Formato de estrutura:** Os logs geralmente possuem um formato estruturado, com informações específicas sobre cada evento registrado. Essas informações podem incluir data e hora, nível de severidade (como informação, aviso ou erro), origem do evento, descrição do evento e outros detalhes relevantes.
- **Armazenamento e gerenciamento:** Os logs são armazenados em arquivos ou em um sistema centralizado de gerenciamento de logs. É importante que os logs sejam protegidos e devidamente gerenciados, especialmente para fins de auditoria e conformidade.
- **Análise e monitoramento:** Os logs são analisados regularmente para identificar possíveis problemas, anomalias ou tendências. O monitoramento contínuo dos logs ajuda a detectar atividades suspeitas ou comportamentos incomuns na rede ou nos sistemas.
- **Ferramentas de análise:** Existem ferramentas específicas, como SIEM (Security Information and Event Management) e sistemas de gerenciamento de logs, que auxiliam na análise, agregação e correlação dos logs de diferentes fontes. Essas ferramentas ajudam a simplificar o processo de identificação de eventos relevantes e a resposta a incidentes.

1.3 SysLog

SysLog é um protocolo padronizado amplamente utilizado para a geração, envio e recebimento de mensagens de registro de eventos em sistemas de computadores e dispositivos de rede. Criado originalmente em ambientes Unix-like, o SysLog tornou-se um dos métodos mais comuns para coletar informações sobre atividades e eventos relevantes que ocorrem nos sistemas e aplicativos.

O funcionamento do SysLog envolve a geração de mensagens de eventos pelos sistemas e sua posterior transmissão para um servidor SysLog centralizado ou outros dispositivos que estejam escutando em uma determinada porta.

As mensagens SysLog são categorizadas em "*facilities*" (instalações) e "*severidades*", permitindo classificar a origem do evento e sua gravidade. O servidor SysLog centralizado consolida as mensagens de vários dispositivos em um único local, facilitando a análise, monitoramento e resposta a incidentes em toda a infraestrutura.

Além de ser uma ferramenta essencial para a manutenção e solução de problemas, o SysLog desempenha um papel fundamental na segurança da rede e dos sistemas, pois permite identificar atividades suspeitas, rastrear acessos não autorizados, detectar falhas de segurança e analisar tendências de eventos.

Ele é frequentemente utilizado em conjunto com ferramentas de análise e gerenciamento de logs, como SIEM (Security Information and Event Management), para proporcionar uma visão abrangente do ambiente de TI e auxiliar na proteção contra ameaças cibernéticas.

1.4 Coleta de Logs

A ***coleta de logs*** (***Log Collection***) é uma etapa essencial no processo de monitoramento e análise de eventos de segurança e atividades em uma rede ou sistema. Existem diferentes abordagens para a coleta de logs, cada uma com suas características específicas. As três principais abordagens são: ***Agent-based*** (***baseada em agente***), ***Collector e Sensor***.

Detalhes:

- **Agent-based:** Na abordagem Agent-based, são instalados agentes (ou agentes de coleta de logs) nos dispositivos e sistemas que se deseja monitorar. Esses agentes são pequenos programas ou módulos que coletam e encaminham os logs relevantes para um servidor centralizado ou outro sistema de gerenciamento de logs. Cada agente é responsável por coletar os logs locais do dispositivo onde está instalado e pode ser configurado para filtrar ou selecionar os logs específicos que serão enviados para a centralização.
- **Coletor:** Na abordagem do Collector, um dispositivo centralizado, conhecido como coletor de logs, é responsável por conectar-se a outros dispositivos, sistemas ou agentes de coleta de logs distribuídos na rede. O coletor recebe os logs enviados por esses dispositivos remotos e os armazena em um repositório central. Essa abordagem é especialmente útil em redes complexas, onde há uma grande quantidade de dispositivos e sistemas a serem monitorados. O Coletor ajuda a centralizar os logs e facilita a análise e correlação de eventos.
- **Sensor:** A abordagem do Sensor é comumente usada em ambientes de rede, especialmente em sistemas de prevenção de intrusões (IPS) e firewalls. Os sensores são dispositivos dedicados que monitoram o tráfego de rede em busca de atividades suspeitas e eventos de segurança. Eles coletam logs de eventos específicos, como tentativas de intrusão, tráfego bloqueado, conexões de rede, entre outros, e os enviam para um sistema centralizado para análise e resposta a incidentes. Os sensores desempenham um papel importante na detecção proativa de ameaças e na proteção da rede contra ataques.

2.Security Information and Event Management (SIEM)

Security Information and Event Management (SIEM) é uma solução de segurança cibernética que combina a funcionalidade de coleta, armazenamento, análise e correlação de eventos e informações de segurança em tempo real, provenientes de diversas fontes em uma rede.

O objetivo principal do SIEM é oferecer uma visão abrangente e centralizada da postura de segurança da organização, permitindo identificar ameaças e responder a incidentes de forma mais eficiente. O funcionamento do SIEM pode ser dividido em etapas:

- **Coleta de dados:** O SIEM coleta dados de várias fontes, como logs de eventos de sistemas, aplicativos, dispositivos de rede, firewalls, IDS/IPS (Sistemas de Detecção e Prevenção de Intrusões), antivírus, entre outros. Esses dados são enviados para o SIEM por meio de agentes, sondas ou dispositivos de coleta.
- **Armazenamento centralizado:** Os dados coletados são armazenados em um repositório centralizado, o que facilita a busca, consulta e análise de informações relevantes. O armazenamento de longo prazo permite a análise histórica e a criação de relatórios de tendências.
- **Normalização e correlação:** O SIEM normaliza os dados recebidos para um formato comum, o que facilita a análise e correlação de eventos. A correlação é uma etapa importante em que o SIEM analisa os eventos coletados para identificar padrões e relacionamentos entre eles, permitindo detectar ameaças complexas que podem não ser evidentes em análises individuais.
- **Detecção de anomalias e ameaças:** O SIEM utiliza regras e algoritmos de detecção para identificar atividades suspeitas e potenciais ameaças à segurança. Ele pode disparar alertas em tempo real para que os analistas de segurança possam responder prontamente a incidentes.
- **Notificação e resposta:** Quando uma atividade maliciosa ou suspeita é detectada, o SIEM pode acionar notificações e alertas para a equipe de segurança. A resposta aos incidentes pode incluir ações como bloqueio de IPs, isolamento de máquinas comprometidas, análise forense, entre outras medidas de mitigação.
- **Relatórios e conformidade:** O SIEM gera relatórios detalhados sobre a atividade de segurança da organização, auxiliando na demonstração de conformidade com padrões regulatórios e políticas internas de segurança.
- **Integração com outras ferramentas:** O SIEM pode se integrar com outras ferramentas de segurança, como Sistemas de Gerenciamento de Vulnerabilidades e Sistemas de Gerenciamento de Incidentes, para proporcionar uma abordagem mais abrangente e colaborativa à segurança cibernética.

2.1 Agregação de logs

A Log Aggregation, ou agregação de logs, é um processo de coleta e centralização de logs de diferentes fontes em um único local. Essa técnica é utilizada para facilitar a análise, monitoramento e correlação de eventos de segurança e atividades em uma rede ou sistema e é normalmente realizado no SIEM.

Funcionamento:

- **Coleta de logs de diferentes fontes:** O processo de Log Aggregation envolve a coleta de logs de diversas fontes, como sistemas operacionais, aplicativos, dispositivos de rede, bancos de dados, servidores, appliances de segurança, entre outros. Esses logs são originados de diferentes dispositivos e podem estar distribuídos por toda a infraestrutura.
- **Centralização dos logs:** Os logs coletados são enviados para um único local centralizado, conhecido como servidor de agregação de logs ou repositório central.

Esse servidor é responsável por armazenar todos os logs coletados e disponibilizá-los para análise e monitoramento.

- **Normalização dos dados:** Antes de armazenar os logs, o processo de agregação pode envolver a normalização dos dados para garantir que todos os logs sejam convertidos para um formato comum. Isso facilita a análise e correlação dos eventos, independentemente de sua origem e formato original.
- **Análise e correlação de eventos:** Com os logs centralizados e normalizados, é possível realizar análises abrangentes e correlacionar eventos de diferentes fontes. A correlação de eventos permite identificar padrões e relacionamentos entre os logs, o que auxilia na detecção de atividades suspeitas e ameaças.
- **Alertas e notificações:** A agregação de logs permite a configuração de regras e alertas para acionar notificações em tempo real quando eventos críticos ou suspeitos são identificados. Isso possibilita uma resposta rápida a incidentes de segurança.
- **Armazenamento de longo prazo:** Além de possibilitar análises em tempo real, a agregação de logs também permite o armazenamento de longo prazo dos registros. Isso é útil para auditorias, conformidade com regulamentos e investigações forenses.
- **Relatórios e inteligência de segurança:** A centralização e agregação de logs também possibilitam a geração de relatórios abrangentes e fornecem informações valiosas sobre a postura de segurança da organização. A análise dos logs agregados pode gerar inteligência de segurança que ajuda a melhorar a proteção da rede contra ameaças cibernéticas.

3.User and Entity Behavior Analytics (UEBA)

User and Entity Behavior Analytics (UEBA), ou Análise de Comportamento de Usuários e Entidades, é uma abordagem avançada de segurança cibernética que utiliza técnicas de inteligência artificial e aprendizado de máquina para detectar ameaças e atividades maliciosas com base no comportamento de usuários e entidades (como dispositivos, aplicativos e sistemas) em uma rede. Geralmente trabalha em conjunto com o SIEM.

O funcionamento do UEBA pode ser detalhado da seguinte forma:

- **Coleta de dados de comportamento:** O UEBA coleta e analisa uma ampla variedade de dados de comportamento dos usuários e entidades na rede. Inclui atividades de login, padrões de acesso a recursos, horários e locais de acesso, atividades de usuários privilegiados, interações com aplicativos e dispositivos, entre outros. Esses dados são coletados de várias fontes, como logs de eventos, registros de autenticação e dados de sistemas de gerenciamento de identidades.
- **Perfil de comportamento baseline:** O UEBA cria um perfil de comportamento baseline para cada usuário e entidade na rede. Esse perfil representa o comportamento normal e esperado de cada entidade. Para isso, o UEBA analisa o histórico de atividades para identificar padrões regulares e comportamentos típicos.
- **Detecção de anomalias:** O UEBA utiliza algoritmos de aprendizado de máquina para identificar anomalias no comportamento das entidades. Essas anomalias são indicativas de atividades incomuns ou suspeitas que podem representar ameaças de

segurança, como acesso a recursos não autorizados, tentativas de autenticação suspeitas, atividades fora do horário comercial, entre outras.

- **Correlação de eventos:** O UEBA também é capaz de correlacionar eventos aparentemente não relacionados para detectar comportamentos anômalos. Por exemplo, ele pode detectar se um usuário realiza uma ação de autenticação em um local geograficamente distante logo após ter se conectado localmente.
- **Pontuação de risco:** Com base nas detecções de anomalias e correlações de eventos, o UEBA atribui pontuações de risco a cada usuário e entidade. Quanto maior a pontuação, maior a probabilidade de comportamento malicioso ou suspeito.
- **Alertas e notificações:** Quando uma atividade suspeita é detectada e a pontuação de risco ultrapassa um limiar pré-definido, o UEBA dispara alertas e notificações para a equipe de segurança. Isso permite uma resposta rápida e pró-ativa a potenciais incidentes de segurança.
- **Adaptação ao ambiente:** O UEBA é capaz de aprender com o ambiente e se adaptar a mudanças no comportamento das entidades ao longo do tempo. Isso evita falsos positivos e aumenta a eficácia na detecção de ameaças em constante evolução.

4.Security Orchestration, Automation and Response (SOAR)

SOAR ou Orquestração, Automatização e Resposta de Segurança, é uma abordagem abrangente de segurança cibernética que combina a orquestração e automação de processos com a capacidade de resposta a incidentes em uma única plataforma integrada. O objetivo é melhorar a eficiência das equipes de segurança, reduzir o tempo de resposta a incidentes e simplificar a gestão de eventos de segurança. Geralmente trabalha em conjunto com o SIEM e o UEBA.

Funcionamento:

- **Coleta e agregação de dados:** O SOAR integra-se a várias fontes de dados, como sistemas de gerenciamento de logs, soluções de detecção de intrusões (IDS/IPS), sistemas de gerenciamento de vulnerabilidades e outras ferramentas de segurança. Ele coleta e agrega informações relevantes em tempo real para ter uma visão abrangente da postura de segurança da organização.
- **Análise e correlação de eventos:** O SOAR utiliza técnicas avançadas de análise e correlação de eventos para identificar incidentes de segurança, detectar padrões e relacionamentos entre eventos e priorizar alertas. Ajuda a reduzir o volume de alertas falsos e permite que a equipe se concentre nas ameaças mais críticas.
- **Automatização de tarefas:** Com base nas análises e correlações, o SOAR pode automatizar tarefas de resposta a incidentes e procedimentos de segurança. Inclui ações como isolamento de máquinas comprometidas, bloqueio de IPs maliciosos, remediação de vulnerabilidades conhecidas, entre outras medidas.
- **Orquestração de fluxo de trabalho:** O SOAR permite criar fluxos de trabalho personalizados para orquestrar as ações de resposta a incidentes. Ele pode coordenar a execução de várias tarefas e a interação entre diferentes sistemas de segurança, criando um processo mais eficiente e consistente.

- **Integração com ferramentas de segurança:** O SOAR é altamente integrado com várias ferramentas de segurança existentes na organização, permitindo interações contínuas e troca de informações entre elas. Isso facilita a automação e a resposta coordenada a incidentes.
- **Geração de relatórios e métricas:** O SOAR oferece recursos de geração de relatórios e métricas para acompanhar o desempenho das equipes de segurança, avaliar a eficácia das medidas de resposta a incidentes e demonstrar a conformidade com políticas e regulamentos de segurança.

5.Manipulação de arquivos

Os seguintes comandos permitem que os usuários extraiam informações relevantes, filtrem dados, registrem eventos e procurem padrões específicos em logs e outros arquivos de texto em sistemas Unix-like:

- **Comando Cat:** O comando cat (concatenate) é usado em sistemas Unix-like para exibir o conteúdo de um ou mais arquivos de texto no terminal. Ele também pode ser utilizado para combinar o conteúdo de vários arquivos em um único arquivo de saída. A sintaxe básica é cat arquivo1 arquivo2 ..., que exibirá o conteúdo do arquivo1, arquivo2 e assim por diante, consecutivamente, no terminal.
- **Comando Head e Tail:** São usados para exibir as primeiras e últimas linhas de um arquivo de texto, respectivamente. A sintaxe do comando head é head -n <número_de_linhas> arquivo, onde <número_de_linhas> é o número de linhas iniciais que se deseja exibir. Já a sintaxe do comando tail é tail -n <número_de_linhas> arquivo, onde <número_de_linhas> é o número de linhas finais que se deseja exibir.
- **Comando Logger:** É utilizado para registrar mensagens ou eventos no sistema de log do sistema operacional. Ele permite que os usuários e scripts adicionem entradas de log para registrar atividades importantes ou informações relevantes. A sintaxe do comando é simples, como por exemplo, logger "Mensagem de log".
- **Sintaxe de expressões regulares (Regex):** São padrões utilizados para identificar e extrair sequências de caracteres específicas em um texto. Elas são amplamente utilizadas em comandos e ferramentas de busca, substituição e filtragem de texto, como o comando grep. As expressões regulares podem incluir caracteres especiais e metacaracteres para definir padrões de busca mais complexos.
- **Comando Grep:** É uma ferramenta poderosa para busca e filtragem de texto baseada em expressões regulares. Ele permite procurar por padrões específicos em arquivos ou na saída de outros comandos. A sintaxe básica do comando é grep <padrão> arquivo, onde <padrão> é a expressão regular que você deseja buscar no arquivo.

6.Execução de sandbox

Uma sandbox é um ambiente de isolamento controlado onde os programas e arquivos suspeitos podem ser executados com segurança. Ela é usada para analisar o comportamento do malware sem comprometer a segurança do sistema principal. Ao executar o malware em uma sandbox, os pesquisadores podem observar como ele se comporta, quais ações executa e como interage com o sistema, identificando assim possíveis ameaças.

Muitas organizações utilizam ambientes de sandbox para analisar o comportamento de arquivos ou aplicativos desconhecidos. Os indicadores de execução de sandbox referem-se a comportamentos que o malware exibe quando é executado em um ambiente de teste. Malwares frequentemente tentam detectar a presença de uma sandbox e podem alterar seu comportamento para evitar a detecção, tornando esse um indicador importante.

6.1 Exemplos de técnicas que malware usa para evitar detecção em ambientes sandbox

O software malicioso é frequentemente projetado para detectar a presença de sandboxes e pode modificar seu comportamento para evitar a detecção.

6.2 Consumo de recurso

O malware muitas vezes consome uma quantidade significativa de recursos do sistema. O consumo excessivo de CPU — ou consumo de memória anormal —, é um indicador importante de atividade maliciosa, uma vez que costuma utilizar os recursos para executar suas operações. Profissionais de segurança monitoram a utilização de recursos em busca de picos ou comportamentos anômalos que possam sugerir a presença de malware.

6.3 Exemplos de ferramentas que monitoram o uso de recursos

Existem diversas ferramentas de monitoramento de recursos que podem ajudar a identificar o consumo anormal de recursos do sistema. Essas ferramentas permitem que os administradores e pesquisadores de segurança rastreiem de perto o desempenho do sistema e identifiquem atividades suspeitas. Alguns exemplos incluem o Monitor de Recursos do Windows e ferramentas de monitoramento de desempenho de código aberto, como o Sysinternals Suite.

7.Mudanças no sistema de arquivos

Quando o malware infecta um sistema, ele frequentemente faz alterações no sistema de arquivos, como criar ou modificar arquivos e diretórios. Essas mudanças podem ser indicativas de atividade maliciosa, pois o malware muitas vezes busca ocultar sua presença ou realizar ações prejudiciais. Os indicadores de mudanças no sistema de arquivos envolvem o rastreamento de qualquer modificação não autorizada e o registro dessas ações como indicativos de atividade suspeita.

7.1 Ferramentas que rastreiam alterações no sistema de arquivos

Para rastrear as mudanças no sistema de arquivos, existem várias ferramentas disponíveis, como o File Integrity Monitoring (FIM) e o Tripwire. Essas ferramentas monitoram continuamente o sistema de arquivos em busca de alterações não autorizadas e fornecem alertas quando identificam atividades suspeitas. Isso permite que os administradores de sistemas ajam rapidamente para conter ameaças.

8.Análise de processos

A análise de processos é uma técnica que se concentra em examinar o comportamento de programas e processos em execução em sistemas e redes. Pode envolver o estudo minucioso do comportamento de aplicativos, processos e serviços em um ambiente de computação. Isso inclui mapear quais ações eles executam, como interagem com outros elementos do sistema e quais recursos utilizam. Essas ações são importantes para detectar a presença de malware, pois muitos desses softwares tentam se camuflar como processos legítimos ou exploram processos existentes para realizar suas atividades maliciosas.

9.Técnicas baseadas em comportamento

- **Análise de tráfego de rede:** Essa técnica envolve a observação e análise do tráfego de rede gerado por processos e aplicativos. Ela é usada para identificar padrões de comunicação, que podem revelar atividades suspeitas, como conexões a servidores remotos ou transmissões não autorizadas de dados.
- **Análise de registros:** A análise de registros e logs do sistema é uma técnica crucial na detecção de atividades anômalas. Os registros, como logs de eventos do sistema ou logs de aplicativos, podem conter informações valiosas sobre ações suspeitas realizadas por processos.
- **Monitoramento de comportamento:** É uma técnica dinâmica que permite observar o comportamento dos processos em tempo real. Essa abordagem proativa ajuda a identificar a criação de arquivos, modificações no registro do sistema, ou outras atividades suspeitas enquanto ocorrem.

10.Ferramentas de análise de processos

- **Wireshark:** É uma ferramenta de análise de tráfego de rede de código aberto. Ela permite capturar e analisar pacotes de dados em tempo real, oferecendo insights sobre a comunicação de rede. Wireshark é uma ferramenta valiosa para identificar conexões suspeitas e comportamento malicioso na rede.
- **Sysinternals Suite:** É um conjunto de ferramentas desenvolvidas pela Microsoft, projetadas para ajudar na análise de processos em sistemas Windows. Dentro dessa suíte, você encontrará ferramentas como o Process Explorer, Process Monitor e Autoruns, que são indispensáveis para monitorar, diagnosticar e detectar atividades suspeitas em sistemas Windows

11.Prevenção de malware

As estratégias de prevenção de malware são medidas proativas adotadas para evitar a infecção por malware e fortalecer a segurança dos sistemas. Isso inclui uma série de práticas recomendadas que reduzem a superfície de ataque e minimizam as chances de infecção. Essas medidas podem abranger desde a configuração de políticas de segurança até a educação dos usuários.

- **Atualizações de software:** A manutenção regular e a atualização de sistemas e software são fundamentais. As atualizações frequentes garantem que os sistemas estejam protegidos contra vulnerabilidades conhecidas, reduzindo a exposição a ataques de malware.

- **Políticas de acesso:** A implementação de políticas de acesso restrito ajuda a controlar quem tem permissão para acessar sistemas e dados sensíveis. Isso limita a exposição à malware que possa ser introduzido por usuários não autorizados.
- **Conscientização dos usuários:** Treinar os usuários para reconhecer práticas inseguras, como clicar em links suspeitos ou fazer download de anexos de e-mail desconhecidos, é uma parte crítica da prevenção de malware.

12.Mitigação de riscos

A mitigação de riscos se concentra em como minimizar o impacto de uma infecção por malware quando as medidas de prevenção falham. Ainda que as medidas de prevenção sejam eficazes, é importante estar preparado para o cenário em que ocorra uma infecção por malware.

- **Estratégias de isolamento e contenção:** Ao detectar uma infecção por malware, é essencial isolar a ameaça para evitar que ela se espalhe para outros sistemas e dados. Isso pode envolver a desconexão da máquina afetada da rede ou a restrição do acesso a recursos críticos.
- **Recuperação e restauração:** Além do isolamento, a mitigação de riscos envolve a recuperação e restauração de sistemas comprometidos. Isso pode incluir a restauração de backups ou a limpeza profunda da máquina afetada para garantir que todo o malware tenha sido removido.
- **Investigação pós-incidente:** Uma parte importante da mitigação de riscos é a investigação pós-incidente para entender como o malware entrou no sistema e identificar possíveis pontos fracos na segurança. Isso ajuda a fortalecer a proteção contra futuras ameaças.