Programa de Estágio Tempest 2023.2 - Teste Técnico

SOC DPM - Security Operations Center Data Platforms

Nesta seção estão as questões específicas para a área de SOC DPM

- Security Operations Center Data Platforms.

31. Selecione abaixo os estágios de envelhecimento dos dados em um indexador por padrão: *

- ( ) Warm Bucket -> Hot Bucket -> Thawed Bucket -> Cold Bucket -> Frozen Bucket
- ( ) Warm Bucket -> Hot Bucket -> Thawed Bucket -> Frozen Bucket -> Cold Bucket
- (•) Hot Bucket -> Warm Bucket -> Cold Bucket -> Frozen Bucket -> Thawed Bucket
- ( ) Hot Bucket -> Warm Bucket -> Frozen Bucket -> Thawed Bucket -> Cold Bucket
- ( ) Hot Bucket -> Cold Bucket -> Warm Bucket -> Frozen Bucket -> Thawed Bucket

32. Quais os comandos para iniciar e parar o SIEM Splunk no modo CLI? *

- ( ) --splunk start | --splunk stop
- ( ) -spl start | -spl stop
- ( ) .splunk start | .splunk stop
- (•) .//splunk start | .//splunk stop
- ( ) ./splunk start | ./splunk stop -

33. Qual das portas padrões do Splunk abaixo é utilizado para obtenção de dados (coleta): *

- (•) 9997
- ( ) 8080
- ( ) 8000
- ( ) 514

34. Em quais arquivos .conf é realizada a configuração para exclusão de eventos (selecione duas alternativas): *

- [x] props.conf
- [ ] indexes.conf
- [ ] inputs.conf
- [x] transforms.conf
- [ ] server.conf

35. Selecione abaixo o comando utilizado para que o Splunk inicialize automaticamente caso o SO seja reinicializado: *

- (•) $SPLUNK_HOME/bin/splunk enable boot-start
- ( ) $SPLUNK_HOME/bin/splunk enable boot-active
- ( ) $SPLUNK_HOME/bin/splunk start boot-active
- ( ) $SPLUNK_HOME/bin/splunk boot-start active
- ( ) $SPLUNK_HOME/bin/splunk active boot-start

36. Em qual arquivo no Splunk é realizada a ofuscação de um trecho de log? *

- (•) props.conf
- ( ) outputs.conf
- ( ) authorize.conf
- ( ) transforms.conf
- ( ) tags.conf

37. Cite por qual objeto é possível controlar o espaço em disco usado por uma determinada fonte de dados: *

- ( ) host
- ( ) sourcetype
- (•) index
- ( ) source

38. Selecione a regex correta para extração de um endereço IPv4 em um log XPTO: (selecione duas opções) *

- [ ] rex field=_raw "(?<ip_address>\d+\.\d+\.\d+\.\d+)"
- [x] rex field= raw "(?<ip_address>\d+\.\d+\.\d+\.\d+)"
- [ ] rex field=_raw "(<ip_address>\d+\.\d+\.\d+\.\d+)"
- [ ] rex field=_raw "(?[ip_address]\d+\.\d+\.\d+\.\d+)"
- [x] rex field=_raw "(?<ip_address>([0-9]{1,3}[\.]){3}[0-9]{1,3})"

Voltar Próxima Limpar formulário