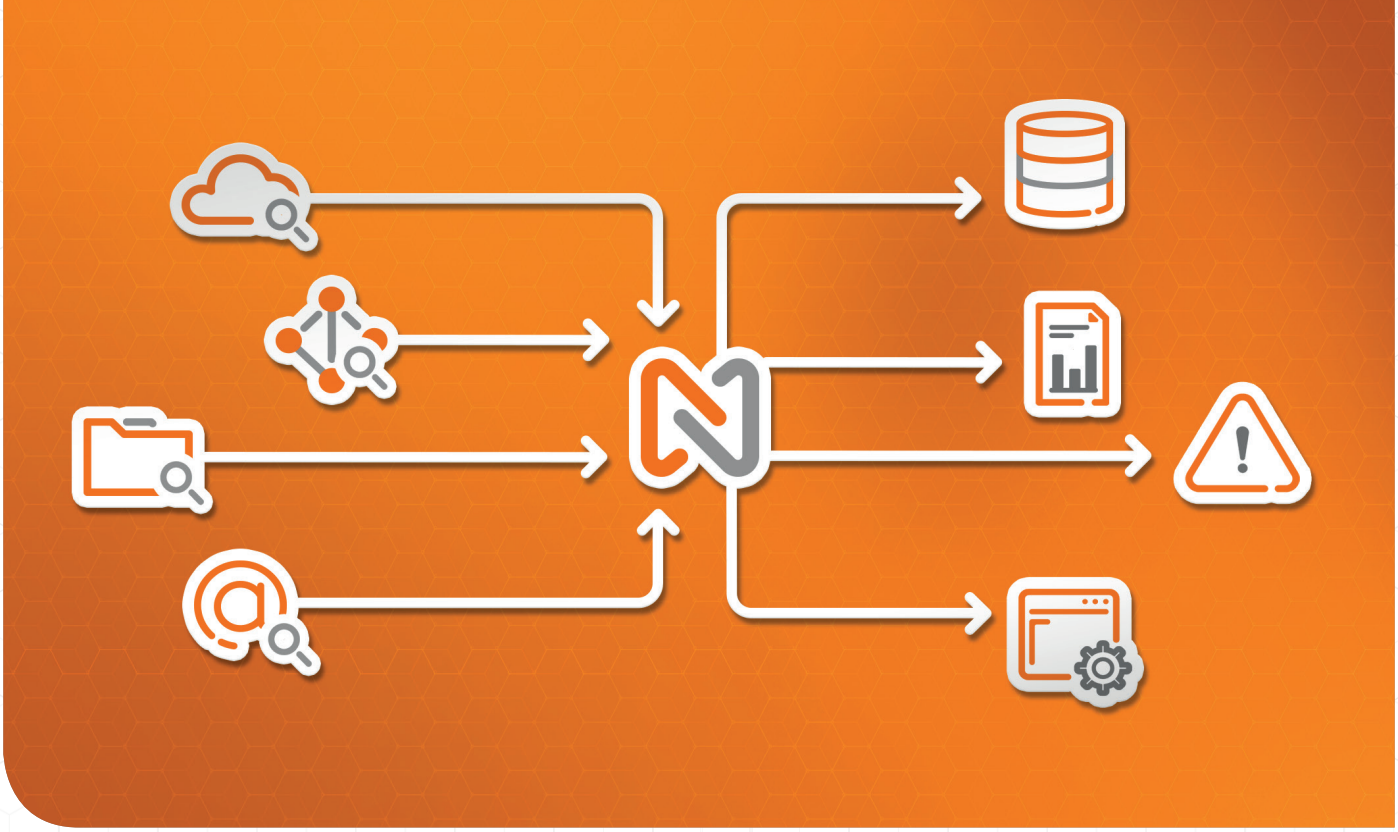
NetAdmin
AUDITORIA DE SISTEMAS



Visão geral

Os módulos de auditoria da plataforma NetAdmin coletam e normalizam os eventos gerados nos controladores de domínio, servidores de arquivos e serviços em nuvem.

Tanto as ações de usuários como as realizadas por administradores são registradas com os objetivos de comprovar autoria das ações, fornecer rastreabilidade de uso e detectar comportamentos atípicos que possam caracterizar ameaças internas a informações sensíveis.

As informações resultantes são disponibilizadas em variados relatórios, acessíveis por gestores e profissionais de segurança da informação.

Para cada plataforma gerenciada (Active Directory, servidores de arquivos e Office 365), existe um módulo específico para a coleta e normalização dos eventos de segurança. O módulo Security Incident Detection (SID) analisa os dados coletados pelos demais módulos, detectando situações adversas que representam possíveis ameaças ou vulnerabilidades. ■

Características gerais

Todos os módulos de auditoria NetAdmin possuem as seguintes características em comum:

Rastreabilidade de ações administrativas

Tratam das trilhas de auditoria geradas pelas ações dos administradores dos sistemas, independente da console utilizada. Essas são as ações mais críticas devido ao potencial impacto na segurança da informação.

Rastreabilidade de ações de usuários

Tratam das trilhas de auditoria geradas pelas ações dos usuários ao utilizarem os recursos computacionais cotidianamente. Essas trilhas de auditoria permitem identificar quais ações foram realizadas por cada usuário, com ou sem sucesso.

Coleta de eventos de diferentes fontes

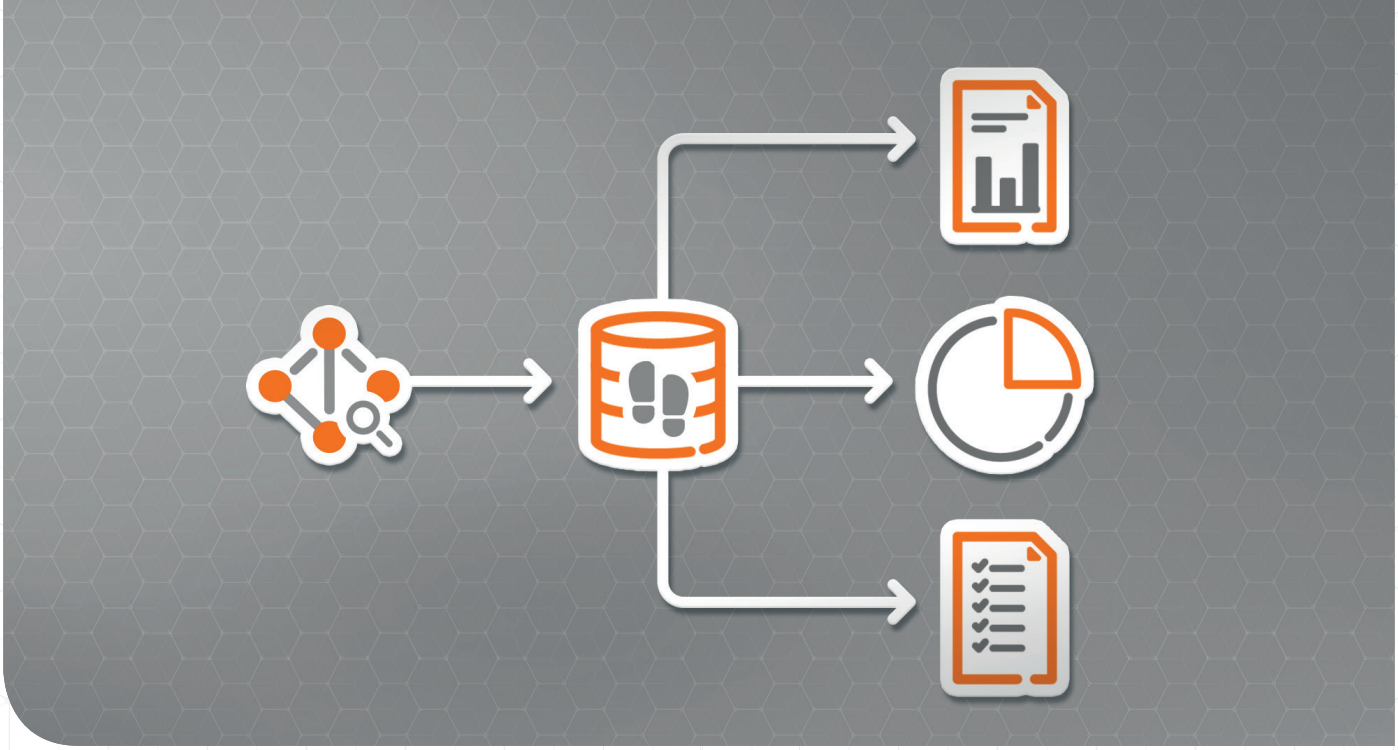
Capturam eventos originados em diferentes plataformas e normalizam os dados coletados para tratamento uniforme, sendo seus eventos elementares consolidados em ações compreensíveis. Os dados são filtrados para que apenas as informações relevantes sejam capturadas, descartando as desnecessárias.

Armazenamento otimizado dos dados

Armazenam os dados coletados em base de dados relacional local (*on-premises*) de forma a minimizar a utilização de espaço e aumentar a velocidade de consultas. Os registros que se tornam obsoletos com o tempo são removidos da base de dados, liberando espaço para novas informações.

Relatórios

Disponibilizam relatórios para gestores de forma simples e segura. Auxiliam na avaliação de *compliance* com as principais normas de segurança, sendo possível personalizá-los. Os relatórios permitem a exibição de dados em gráficos e texto de forma interativa. ■



ADA - Active Directory Auditing

Auditoria de Active Directory

O módulo ADA está na versão 1.2 e registra as ações realizadas no Microsoft Active Directory (AD) do Windows 2003 ou superior.

Suporta um grande número de controladores de domínio, podendo estar distribuídos em múltiplas localidades.

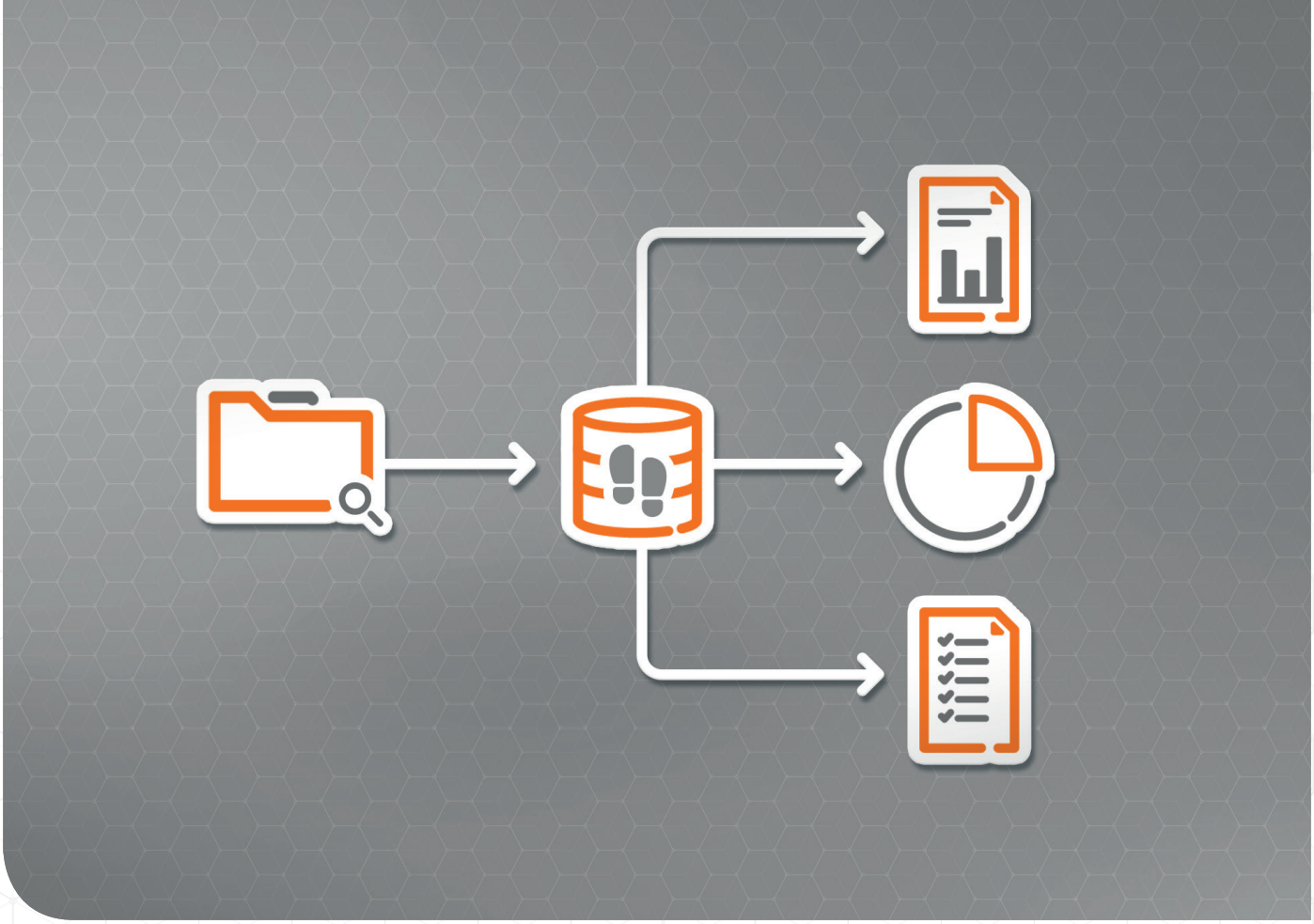
Não requer a instalação de agentes.

Exemplos de ações administrativas auditadas:

- Criação e exclusão de contas de usuários e computadores;
- Alteração de propriedade das contas;
- Alteração de políticas de segurança;
- Remoção e inclusão de membros nos grupos;
- Criação, renomeação e exclusão de grupos;
- Criação, exclusão ou alteração de OUs e GPOs;
- Demais alterações de configurações no AD;
- Alterações de registros DNS, de zonas integradas ao AD.

Exemplos de ações de usuários auditadas:

- *Logon* dos usuários;
- Erro de senha por parte do usuário;
- Bloqueio de contas após sucessivos erros de senha. ■



FSA- File Server Auditing

Auditoria de Servidor de Arquivos

O módulo FSA está na versão 1.9 e registra as ações realizadas em servidores de arquivos.

Possui versões específicas para as plataformas Windows 2003 ou superior, NetApp, SAMBA e EMC.

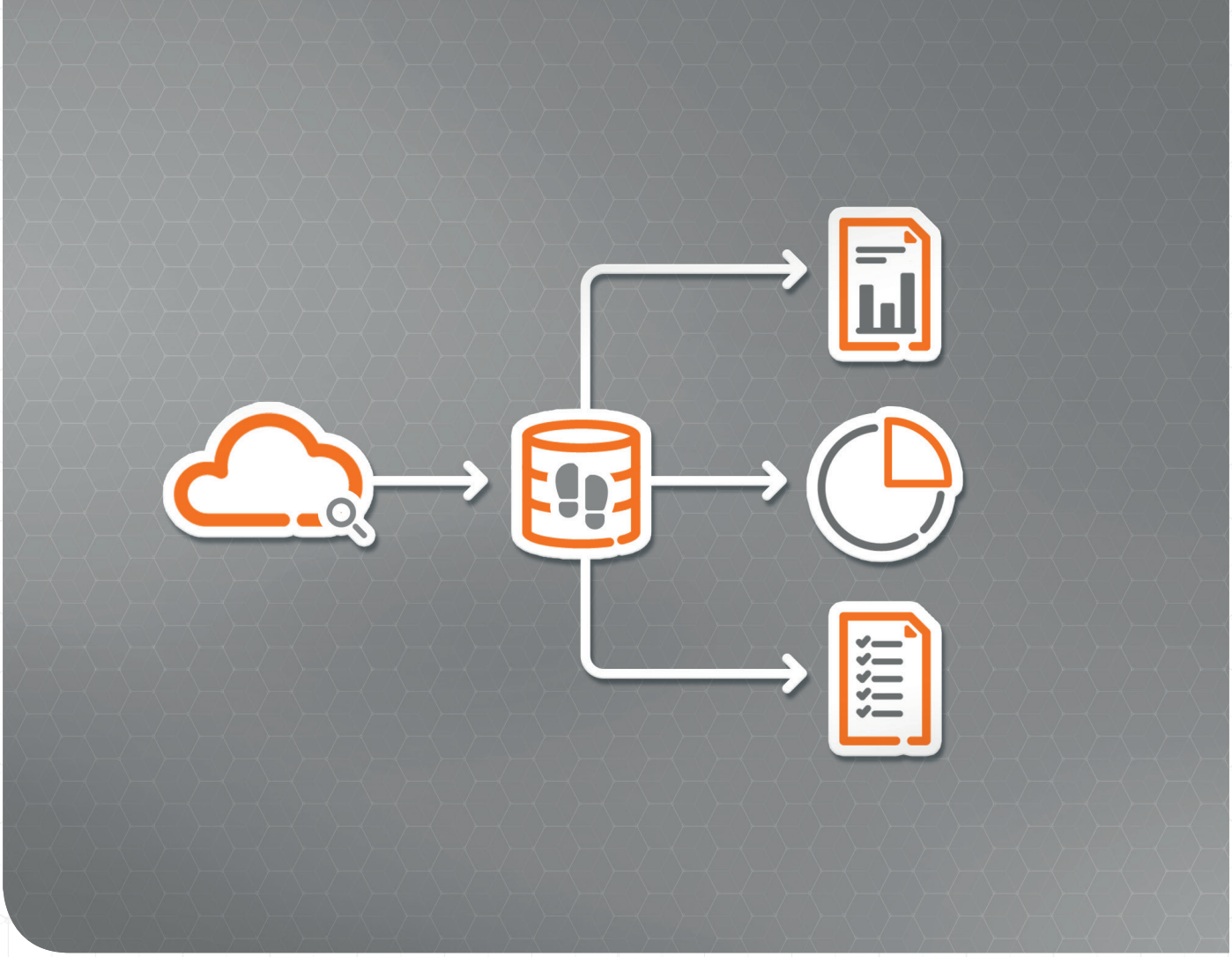
Permite classificar as pastas por nível de confidencialidade e configurar automaticamente a auditoria de acordo com a sensibilidade dos dados.

Exemplos de ações administrativas auditadas:

- Alteração de permissões em pastas;
- Alteração de compartilhamentos.

Exemplos de ações de usuários auditadas em arquivos e pastas:

- Criação;
- Exclusão;
- Modificação;
- Renomeação;
- Abertura/Leitura;
- Cópia/Movimentação. ■



OFA - Office 365 Auditing

Auditoria de Office 365

O módulo OFA está na versão 1.1 e registra as ações realizadas no Microsoft Office 365.

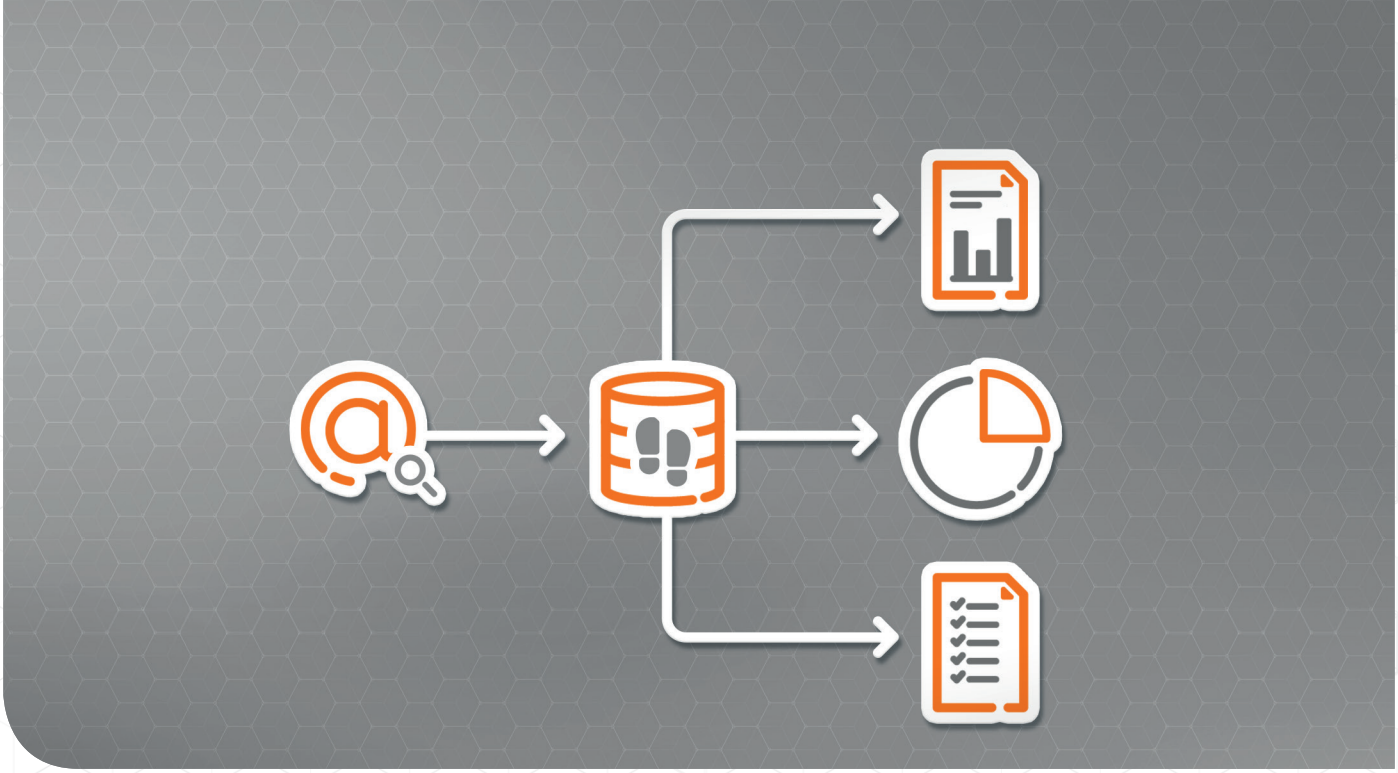
Trata as trilhas de auditoria geradas no Azure AD, Exchange Online e SharePoint Online.

Exemplos de ações administrativas auditadas:

- Criação e modificação de contas de usuários, grupos e caixas postais;
- Criação de grupos de distribuição;
- Criação de pastas e alteração de permissões no SharePoint Online.

Exemplos de ações de usuários auditadas:

- Acesso a caixas postais;
- Envio de e-mails;
- Autenticação no Azure AD;
- Registro de informações sobre as mensagens trafegadas na organização;
- Criação, alteração e exclusão de conteúdo das pastas no SharePoint. ■



EXA - Exchange Server Auditing

Auditoria de Servidor Exchange

O módulo EXA está na versão 1.0 e registra as ações realizadas nos servidores Microsoft Exchange 2010 ou superior.

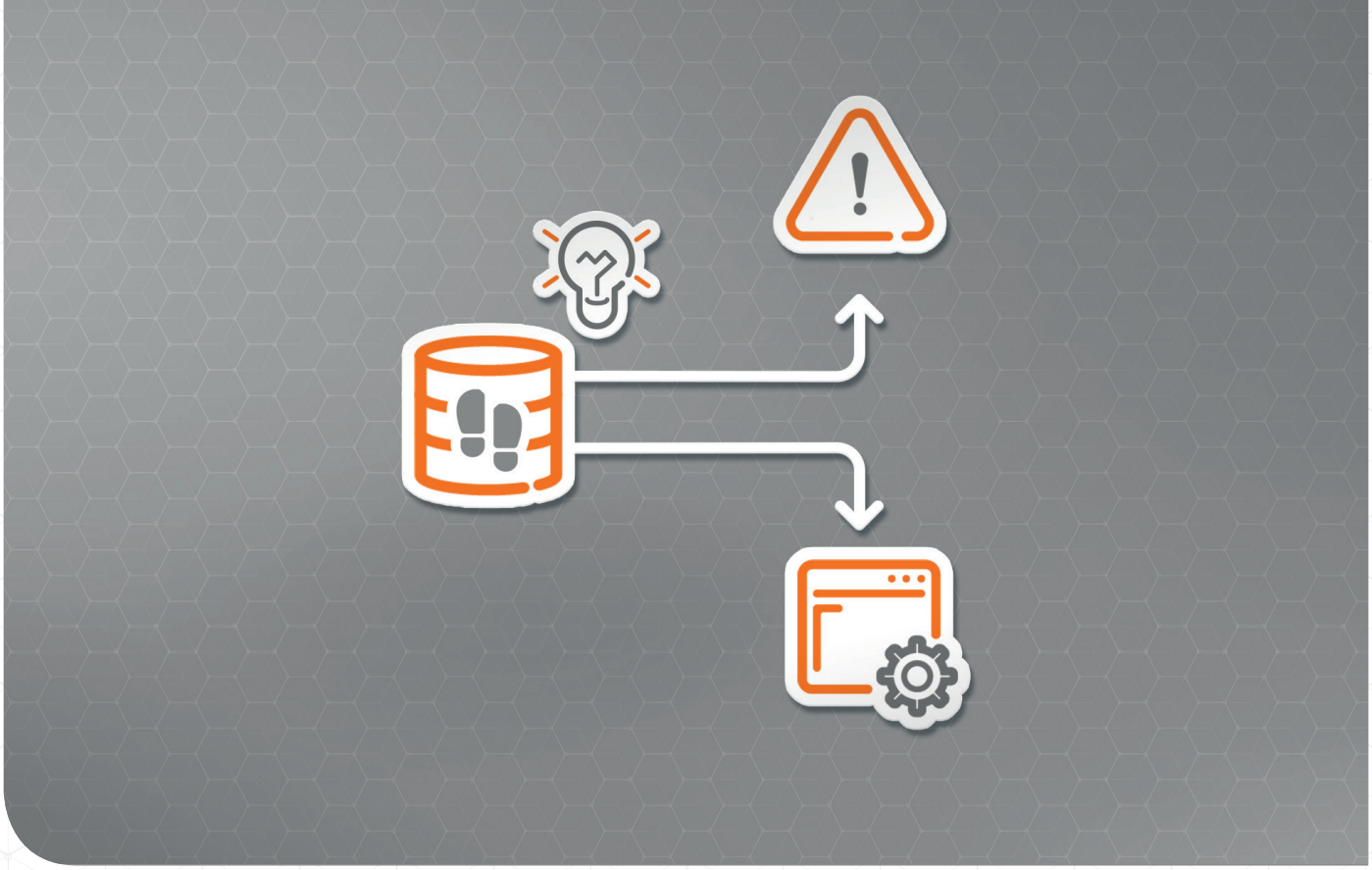
Trata as ações realizadas sobre as caixas postais, informações sobre as mensagens trafegadas na organização e logs de protocolos.

Exemplos de ações administrativas auditadas:

- Criação e exclusão de caixas postais;
- Alteração de propriedades das caixas postais;
- Alteração de configurações do servidor Exchange;
- Demais comandos realizados através da console PowerShell e outras interfaces de gerenciamento.

Exemplos de ações de usuários auditadas:

- Envio e recebimento de mensagens;
- Abertura de caixa postal;
- Remoção e cópia de mensagens;
- Abertura de mensagens;
- Exclusão de mensagens;
- Criação e exclusão de itens da caixa postal;
- Envio de mensagens com permissão "em nome de" (*send on behalf*);
- Envio de mensagens com permissão "enviar como" (*send as*). ■



SID - Security Incident Detection

Detecção de incidentes de segurança

O módulo SID está na versão 1.1 e atua em conjunto com os módulos Active Directory Auditing (ADA), File Server Auditing (FSA), Exchange Server Auditing (EXA) e Office 365 Auditing (OFA). Analisa em tempo real os eventos gerados e detecta situações adversas que representam possíveis ameaças ou vulnerabilidades.

O SID correlaciona os eventos e suas séries históricas utilizando algoritmos disponíveis em uma base de conhecimento, detectando comportamentos suspeitos que poderão ativar alertas e propor correções. Tal análise pode ser focada em determinado usuário ou recurso sensível, como uma pasta no servidor de arquivos ou caixa postal.

Os incidentes detectados podem ser enviados por e-mail ou SMS, apresentados em um *dashboard* ou encaminhados para sistemas SIEM.

São exemplos de incidentes identificados pelo SID:

- *Logon* simultâneo de uma mesma conta em vários computadores;
- Inclusão de usuário em um grupo de segurança restrito;
- Envio de grande volume de e-mails para um único destinatário externo;
- Concessão de permissão a si mesmo em caixa postal de outra pessoa;
- Suspeita de *ransomware* provocada por alteração massiva de arquivos;
- Modificação em GPOs críticas;
- Utilização de conta de serviço para *logon* interativo. ■

Conheça outras soluções da NetAdmin

NetAdmin é uma plataforma composta por módulos voltados para segurança, produtividade e conformidade na administração e operação em Tecnologia da Informação (TI).

Gerenciamento de Sistemas

- ADM - Active Directory Management
- FSM - File Server Management
- OFM - Office 365 Management

Auditoria de Sistemas

- ADA - Active Directory Auditing
- FSA - File Server Auditing
- OFA - Office 365 Auditing
- EXA - Exchange Server Auditing
- SID - Security Incident Detection

Gerenciamento de Identidade e Acesso

- IAM – Identity and Access Management

NetAdmin
SOFTWARE

AUDITORIA DE SISTEMAS

Versão Julho 2019 • © Copyright 2003 - 2019

NetAdmin é marca registrada da NetAdmin Software. Active Directory, Office 365, Windows, Azure, SharePoint Online, Microsoft e PowerShell são marcas registradas da Microsoft Corporation. EMC é marca registrada da DELL Corporation. NetApp é marca registrada da NetApp Corporation. SAMBA é uma reimplementação do protocolo de rede SMB. Todos os demais produtos descritos neste material são marcas registradas de seus respectivos proprietários.

www.netadmin.software