



[Nível 3] Auditoria Administrativa e Logs de Segurança

Guia Oficial iT Guys

Público Alvo: Segurança / Auditoria

Objetivo: Descobrir "Quem fez o que" no servidor.

Introdução

O Exchange registra **cada comando PowerShell** executado, seja por um administrador via Shell ou via interface ECP (a interface web apenas roda comandos PowerShell por trás).

Buscando Eventos (Search-AdminAuditLog)

Exemplo 1: Quem mexeu na caixa do Diretor?

Procurar qualquer alteração feita na caixa "diretor@itguys.com.br" nos últimos 30 dias.

```
Search-AdminAuditLog -StartDate (Get-Date).AddDays(-30) -ObjectIds "diretor"
```

Exemplo 2: Quem deu permissão de "FullAccess"?

Procurar comandos específicos (`Add-MailboxPermission`).

```
Search-AdminAuditLog -Cmdlets Add-MailboxPermission -StartDate (Get-Date).AddDays(-7)
```

Exemplo 3: Quem apagou uma caixa?

Comandos de remoção (`Remove-Mailbox`).

```
Search-AdminAuditLog -Cmdlets Remove-Mailbox
```

Interpretando o Resultado

- **Caller:** O usuário (admin) que executou a ação.
- **CmdletName:** O comando rodado.
- **ObjectModified:** Qual objeto foi alterado.
- **CmdletParameters:** Os parâmetros usados (ex: qual permissão foi dada).

Dica de Exportação

Para ler melhor, exporte para HTML ou CSV.

```
Search-AdminAuditLog ... | New-AdminAuditLogSearch -Name "Auditoria_Diretor" -Emails  
"seu.email@itguys.com.br"
```

(Isso enviará um relatório XML por e-mail para você).
_