ANEXO A4

Solución de Orquestación de Seguridad, Automatización y Respuesta (SOAR)

MARCA	
MODELO	
NUMERO DE PARTE DEL FABRICANTE	
CANTIDAD	

Característica	**Fuente (**Folletos, brochures, certificados, enlaces web, catálogos, instructivos, hojas de datos y/o manuales técnicos, o carta del fabricante.**)**	**Pág.**	**Ítem, numeral, capítulo de la pagina**	**Indicar texto o párrafo donde se evidencie cumplimiento de la característica solicita.**
Solución de Orquestación de Seguridad, Automatización y Respuesta (SOAR)				
1. Debe incluir una tecnología SOAR para la automatización de respuesta ante incidentes. Esta tecnología deberá ser totalmente integrable con soluciones SIEM.				
2. Debe automatizar las tareas básicas de respuesta a incidentes, haciendo que sus analistas sean más eficientes y efectivos.				
3. La automatización se debe lograr utilizando flujos de trabajo modulares y scripts.				
4. Debe ser compatible con Python y JavaScript, debe tener la capacidad de exportar paquetes de Python a Dockers (de preferencia) o contenedores para que librerías de Python existentes puedan ser reutilizadas.				
5. Debe incluir una función "BYOI" o similar que permita a los analistas escribir sus propias integraciones a través de un SDK interno y un wizard.				

6. La ejecución de los playbooks y la actividad relacionada por el analista debe ser automáticamente documentada para cada incidente de seguridad.				
7. Debe poseer la capacidad de asignar a cualquiera de los usuarios disponibles en el sistema basado en las capacidades RBAC				
8. La herramienta debe tener un API capaz de ejecutar las mismas funciones que la interfaz gráfica.				

Solución de Actualizaciones y Distribuciones de Software

MARCA	
MODELO	
NUMERO DE PARTE DEL FABRICANTE	
CANTIDAD	

Característica	**Fuente (**Folletos, brochures, certificados, enlaces web, catálogos, instructivos, hojas de datos y/o manuales técnicos, o carta del fabricante.**)**	**Pág.**	**Ítem, numeral, capítulo de la pagina**	**Indicar texto o párrafo donde se evidencie cumplimiento de la característica solicita.**
Solución de Actualizaciones y Distribuciones de Software				
A. Características Generales				
1. Debe construir un perfil detallado de software y hardware instalado, inventario de red, parches faltantes de Microsoft, estado del antivirus (opcional), criterios de seguridad				
2. Debe detectar actualizaciones pendientes como mínimo para los siguientes tipos de software: • Sistemas Operativos (Windows 7, Windows 8.1, Windows 10, Red Hat Enterprice Linux). • Debe reconocer por lo menos 44 aplicaciones diferente, mínimamente que incluyan las siguientes: Microsoft Office, Adobe Reader, Adobe Acrobat Professional ,Adobe Air, Adobe Flash, Adobe Reader, Adobe Shockwave, Apache Tomcat, Apple iTunes, Citrix Receiver para Windows Enterprise, FileZilla Client, Foxit Enterprise Reader, Foxit Reader, Google Chrome, Mozilla Firefox, Mozilla Thunderbird, Notepad++, Oracle Java, QuickTime Player para Windows, RealPlayer, Skype, VLC Media Player,7-Zip,WinRAR, WinZip, Wireshark. Se aceptarán protocolos alternativos a DSSP para el monitoreo de sitios globales o geográficos.				
3. Debe poder integrarse al servidor de directorio.				
4. Debe poder integrarse a soluciones SIEMS. La Integración de la solución con el SIEM puede realizarse a nivel del sistema operativo donde se encuentra instalada la solución siempre y cuando los eventos generados por la solución y todos los componentes que la integren sean enviados al SIEM.				
5. Debe soportar instalar el agente como mínimo en sistemas operativos Windows 8.1, 10 y versiones de servidor como Windows 2012, 2016, 2019.				

6. Debe soportar instalar el agente como mínimo en sistemas Linux RHEL 6, 7 y superior. Se consideran como opcional para sistemas Linux RHEL 6				