Universidad Nacional de La Matanza

ANEXO CONVOCATORIA

22/2018

RENGLONES

Renglón	Especificación Técnica	Imagen
	1. La Solución deberá contar con: 1.1. Administración Centralizada 1.1.1. La solución deberá soportar administración centralizada con un mecanismo simple de licenciamiento 1.1.2. No se deberá necesitar implementar hardware adicional para la administración centralizada 1.1.3. La solución deberá soportar multi-tenancy vía dominios administrativos, al menos 4 por appliance y un hasta 64 1.1.4. La solución debe soportar administración RESTful API 1.1.5. Debe tener la capacidad de almacenar automáticamente copias de seguridad cifradas por contraseña de manera programada a través de FTP y SFTP 1.2. Detalles Técnicos 1.2.1. La solución debe ser virtual 1.2.2. Debe ser compatible con: VMware, Hyper-V, KVM, Citrix Xen Server y Open Source Xen 1.2.3. La solución debe tener un throughput mínimo de 500 Mbps 1.2.4. El throughput arriba mencionado, debe conseguirse con los siguientes recursos: 1.2.4.1. Hardware: 2x Intel Xeon E5504 2.0 GHz 4 MB de caché. 1.2.4.2. Hypervisor: VMware ESXi 5.5 con 4 GB de vRAM asignados a 4 vCPU y 8 vCPU Virtual Appliance y 4 GB de vRAM asignados a los 2 vCPU Virtual Appliance 1.3. Alta Disponibilidad 1.3.1. La solución debe estar disponible en failover activo / pasivo y activo / activo con modos de sincronización de configuración 1.3.2. La conmutación por error secundaria debe ser posible 1.3.3. Una solución de administración centralizada NO debería ser necesaria cuando se usa un grupo de unidades 1.3.4. Las unidades deben sincronizar los siguientes objetos: conjunto de reglas, políticas configuradas, objetos 1.3.5. La alta disponibilidad debe ser compatible con todos los modos de implementación en línea 1.3.6. Ambas unidades en una solución de alta disponibilidad activa / pasiva deben usar la misma dirección MAC y solo la unidad principal debe responder 1.3.7. La capacidad del clúster en una solución de alta disponibilidad activa / activa debería aumentar en un 50% al agregar hasta 8 miembros del clúster 2. Características de Seguridad 2.1. Modelo de seguridad positiva 2.1.1. Debe soportar un modelo de seguridad positiva. Describir como la solución lo proporciona 2.1.2. La solución no debe mover automáticamente los detalles aprendidos a la detección o prevención, ya que violaría las políticas de control de cambios en la mayoría de las empresas. En cambio, un administrador debe tener controles de implementación fáciles 2.1.3. Los detalles aprendidos deben ser ajustables para permitir el ajuste fino de las políticas aprendidas 2.1.4. Debe ser posible el despliegue y el aprendizaje de reglas de seguridad positivas a la vez que se siguen aplicando de manera agresiva las políticas negativas apropiadas. Durante el aprendizaje de este modelo de seguridad positivo, el nivel de seguridad no debería reducirse 2.1.5. No se debe forzar al administrador de la solución a elegir entre "activar / desactivar el aprendizaje" y/o "activar / desactivar la protección". Estos deberían coexistir 2.2. Modelo de seguridad negativa	

Universidad Nacional de La Matanza

Renglón	Especificación Técnica	Imagen
	3.2.1. La solución debe ofrecer un modelo de seguridad negativo 3.2.2. La base de firmas debe actualizarse automáticamente 3.2.3. Configuración por firma de excepciones 3.2.4. Se pueden crear excepciones a partir del archivo de registro 3.2.5. Las políticas predeterminadas deben estar disponibles en varias clasificaciones, solo alerta, seguridad media, alta seguridad 2.2.1. Las firmas deben agruparse lógicamente. La lista debe contener al menos: 2.2.1.1. Cross Site Scripting 2.2.1.2. SQL Injection 2.2.1.3. Generic Attacks 2.2.1.4. Known Exploits 2.2.1.5. Trojans 2.2.1.6. Information Disclosure 2.2.1.7. Bad Robot 2.2.1.8. Credit Card Detection 2.2.2. Las mediciones de falsos positivos deben estar disponibles para reducir o eliminarlos 2.2.2.1. La solución debe admitir medidas específicas de inyección SQL mediante mitigación falsa positiva o validación de sintaxis SQL 2.2.2.2. La solución debe admitir la detección basada en umbrales mediante asignaciones de peso personalizables en las firmas 2.3. Comunicaciones entre (XML Webservices) 2.3.1. La solución debe proveer filtrado y validación XML 2.4. Solución Anti-DoS 2.4.1. La solución debe ofrecer capacidades de DDoS en capa 7 2.4.2. La detención a nivel aplicaciones debe soportar: 2.4.2.1. HTTP request limitado por source 2.4.2.2. Conexiones TCP usando misma cookie 2.4.2.3. HTTP requests usando misma cookie 2.4.2.4. Un mecanismo de challenge-response, que será completamente transparente para el usuario final 2.4.2.5. Un mecanismo de challenge-response que desafíe activamente al usuario final 2.5. Anti-Virus y Malware 3.5.1. La solución debería ofrecer una solución de antivirus integrada 3.5.2. La base de datos del AV debe actualizarse automáticamente 3.5.3. La solución de AV debe tener revisiones públicas que rindan cuenta de altas calificaciones de efectividad con bajos falsos positivos de un proveedor independiente de pruebas AV de terceros 3.5.1. Las cargas de archivos deben estar restringidas en el tipo de archivo y tamaño del archivo 3.5.2. La solución AV NO debe introducir implementaciones adicionales de software o hardware ni requisitos de integración de terceros 3.5.3. Se debe admitir la exploración AV de las cargas de archivos adjuntos de correo desde dispositivos móviles por OWA y ActiveSync 3.5.4. La solución debe integrarse estrechamente con la solución de Sandboxing para la protección de carga de archivos y aprender de ella el contenido malicioso observado 2.6. Bot y Bad-IP detección y protección 3.6.1. La solución debe ser capaz de detectar y distinguir dos tipos de Bots: 3.6.1.1. Motores de búsqueda conocidos 3.6.1.2. Malos robots (escáneres, rastreadores, arañas) 3.6.2. La solución debe tener un tablero para mostrar las estadísticas de eventos de los clientes normales y basados en robots. 3.6.3. La solución debería proteger contra la baja reputación proveniente de botnets, proxy anónimo, escáneres, spammers, redes Tor, hosts de phishing 2.7. Tracking 2.7.1. La solución debe poder seguir, correlacionar e informar el tráfico 2.7.1.1. IP-address 2.7.1.2. User 2.7.1.3. Device 3.7.2. La solución debe poder proteger en función de la dirección IP del cliente proporcionado por el X-header 3.7.3. La solución debe poder insertar el encabezado X-Forwarded-For 3.7.4. La solución debe ser capaz de distinguir entre las direcciones IP de cliente único y compartido 3.7.5. La solución debe poder bloquear por dirección IP o sesión HTTP del cliente 2.8. Data Leak Prevention 2.8.1. La solución debe soportar al menos los siguientes tipos de Data Leak	

Universidad Nacional de La Matanza

Renglón	Especificación Técnica	Imagen
	Prevention: 2.8.1.1. PHP information leakages 2.8.1.2. IIS default location 2.8.1.3. Application Availability / Errors 2.8.1.4. File or Directory Names Leakage 2.8.1.5. ASP/JSP Source Code Leakage 2.8.1.6. SQL Errors Leakage 2.8.1.7. IIS Errors Leakage 2.8.1.8. Directory Listing 2.8.1.9. HTTP Header Leakage 2.8.1.10. Prevention of Error messages leakage 2.9. Prevención de robo de identidad 2.9.1. La solución debe prohibir el acceso autenticado a las credenciales conocidas filtradas públicamente de los principales sitios web de Internet (como haveibeenpwned.com) 2.10. Anti-Web Defacement 2.10.1. La solución debe tener la capacidad de prevenir, detectar y restaurar la desfiguración de la web. 2.10.2. La solución debe copiar el contenido del servidor web a su propio disco duro y compararlo en un cronograma definible si los archivos han sido cambiados en el servidor web. 2.10.3. Opcionalmente debería ser posible restaurar los archivos modificados. 2.10.4. Se deben admitir múltiples protocolos (FTP / SSH / Windows File Share) para maximizar la compatibilidad con la plataforma del servidor de destino. 2.11. Validación de cumplimiento HTTP RFC 2.11.1. La solución debe tener la opción de verificar estándares HTTP RFC. Los siguientes objetos debe ser revisados y aplicados: 2.11.2. Content Length 2.11.2.1. Content Length 2.11.2.2. Illegal Content Length 2.11.3. HTTP Header 2.11.3.1. Header Length 2.11.3.2. Header Name Length 2.11.3.3. Header Value Length 2.11.3.4. Illegal Character in Header Name 2.11.3.5. Illegal Character in Header Value 2.11.3.6. Redundant HTTP Headers 2.11.4. HTTP Parameter 2.11.4.1. Total URL Parameters Length 2.11.4.2. Total Body Parameters Length 2.11.4.3. Number of URL Parameters 2.11.4.4. NULL Character in Parameter Name 2.11.4.5. NULL Character in Parameter Value 2.11.4.6. Maximum URL Parameter Name Length 2.11.4.7. Maximum URL Parameter Value Length 2.11.4.8. Illegal Character in Parameter Name 2.11.4.9. Illegal Character in Parameter Value 2.11.4.10. Duplicate Parameter Name 2.11.5. HTTP Request 2.11.5.1. Illegal HTTP Request Method 2.11.5.2. HTTP Request Filename Length 2.11.5.3. HTTP Request Length 2.11.5.4. Number of Header Lines in Request 2.11.5.5. Missing Content Type 2.11.5.6. NULL Character in URL 2.11.5.7. Illegal Character in URL 2.11.5.8. Malformed URL 2.11.6. HTTP/2 Frame 2.11.6.1. Header Compression Table Size 2.11.6.2. Number of Concurrent Streams 2.11.6.3. Initial Window Size 2.11.6.4. Frame Size 2.11.6.5. Header List Size 2.11.7. Generic 2.11.7.1. Illegal Content Type 2.11.7.2. Illegal Response Code 2.11.7.3. Illegal Host Name 2.11.7.4. Illegal HTTP Version 2.11.7.5. Body Length	

Universidad Nacional de La Matanza

Renglón	Especificación Técnica	Imagen
	2.11.7.6. Number of Cookies in Request 2.11.7.7. Number of Ranges in Range Header 2.11.7.8. Malformed Request 2.11.7.9. WebSocket Protocol 2.11.7.10. Illegal Connection Preface 2.11.7.11. Illegal Frame Type 2.11.7.12. Illegal Frame Flags 2.11.7.13. Illegal Chunk Size 2.12. Seguridad en protocolos HTTP y HTTPS 2.12.1. La solución debe tener la opción de aplicar HSTS 2.12.2. La solución debe tener la opción de aplicar HPKP 2.12.3. La solución debe tener seguridad de cookies 2.12.3.1. Hacer cumplir la bandera HTTPOnly Cookie 2.12.3.2. Hacer cumplir la bandera Secure Cookie 2.13. Application Business Logic Enforcement 2.13.1. La solución debe ser capaz de aplicar las páginas de inicio 2.13.2. La solución debe ser capaz de aplicar la lógica de la aplicación definiendo un conjunto de reglas de acceso a la página 2.13.3. Los métodos apropiados de acceso deben ser aprendidos y exigibles por la solución 2.13.4. Los parámetros requeridos en una página URL dada deben ser aprendidos y exigibles por la solución 2.13.5. La solución debe poder rastrear el uso de cookies en una URL, con granularidad página por página 3. Características de Entrega de Aplicaciones 3.1. Protocolos Soportados 3.1.1. La solución debe soportar IPv4 e IPv6 3.1.2. Soporte de cliente IPv6 para despliegue lateral back-end de IPv4 3.1.3. La solución debe soportar HTTP/1.1 y HTTP/2 3.1.3.1. Soportar service delivery y seguridad en HTTP/1.1 y HTTP/2 3.1.3.2. Admitir el cliente HTTP / 2 para la implementación del lado del backend HTTP / 1.1 3.2. Balanceo de Carga 3.2.1. La solución debe ser capaz de balancear la carga del trafico protegido a varios servidores 3.2.2. Los siguientes algoritmos deben ser soportados 3.2.2.1. Round Robin 3.2.2.2. Weighted Round Robin 3.2.2.3. Least Connection 3.2.2.4. Source IP Hash 3.2.2.5. URI Hash 3.2.2.6. Full URI Hash 3.2.2.7. Host Hash 3.2.2.8. Host Domain Hash 3.2.3. La solución debe tener características de persistencia configurables para mantener las sesiones en los servidores de load balance 3.2.4. La solución debe ser capaz de soportar las siguientes Caracteristicas de persistencia: 3.2.4.1. Persistent IP (IPv4 and IPv6) 3.2.4.2. HTTP Header 3.2.4.3. URL parameter 3.2.4.4. Persistent Cookie 3.2.4.5. Insert Cookie 3.2.4.6. Rewrite Cookie 3.2.4.7. Embedded Cookie 3.2.4.8. ASP Session ID 3.2.4.9. PHP Session ID 3.2.4.10. JSP Session ID 3.2.4.11. SSL Session ID 3.3. Publicación de Aplicaciones 3.3.1. La solución debe ser capaz de publicar aplicaciones web y ofrecer acceso Single Sign On de fondo 3.3.2. Soporte estándar para aplicaciones comunes como: 3.3.2.1. Microsoft ActiveSync 3.3.2.2. Microsoft Outlook Web Access 3.3.2.3. Microsoft SharePoint 3.3.2.4. Microsoft Lync 3.4. Autenticación 3.4.1. La solución debe ser compatible con el método de autenticación de múltiples	

Universidad Nacional de La Matanza

Renglón	Especificación Técnica	Imagen
	clientes 3.4.1.1. Autenticación Básica 3.4.1.2. Autenticación basada en formularios 3.4.1.3. Autenticación de certificados de clientes 3.4.1.4. Autenticación SAML 3.4.2. La solución debe ser compatible con Authentication Delegation en servidores remotos 3.4.2.1. Kerberos Authentication, incluida la opción de servidor múltiple 3.4.3. La solución debe soportar Single Sign On 3.5. La solución debe soportar funciones de aceleración web 3.5.1.1. Caching 3.5.1.2. Compression 3.5.1.3. SSL offloading 4. Monitoreo y Reportes 4.1. Monitoreo 4.1.1. La solución debe tener un dashboard que muestre: 4.1.1.1. Uso de los recursos del sistema 4.1.1.2. Trafico en tiempo real, conexiones, ataques y respuesta de información 4.1.1.3. Servicios Web y el estado de los servidores de back-end 4.1.2. La solución debe tener una visión general de la topología del servicio web 4.1.3. Las soluciones deben tener una función de desglose durante al menos las últimas 24 horas en: 4.1.3.1. Seguridad por origen y amenazas 4.1.3.2. Transacciones de trafico por origen 4.1.3.3. Sesiones por origen y políticas 4.2. Logging y Reportes 4.2.1. La solución debe ser capaz de almacenar localmente la información del evento (auditoría) 4.2.2. La solución debe tener la capacidad de almacenar localmente las alertas 4.2.3. La solución debe tener la capacidad de almacenar localmente la información del tráfico 4.2.4. La solución debe poder enviar los 3 tipos de registros anteriores a un sistema de registro centralizado 4.2.5. La solución debe ser capaz de enviar todos los tipos de log anteriores, a un syslog externo 4.2.6. La información de alertas debe contener al menos la siguiente información: 4.2.6.1. Información de conexiones origen a destino 4.2.6.2. Amplia información del encabezado del paquete 4.2.6.3. Vista de parámetro completo 4.2.6.4. Destacando el ataque en el registro de ataque 4.2.6.5. Con las alertas de cookies, se muestra la cookie alertada y los valores modificados 4.2.6.6. La solución debe agregar el registro por día y por tipo de ataque 4.2.6.7. El registro debe mostrar tanto la codificación original como los valores decodificados para el análisis 4.3. Data Analytics 4.3.1. La solución debe tener un panel de análisis de datos en el que pueda ver: 4.3.1.1. Ataques por país 4.3.1.2. Hits por país 4.3.1.3. Datos por país 4.3.1.4. Exportar a PDF 4.3.1.5. Vista clickeable de varios ataques por sitio web 4.3.1.6. Mapa mundial con zoom y codificación de color de los ataques 4.4. Análisis Botnet 4.4.1. La solución debe tener una vista histórica de Botnets y motores de búsqueda 4.5. IP's Bloqueadas 4.5.1. La solución debe tener una vista de todas las direcciones IP bloqueadas y el periodo de bloqueo 4.5.2. Desde la vista anterior, debe ser posible liberar las direcciones IP bloqueadas 5. Compliance 5.1. La solución debe proteger contra amenazas comunes como las identificadas en el top 10 de OWASP 5.2. La solución debe ser certificada como "Recommended" por las pruebas independientes de NSS Lab's 5.3. La solución debe tener certificado ICSA 5.4. La solución debe cumplir con TAA 6. Soporte y Training 6.1. El oferente describirá la estructura de soporte 6.2. El oferente describirá la estructura de servicios profesionales	

Universidad Nacional de La Matanza

Renglón	Especificación Técnica	Imagen
	6.3. El soporte debe estar disponible las 24 horas, todos los días de la semana 7. Implementación 7.1. Se deberá incluir la instalación completa de la solución 7.2. Se deberá incluir capacitación del producto y configuración para el personal a cargo de la administración del producto	

Firma del Responsable de Contrataciones