Caso práctico semana #6: GAP análisis de cumplimiento.

Objetivo:

Realizar un GAP Análisis para una auditoria de cumplimiento.

Contexto:

Ustedes trabajan para la organización multinacional que se dedica a la producción, venta de productos a distribuidores, desean realizar una alianza importante con una empresa en los Estados Unidos, Los directores están sumamente interesados ya que podrían ampliar sus operaciones y aumentar un 600% las utilidades percibidas anuales, sin embargo le han solicitado a la compañía que debe cumplir con algunos requisitos para que la alianza se concrete, entre ellos deben realizar una evaluación de su postura de ciberseguridad con el marco de trabajo NIST CSF 2.0 (cybersecurity framework), deben realizar una autoevaluación inicial para saber en que nivel de madurez están, por que posteriormente mandarán a un auditor extranjero a revisar el trabajo realizado.

Su equipo está a cargo de llevar a cabo la auditoria. **Infraestructura**

Actual

- ERP SAP Hana
- Sistemas SCADA en plantas
- Red OT segregada por Vlans
- Infraestructura legacy en plantas
- Sistemas de control industrial
- IoT para monitoreo de producción
- Múltiples integraciones con proveedores
- Antivirus Microsoft Defender
- Firewall Checkpoint y licencimiento IPS.
- Access point ubiquiti con redes Wireless con autenticación empresarial.
- No existe un centro de operaciones de seguridad.
- No existe un DRP ni un BCP.

Instrucciones:

- Deberá realizar un cronograma de actividades para dicha evaluación. - Descargue la herramienta CSET de CISA:

  https://www.cisa.gov/downloading-and-installing-cset

- Cree un nuevo assessment de “The NIST Cybersecurity Framework (CSF) 2.0” - Complete el assessment.
- Realice un informe sobre sobre el cumplimiento, cumplimiento por categoría y los resultados generales de la evaluación.
- Establezca cuales son los puntos que necesitan mayor atención, si son críticos o no, evalúe el riesgo de implementar alguna solución o no realizarlo.
- Si bien para nuestra organización no era necesario cumplir con este estándar, es importante para concretar la alianza, por ello debe establecer un plan de acción con las recomendaciones de mayor impacto y con mayor prioridad.

Entregables:

- Cronograma en Trello o Planner.
- Informe de resultados.
- Conclusión sobre las 5 mayores prioridades identificadas.
- Riesgos asociados a las debilidades.
- Plan de acción.

Se calificará:

- Organización del cronograma y claridad del plan - Uso de la herramienta CSET
- Calidad del informe de resultados. - Priorización de debilidades.

Fecha de entrega:

Auditoría Firewall

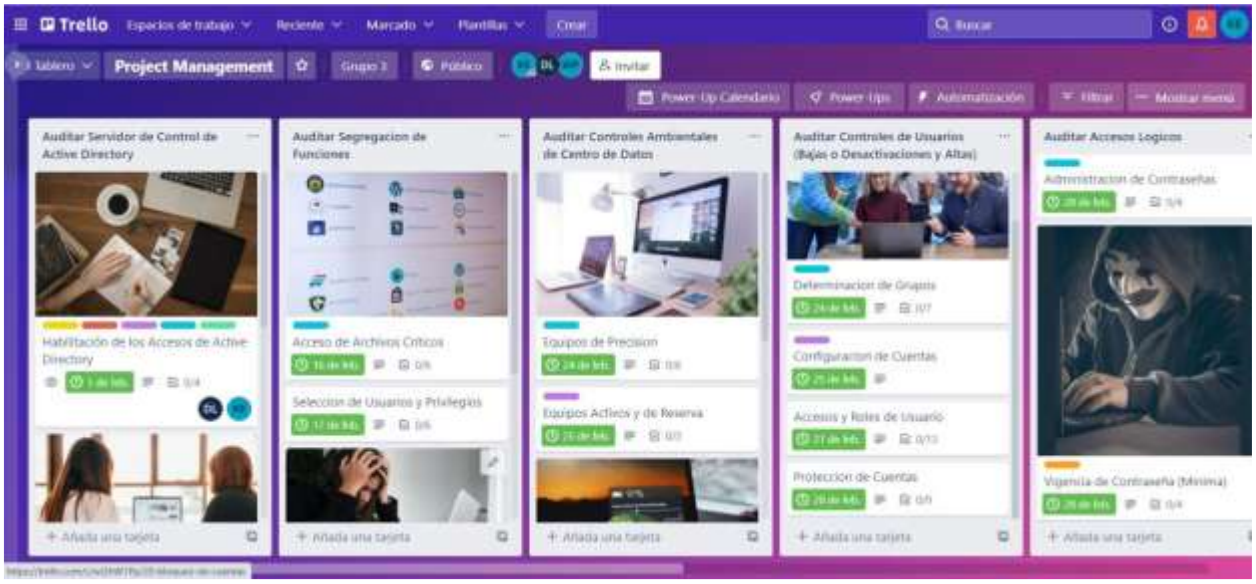
Se requiere que tras su expertis en el tema de seguridad informática pueda dar certeza sobre las configuraciones del firewall, siendo en este caso un experto externo de Auditoria de Sistemas.

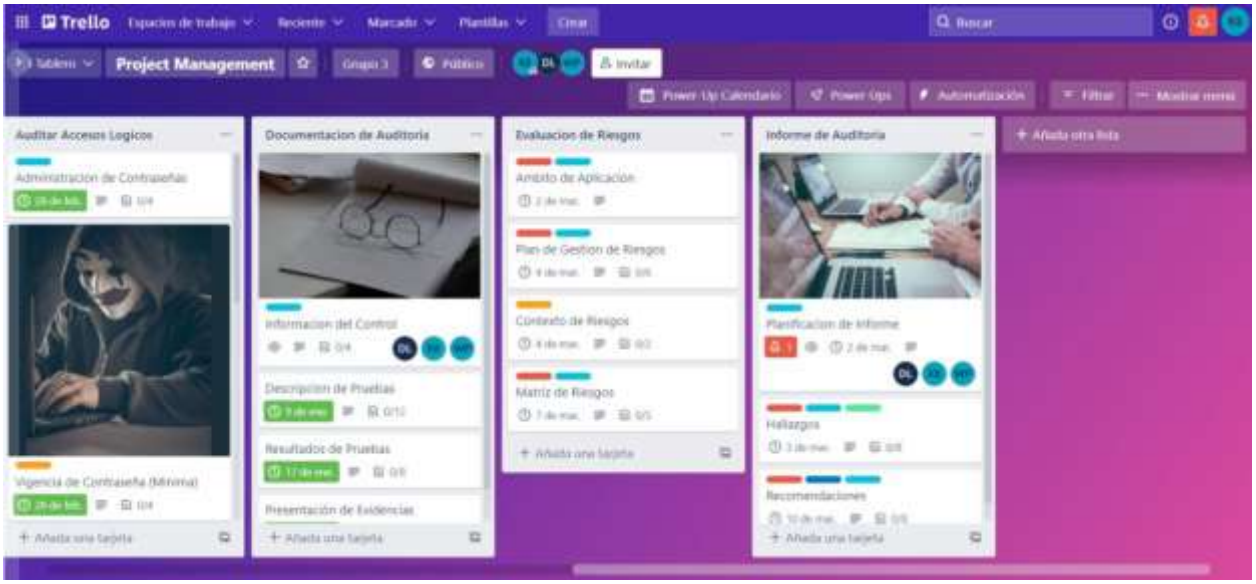
Por lo que usted y su equipo son contratados para aplicar una auditoría externa al banco XYZBA en relación al nivel de seguridad y buenas prácticas aplicadas sobre el activo Fortigate 2000E, donde la entidad les solicita los siguientes entregables:

1. Plan de trabajo (En Trello, puede utilizar la cuenta de miumg o bien otro equivalente online).
2. Desarrollo de herramientas de auditoria (Checklist Aplicables – Forms y Software de terceros solo como referencia ya que no contamos con un ambiente propio para este alcance).
3. Definir el marco de trabajo o estándar ya que a sus observaciones/hallazgos deberán estar relacionados a dichos puntos de control.
4. Puede simular la auditoria a través del ambiente demo https://fortigate.fortidemo.com/

Nota: previo al inicio de la auditoria el cliente le solicita la firma de un acuerdo de confidencialidad y buen uso de la información, por lo que debe de presentar el mismo (el Banco XYZBA no cuenta con uno y desea promover esta práctica).

Ejemplos de Trello:


Trello
Project Management
Auditar Servidor de Control de Active Directory
Habilitación de los Accesos de Active Directory
Auditar Segregacion de Funciones
Acceso de Archivos Críticos
Seleccion de Usuarios y Privilegios
Auditar Controles Ambientales de Centro de Datos
Equipos de Precision
Equipos Activos y de Reserva
Auditar Controles de Usuarios (Bajas o Desactivaciones y Altas)
Determinacion de Grupos
Configuracion de Cuentas
Accesos y Roles de Usuario
Proteccion de Cuentas
Auditar Accesos Logicos
Administracion de Contraseñas
Vigencia de Contraseña (Minima)


Trello
Project Management
Auditar Accesos Logicos
Administracion de Contraseñas
Vigencia de Contraseña (Minima)
Documentacion de Auditoria
Informacion del Control
Descripcion de Pruebas
Resultados de Pruebas
Presentacion de Evidencias
Evaluacion de Riesgos
Ambito de Aplicacion
Plan de Gestion de Riesgos
Contexto de Riesgos
Matriz de Riesgos
Informe de Auditoria
Planificacion de Informe
Hallazgos
Recomendaciones


Trello
Gestión de Proyectos-VN-C
COSTOS
ACTIVIDADES
APRENDIZAJE / REFLEXIÓN
TIEMPO - COSTO - ACTIVIDADES
APLICACIÓN KAHEN GAMES
KAHEN GAMES
MISSION ACCOMPLISHED
FUE DIFICIL..
PERO LO LOGRAMOS