Monitoramento & Auditoria no **Ambiente de Mainframe**

Solução de auditoria e monitoração agressiva e abrangente, direcionada ao negócio.

A segurança do ambiente corporativo exige a captura e o armazenamento de todo o tráfego de informação interativa para processos de auditoria de forma ampla e completa, com exibição das telas e impressões relacionadas ao ambiente de mainframe.

Overview

Erros operacionais ou transações maliciosas que executem alterações nas bases de dados, nem sempre são alvos de auditoria ou permitem a geração de evidências, que as comprovem posteriormente.

Diversos níveis de usuários de sistemas possuem privilégios que podem mantê-los 'isentos' de controles que registrem suas ações.

A solução para este cenário é uma ferramenta que possibilite a monitoração de 100% do tráfego do acesso dos usuários mainframe com total rastreabilidade de origem dos acessos, possibilitando a identificação e comprovação de uma possível fraude e a geração de alertas em tempo real.

O Desafio

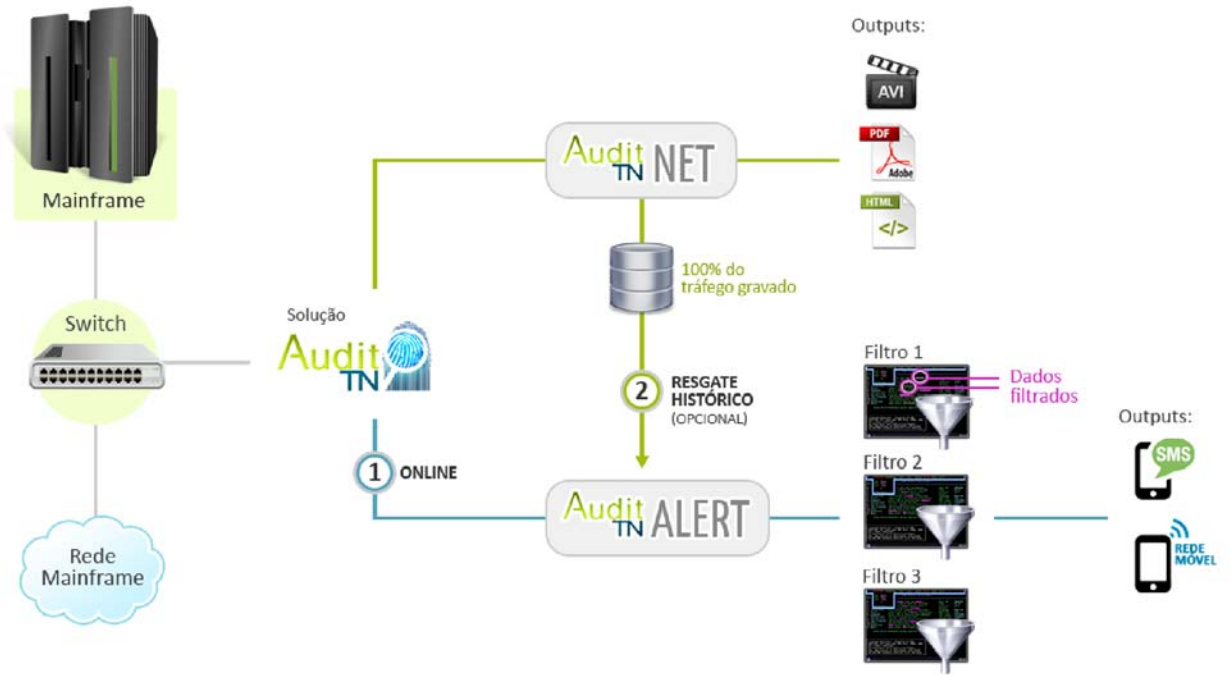
Estabelecer um processo ágil e de permanente monitoração da segurança nos ambientes de TI aderente às recomendações do mercado (ex: SOX). Além disso, ter a capacidade de replicar fielmente o perfil de acesso dos usuários aos recursos de sistema, permitindo analisar seu comportamento e desenvolver ações que viabilizem as melhores práticas para proteger ambientes críticos e de altos volumes de transações.

A solução

O **Audit-TN** oferece total monitoração e rastreabilidade, fazendo um registro detalhado das operações efetuadas nos ambientes de Mainframe.

1. Permite uma completa reconstrução dos acessos TN3270, através da captura de sessões TCP/IP.
2. Monitora administradores, desenvolvedores e usuários finais em qualquer operação de emulação TN3270, exibindo em formato AVI, HTML, RTF ou texto todas as telas e comandos emitidos ao Mainframe.
3. Identifica robôs de automação e acessos fora do padrão.
4. Suporta o tráfego de sessões TN3270 criptografadas (SSL) e de emulação via Web Browser (HOD).
5. Gera alertas real-time relativos a padrões de atividades suspeitas:
   - Ilimitadas regras podem ser estabelecidas para ativação dos alertas;
   - A implementação desses alertas pode ocorrer de forma distribuída, provendo a robustez exigida em cada ambiente;
   - Os alertas poderão ser emitidos via popup na estação, email e SMS.
   - Através de uma console web gerencia as configurações dos filtros geradores dos alertas, das telas capturadas nos alertas e dos logs da ferramenta.

Com o **Audit-TN** é possível capturar e reproduzir sessões, ou seja, registro de 100% das telas e impressões TN3270 e ainda contar com recursos de alerta e pesquisa em toda a rede



O Audit-TN é uma solução de auditoria não intrusiva de sistemas mainframe que:

- Não altera o consumo de MIPs/MSUs.
- Não oferece riscos para a continuidade dos processos da empresa.
- Não exige especialista em Mainframe para sua implementação e uso.

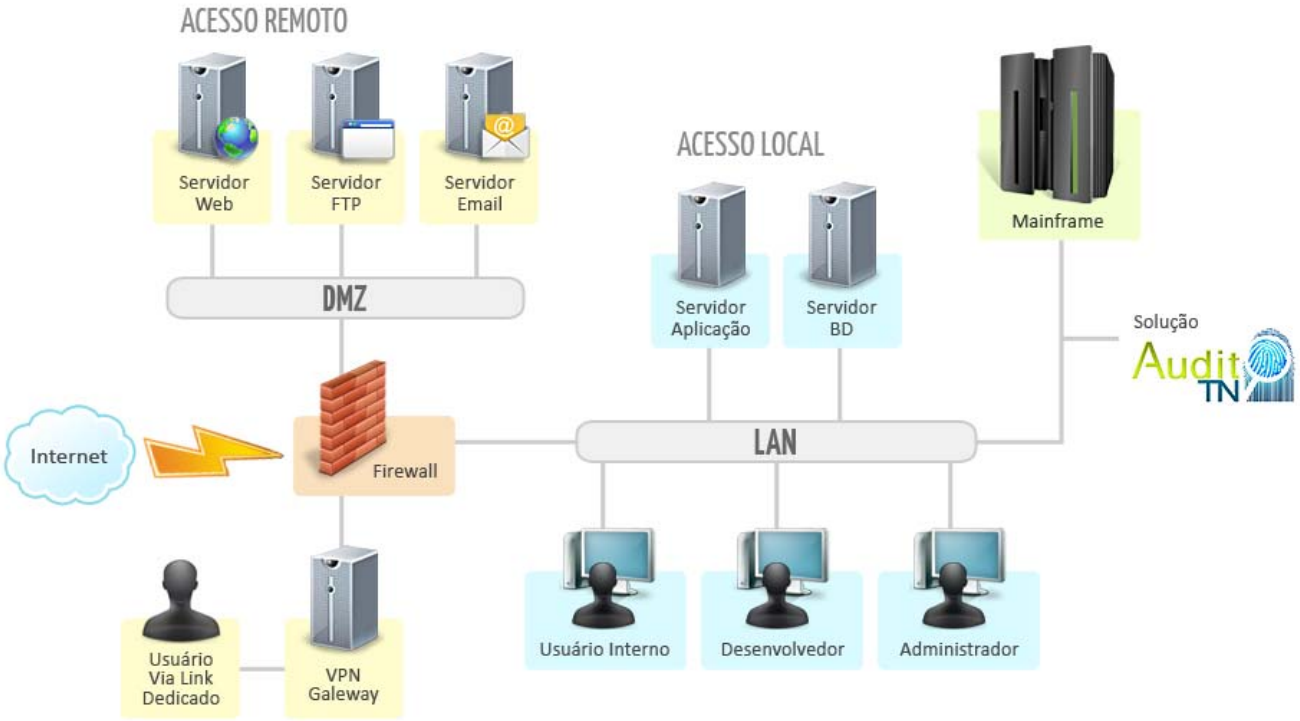
Vulnerabilidades monitoradas pelo Audit-TN:

Parceiros e Usuários Finais:
Gestão de acesso inconsistente no controle do que é acessado, por quem, de onde e quando.

Administradores de Sistemas:
Acesso total aos logs existentes e possibilidade de execução de qualquer operação não oficial no ambiente.

Desenvolvedores:
Acesso ao ambiente de produção para alteração nas bases de dados fora do horário para sustentação.

Ataques de "BRUTE FORCE":
Grandes massas de logins e senhas, com possibilidade de REVOKE dessas credenciais, simultaneamente, gerando aumento de consumo do RACF/Autenticador.



Características & Vantagens do Audit-TN:

- Captura do tráfego de acessos ao Mainframe.
- Arquivamento histórico e permanente, com indexação completa de ações TN3270 de todos os usuários do ambiente de mainframe.
- Fornece dados para geração de relatórios estatísticos e elaboração de matriz de tráfegos de acessos suspeitos/fraudulentos.
- Pesquisa indexada de metadados definidos (IP origem, IP destino, porta e hora).
- Consultas de Strings nos pacotes rastreados.
- Replay de telas originais e das ações de usuários efetuadas no Mainframe, incluindo recursos de avanço, retrocesso e pausa durante as reproduções.
- Geração de vídeos e relatórios para evidências de laudos forenses.
- Remontagem de sessões, possibilitando visualização e análise com sensibilidade idêntica ao usuário executor.
- Exportação de sessões em formato AVI, RTF , HTML e TXT incluindo teclas pressionadas e entradas dos usuário, além de informações sobre IPs e portas de origem e destino.
- Seleção e exportação simultânea de múltiplas sessões.
- Opção para visualização ou não de campos ocultos.
- Exportação de sessões em arquivos compactados.
- Preview de sessões nas telas de busca e opção simplificada para reprodução de sessões na tela do preview.
- Permitir a seleção e cópia dos campos na parte da listagem dos vídeos.
- Busca de sessões por string enviada do usuário para o mainframe ou vice-versa.
- Identificação e separação automática de início e fim de sessões.
- Proteção do sistema através de telas de autenticação.
- Scripts via linha de comando Windows para processamento offline.
- Geração de alertassobre eventos suspeitos.

Benefícios propostos:

Financeiro:

- Nenhum consumo de MIPs no mainframe.
- Desenvolvido para apoio nas decisões que previnam prejuízos com fraudes.

Segurança:

- Evidencia ações suspeitas e fraudulentas.
- Apoio na criação de mecanismos para restrição dessas ações.

Requisitos:

Auditor:

- Windows XP ou superior.
- Emulador de Terminal QWS3270 Plus (incluído na solução).

Servidor:

- Linux com MySQL.