Amanda da Solidade Silva

De: Amanda da Solidade Silva em nome de Comissão Permanente de Licitação
Enviado em: segunda-feira, 4 de janeiro de 2021 09:49
Para: 'ney.santos@globalip.com.br'
Assunto: ENC: Pregão 19/20 - Registro de Preço - Endpoint - QUESTIONAMENTO

Prezado licitante,

Segue respostas dos questionamentos, referentes ao Pregão 19/2020.

Atenciosamente,
Amanda
CPL

De: Marcelo Dias de Sá
Enviada em: segunda-feira, 4 de janeiro de 2021 09:45
Para: Comissão Permanente de Licitação <cpl@funasa.gov.br>; Darlan Henrique da Silva Venturelli <darlan.venturelli@funasa.gov.br>; CGMTI <cgmti.assessoria@funasa.gov.br>
Assunto: RES: Pregão 19/20 - Registro de Preço - Endpoint - QUESTIONAMENTO

Prezada CPL,

Segue abaixo as respostas dos questionamentos,

Questionamento item 3.30 , 3.31 e item 5

"3.30. IPS/IDS integrado à solução de antivírus e gerenciado de forma centralizada;
3.31. O IPS/IDS deverá proteger contra exploração de vulnerabilidades de softwares;
5. Módulo para proteção de vulnerabilidades e Host IPS (HIPS) 5.1. Todas as regras das funcionalidades de Host IPS ……."

Conforme edital os item 3.30 e 3.31 descrevem funcionalidades de IPS/IDS, essas soluções são focadas em combater ameaças com assinaturas reconhecidas, entretanto a nova geração de Endpoint está baseada em ameaças com assinaturas reconhecidas e não reconhecidas, realizadas através de análise comportamental e inteligência artificial, o que por sua vez proporciona maior segurança aos dispositivos. A solução baseada em políticas para detectar e impedir a comunicação por processos com comandos maliciosos, monitorando todo o tráfego da rede vindo de todos os processos executados no endpoint ações baseadas em assinaturas conhecidas e não conhecidas. A solução de endpoint EDR acrescenta ao modelo tradicional uma análise comportamental e inteligência artificial , além das assinaturas reconhecidas e não conhecidas, a qual é superior a solução de IPS/IDS nos endpoints.
Desta forma podemos entender que uma solução que execute funcionalidades superior à solicitada nos itens será aceita ?
Resposta: O entendimento está correto.

Questionamento item 8.2

"8.2. Sandbox customizada do tipo On-Premise com hardware físico homologado pelo fabricante ou em máquina virtual local;"

As funcionalidades a serem desempenhadas pelo sandbox são baseadas em análise de artefatos. Essa atividade é mensuradas por quantidade de artefatos(arquivos) a serem emulados, analisados e executada

a extração da ameaça, quando houver, recentemente vários órgão migraram de uma rede corporativa para vários clientes remotos, o que ampliou a carga de tentativas de invasões vindas de diversos hosts externos.

Dependendo da quantidade de hosts externos e internos enviando requisições ao Gateway Sandbox isso pode gerar gargalos na entrega das requisições , essa quantidade poderá gerar latência na rede corporativa, ocasionando uma demora na entrega do artefato ao usuário final, gerando uma impressão de lentidão das análises Dada a flexibilidade do Gateway Sandbox em nuvem privada essa deficiência não ocorre .

Acretitamos que a solicitação de Sandbox on-premise ou em máquina virtual no cliente bisa garantir o não vazamento de informações sensíveis de artefato(arquivo) , contudo não evita o vazamento das informações pois os artefatos trafegarão necessariamente por uma rede que o órgão não possui controle .

A checkpoint possui sandbox gateway com emulação em nuvem proprietária e privada com a certificado NBA - que garante total confidencialidade dos artefatos analisados nesta rede , proporcionando assim uma entrega mais ágil para seus clientes dos artefatos apresentados , devido ao seu alto grau de engenharia nas análises .

Desta forma uma solução de Sandbox em nuvem proprietária no fabricante o qual atende às funcionalidades de análise, monitoramento, alerta e extração de ameaças será aceita?

Resposta: O entendimento está incorreto.

Atenciosamwnte,

De: Adalberto Caetano Lopes em nome de Comissão Permanente de Licitação
Enviado: quinta-feira, 31 de dezembro de 2020 9:28
Para: Darlan Henrique da Silva Venturelli; CGMTI; Marcelo Dias de Sá
Assunto: ENC: Pregão 19/20 - Registro de Preço - Endpoint - QUESTIONAMENTO

Bom dia,

Segue pedido de esclarecimento,

Adalberto Caetano
CPL

De: Ney Santos [mailto:ney.santos@globalip.com.br]
Enviada em: quarta-feira, 30 de dezembro de 2020 16:20
Para: Comissão Permanente de Licitação <cpl@funasa.gov.br>
Assunto: Pregão 19/20 - Registro de Preço - Endpoint - QUESTIONAMENTO

Prezado Pregoeiro ,

Segue pedido de esclarecimento do Pregão 19/20 .

Questionamento item 3.30 , 3.31 e item 5

“3.30. IPS/IDS integrado à solução de antivírus e gerenciado de forma centralizada;
3.31. O IPS/IDS deverá proteger contra exploração de vulnerabilidades de softwares;
5. Módulo para proteção de vulnerabilidades e Host IPS (HIPS) 5.1. Todas as regras das funcionalidades de Host IPS …….”

Conforme edital os item 3.30 e 3.31 descrevem funcionalidades de IPS/IDS, essas soluções são focadas em combater ameaças com assinaturas reconhecidas, entretanto a nova geração de Endpoint está baseada em ameaças com assinaturas reconhecidas e não reconhecidas, realizadas através de análise comportamental e inteligência artificial, o que por sua vez proporciona maior segurança aos dispositivos. A solução baseada em políticas para detectar e impedir a comunicação por processos com comandos maliciosos, monitorando todo o tráfego da rede vindo de todos os processos executados no endpoint ações baseadas em assinaturas conhecidas e não conhecidas. A solução de endpoint EDR acrescenta ao modelo tradicional uma análise comportamental e inteligência artificial , além das assinaturas reconhecidas e não conhecidas, a qual é superior a solução de IPS/IDS nos endpoints.
Desta forma podemos entender que uma solução que execute funcionalidades superior à solicitada nos itens será aceita ?

Questionamento item 8.2

“8.2. Sandbox customizada do tipo On-Premise com hardware físico homologado pelo fabricante ou em máquina virtual local;”

As funcionalidades a serem desempenhadas pelo sandbox são baseadas em análise de artefatos. Essa atividade é mensuradas por quantidade de artefatos(arquivos) a serem emulados, analisados e executada a extração da ameaça, quando houver, recentemente vários órgão migraram de uma rede corporativa para vários clientes remotos, o que ampliou a carga de tentativas de invasões vindas de diversos hosts externos.

Dependendo da quantidade de hosts externos e internos enviando requisições ao Gateway Sandbox isso pode gerar gargalos na entrega das requisições , essa quantidade poderá gerar latência na rede corporativa, ocasionando uma demora na entrega do artefato ao usuário final, gerando uma impressão de lentidão das análises Dada a flexibilidade do Gateway Sandbox em nuvem privada essa deficiência não ocorre .

Acretitamos que a solicitação de Sandbox on-premise ou em máquina virtual no cliente bisa garantir o não vazamento de informações sensíveis de artefato(arquivo) , contudo não evita o vazamento das informações pois os artefatos trafegarão necessariamente por uma rede que o órgão não possui controle .

A checkpoint possui sandbox gateway com emulação em nuvem proprietária e privada com a certificado NBA - que garante total confidencialidade dos artefatos analisados nesta rede , proporcionando assim uma entrega mais ágil para seus clientes dos artefatos apresentados , devido ao seu alto grau de engenharia nas análises .

Desta forma uma solução de Sandbox em nuvem proprietária no fabricante o qual atende às funcionalidades de análise, monitoramento, alerta e extração de ameaças será aceita?

--
Atenciosamente,

Ney Santos

Gerente de Contas Governo
Divisão de Inteligência e Anti Fraude
Global IP Tecnologia da Informação
SCN Qd. 4 Bl. B Cobertura Pétala D sala 1404
E-mail : ney.santos@globalip.com.br
061 3327 2777 061 99333 0202

--
Atenciosamente,

Ney Santos
Gerente de Contas
Divisão de Inteligência e Anti Fraude
Global IP Tecnologia da Informação
SCN Qd. 4 Bl. B Cobertura Pétala D sala 1404
E-mail : ney.santos@globalip.com.br
061 3327 2777 061 99333 0202