CENTRO PAULA SOUZA GOVERNO DO ESTADO DE SÃO PAULO

Professor:	Disciplina:
Aluno:	Número:
Data:	Conceito:

Auditoria de Conformidade e Análise de Logs de Backups

A tarefa é usar o Documento de Especificação de Auditoria e as regras de alerta para analisar um conjunto de logs e verificar se o sistema de auditoria* está funcionando corretamente.

*Script java passado em aula

1. Análise Regra por Regra

Você deve revisar o arquivo criado alertas_logbackup.log linha por linha após a execução do script em JAva , aplicando as regras R01 e R02 e R03,manualmente para determinar se o sistema de auditoria agiu corretamente.

- R01 Falha de Execução O nível da linha é ERROR e a mensagem contém "Falha ao realizar o backup."
- R02 Atraso de Execução O intervalo entre duas linhas de "Backup iniciado." consecutivas for maior que 2 horas (02:00:00).
- R03 Log Malformado A linha de log não segue o Padrão de Linha ou o LEVEL não é INFO ou ERROR.

Conforme exemplo abaixo:

Evento	Timestamp de Início	Último Início Válido	Intervalo (H:M:S)	Regra Violada?	Alerta Manual (Sim/Não)	Alerta no Relatório (Sim/Não)	Conclusão (OK/Erro)
Falha	03:05:00	N/A	N/A	R01	Sim	...	...
Início	05:00:00	03:00:00	02:00:00	Nenhuma	Não	...	...
Início	09:30:00	07:00:00	02:30:00	R02	Sim	...	...
Falha	11:40:00	N/A	N/A	R01	Sim	...	...
Início	18:00:00	12:00:00	06:00:00	R02	Sim	...	...
(... e assim por diante para todas as linhas de início e erro)							

Proposta de Melhoria

Você um sistema que monitora processos automatizados (como backup, deploy ou atualização). Esse sistema já possui algumas regras de auditoria, e você deve criar uma nova regra, seguindo a lógica do exemplo abaixo:

Exemplo:
R04 — Falhas Frequentes: Disparar alerta caso mais de 3 falhas ocorram dentro de um período de 4 horas.

Crie uma nova regra de auditoria que ainda não existe no sistema.

Depois, você deve documentar conforme o padrão abaixo:

1. ID e Nome da Regra

2. Condição de Disparo (em linguagem natural, sem código)
   Explique quando essa regra deve ativar o alerta.

3. Mensagem de Alerta que o sistema exibirá

4. Onde essa regra seria registrada no arquivo logbackup.log
   Especifique qual tipo de registro ou linha do log acionaria a regra.