11 mar 2026

Hallazgos de Seguridad

Invitados Jaime Alexander Méndez Pulecio Dario Orlando Becerra Erazo Jimy Velez Muñoz Diego Ferney Ramirez Pulido Faver Perez Gutierrez Ferney Cuestas Mahecha Daniel Enrique Bernal Contreras Luis Alexander Jimenez Alvarado Yeison Moreno Gómez

Archivos adjuntos Hallazgos de Seguridad

Registros de la reunión Transcripción Grabación

Resumen

Reunión contextualizó hallazgos de vulnerabilidades en máquinas virtuales con software base antiguo, discutiendo casos de seguridad con rootkits y accesos no autorizados para definir la estrategia de mitigación de EDR y la modernización de infraestructura.

Mitigación de Vulnerabilidades es Necesaria
El grupo de infraestructura encontró vulnerabilidades, posibles ataques y minería de datos en máquinas virtuales debido al software base antiguo. El plan de mitigación se centrará en la modernización de componentes y la implementación de soluciones de seguridad para abordar riesgos.

Servidores Comprometidos por Rootkit
Se presentaron hallazgos de un servidor de aplicaciones misionales comprometido por un rootkit conocido que permite sesiones remotas y acceso privilegiado continuo. También se detectó actividad anómala, como intentos de acceso a bases de datos y conexiones salientes desde el servidor GLPI.

Protección de Servidores y Licenciamiento
Se decidió asignar recursos para comenzar la modernización de la arquitectura con Docker en lugar de esperar más, aunque Legal Boca (IDM) es un desafío importante. Se discutió reasignar licencias de

FortiEDR a servidores de infraestructura críticos e iniciar mesas de trabajo con Fortinet para afinar la seguridad perimetral.

Detalles

- **Introducción y Contextualización de Hallazgos**: Jaime Alexander Méndez Pulecio contextualizó la reunión indicando que el grupo de infraestructura ha encontrado vulnerabilidades, posibles ataques y minería de datos en las máquinas virtuales, lo cual creen que se debe en gran medida al software base antiguo que poseen. Por lo tanto, se sugiere la necesidad de comenzar un plan de mitigación enfocado en la modernización de los componentes del sistema (00:05:55).
- **Presentación del Primer Caso de Seguridad (Servidor de Aplicaciones Misionales)**: Dario Orlando Becerra Erazo presentó hallazgos en un servidor de sistemas misionales donde un antivirus detectó y eliminó archivos maliciosos que luego reaparecieron, indicando que algo o alguien está ejecutándose para regenerar los archivos. El análisis de un archivo subido a Gemini reveló que se trataba de un rootkit conocido que permite sesiones remotas, la capacidad de convertirse en un bot, y ofrece acceso privilegiado y continuo de manera oculta (00:07:06). Se ha utilizado la herramienta Kaspersky Removal Virus Tool para borrar los archivos, pero reaparecen, y hay archivos vulnerables que no se han borrado por miedo a afectar los servicios del aplicativo (00:09:34).
- **Discusión sobre Solución EDR y Tarea de Inventario**: Diego Ferney Ramirez Pulido preguntó si el servidor de aplicaciones misionales ya tenía instalada la solución EDR de la entidad, a lo que Dario Orlando Becerra Erazo respondió que no la conocen y no han visto ningún antivirus instalado en ningún servidor. Diego Ferney Ramirez Pulido asignó a Ferney Cuestas Mahecha la tarea de realizar un inventario de los servidores y el estado de la solución EDR, advirtiendo que la instalación debe ser escalonada y controlada (máquinas de prueba antes de producción) debido a posibles bloqueos (00:11:04) (00:13:40).
- **Aclaración sobre la Cobertura de FortiEDR**: Ferney Cuestas Mahecha señaló que la herramienta FortiEDR fue adquirida para 220 endpoints y usuarios finales. No obstante, Diego Ferney Ramirez Pulido aclaró que la adquisición se hizo para los equipos de infraestructura tecnológica, incluyendo servidores físicos y virtuales (00:12:22). Se discutió la posibilidad de reasignar licencias de FortiEDR de endpoints menos críticos a servidores de infraestructura para

iniciar la mitigación, y se confirmó la necesidad de identificar la cantidad de licencias existentes y cómo se protegerán los servidores (00:13:40).

- **Presentación del Segundo Caso de Seguridad (Servidor GLPI)**: Dario Orlando Becerra Erazo presentó un segundo caso en el servidor 10.54.80.103, donde encontraron logs de intentos de acceso a la base de datos desde otras máquinas como la 10.80.50.99 (servidor Smart) y la 10.54.80.219 (servidor Legal Boca) (00:14:44) (00:16:57). También se detectaron conexiones salientes hacia Cloudflare, ocultando consultas a internet, lo cual es considerado anómalo ya que el servidor debería usar los DNS internos (00:19:05). Este escaneo hacia la red, el uso de un bash generado por algo en Python y la ejecución de múltiples bash son motivo de preocupación en el servidor de producción Legal Boca (00:20:11).
- **Estrategias Inmediatas y Documentación de Servidores**: Diego Ferney Ramirez Pulido solicitó a Dario Orlando Becerra Erazo enviar un correo electrónico al ingeniero Óscar detallando los hallazgos para iniciar mesas de trabajo con varios analistas, incluyendo el ingeniero Jiménez para el tema de bases de datos (00:21:18). Jaime Alexander Méndez Pulecio sugirió como plan de investigación inicial deshabilitar el acceso a internet para el servidor GLPI, dejándolo solo para consultas, ya que el servidor es una víctima y no el origen del problema (00:22:16). Se confirmó que existe un inventario completo de servidores, arquitectura, y componentes para Legal Boca, pero se necesita actualizar y validar el estado de los demás servidores (00:23:20).
- **Afinamiento de Seguridad Perimetral y Protección de Servidores**: Diego Ferney Ramirez Pulido informó que se llevará a cabo un QA por parte del fabricante Fortinet para afinar los equipos de seguridad perimetral debido a las brechas de seguridad alarmantes. Yeison Moreno Gómez deberá coordinar una reunión virtual con las personas que realizarán el QA para comenzar el afinamiento (00:26:24). Diego Ferney Ramirez Pulido considera grave que no haya una solución EDR para la protección de servidores y reitera la necesidad de documentar los hallazgos por correo electrónico al ingeniero Óscar (00:27:42).
- **Uso de Vicarius para Escaneo de Vulnerabilidades y Plan de Instalación**: Se discutió el uso de Vicarius como herramienta para obtener un panorama global de las vulnerabilidades. Se sugirió suspender las instalaciones de Vicarius en endpoints de usuario final para centrarse en los servidores productivos (sistemas misionales, SIGA, Smart, Legal Boca) de manera prioritaria (00:28:48). Ferney Cuestas Mahecha mencionó que Vicarius ya ha generado un informe preliminar con 32 riesgos de criticidad alta en 64

máquinas, y la GPO se reactivó para automatizar la instalación en 120 activos (00:31:00).

- **Avance en la Modernización de Aplicaciones y Arquitectura de Legal Boca**: Daniel Enrique Bernal Contreras propuso avanzar en la migración de aplicaciones a nuevos servidores e instalaciones limpias (como la iniciativa de Docker de Dani) para mitigar riesgos, en lugar de esperar una línea de acción del ingeniero Óscar (00:33:19). Jaime Alexander Méndez Pulecio estuvo de acuerdo en proveer recursos para que se comience con la infraestructura de Docker. Jimy Velez Muñoz y Jaime Alexander Méndez Pulecio señalaron que Legal Boca (IDM) presenta un desafío significativo debido a su arquitectura y la necesidad de licenciar y reestructurar si se cambia la versión del software base, lo cual no es un tema de corto plazo (00:35:34).
- **Tareas Finales y Revisión de Licenciamiento**: Diego Ferney Ramirez Pulido reiteró las tareas principales: continuar con la instalación de Vicarius y comenzar las mesas de trabajo con Jason y Fortinet para el afinamiento de los equipos de seguridad (00:36:52). Se acordó revisar la documentación para confirmar si la licencia de FortiEDR (220 licencias) es compatible con los sistemas operativos de los servidores (Oracle Linux 7, 8, 9 y Windows Server 2016, 2022, 2025) (00:39:49). Se pidió no olvidar el correo electrónico detallando los movimientos laterales y la comunicación entre servidores para consultar al ingeniero Óscar (00:40:56).

Pasos siguientes recomendados

- ☐ Yeison Moreno Gómez contará a Diego Ferney Ramirez Pulido las fechas y horas tentativas para programar una reunión virtual con Fortinet para realizar el QA y afinamiento de los equipos de seguridad perimetral.
- ☐ Jaime Alexander Méndez Pulecio y Dario Orlando Becerra Erazo actualizarán la documentación e inventario de máquinas virtuales y servidores en servicio para validar su estado, y realizarán una sesión de trabajo esta noche para hacer la evaluación y el match con el listado de servidores y las IPs reportadas.
- ☐ Daniel Enrique Bernal Contreras enviará a Jaime Alexander Méndez Pulecio las características de las máquinas que necesita para el plan de modernización de los sistemas misionales en Docker.

- [ ] Dario Orlando Becerra Erazo y Ferney Cuestas Mahecha revisarán el problema de la máquina donde instalaron Vicarius para verificar si se visualiza en la consola.

Revisa las notas de Gemini para asegurarte de que sean correctas. Obtén consejos y descubre cómo toma notas Gemini

Danos tu opinión sobre el uso de Gemini para tomar notas en una breve encuesta.