

BANCO DE DESENVOLVIMENTO DO ESPÍRITO SANTO S.A

Pregão BANDES Eletrônico Nº 2023/012

ESCLARECIMENTO 07

OBJETO: Contratação de empresa especializada para fornecimento de soluções de antimalware de próxima geração (NGAV), solução para detecção e resposta a ameaças (EDR), implementação, serviços gerenciados de segurança com resposta a incidentes, suporte técnico ilimitado 8x5, proteção 24x7x365 e garantia de atualização para 380 endpoints, durante o período de 24 meses, conforme especificações estabelecidas neste Edital e de seus Anexos.

“6.2. DETALHAMENTO DO MÓDULO ENDPOINT DETECTION AND RESPONSE (EDR):

6.2.1. Deve possuir a capacidade de realizar uma conexão remota nas máquinas através da console de gerenciamento para coletar arquivos de logs para análise forense;”

Pergunta Nº 1

Levando em consideração o item acima, é válido entregar essa COLETA DE LOGS diretamente da gerência centralizada sem a necessidade de acesso remoto e com uma aba específica que exibe os logs de todos os agentes em execução, permitindo a exibição de relatório forense e filtro por dispositivo?

Resposta do BANDES:

A gestão das ameaças será feita externamente pelo terceiro, portanto, os logs coletados dos dispositivos devem ser enviados automaticamente para fora de alguma maneira e de forma segura.

Pergunta Nº 2

Entendemos que a coleta de log está relacionada ao que o agente de AV registra da atividade da estação de trabalho e não de qualquer outra função que fuja da atividade do antivírus, está correto o nosso entendimento?

Resposta do BANDES:

Está correto o entendimento.

Vitória, 13 de julho de 2023.

Andressa Maria Gujansky Santana dos Santos
Pregoeira – BANDES