sescam
Servicio de Salud de Castilla-La Mancha

Dirección General de Salud Digital

PRESENTACIÓN DE CANDIDATURAS A LOS PREMIOS SOCINFO DIGITAL POR PARTE DE LA DIRECCIÓN GENERAL DE SALUD DIGITAL DEL SERVICIO DE SALUD DE CASTILLA LA-MANCHA

Castilla-La Mancha
Avda. Río Guadiana - 45071 TOLEDO

PREMIO SEGURIDAD Y PROTECCIÓN DEL DATO

Descripción del Proyecto. Securizacion, gestión e integración de dispositivos Iot-IoMT

El principal objetivo del proyecto es alcanzar la seguridad del paciente y de los datos e información que se genera a través de la multitud de dispositivos que interactúan con él. Para poder abordar, controlar y gestionar todos estos dispositivos así como la información asociada a los mismos, el SESCAM contempla, dentro de la Estrategia de Salud digital de la Dirección General de Salud Digital, DGSD, la securización, gestión e integración de los dispositivos IoT/IoMT (Internet of Things /Internet of Medical Things)

La DGSD cuenta con una herramienta o solución de securización de todo el universo IoMT/IoT distribuida y con gestión centralizada que se está instalando en todos los Hospitales del SESCAM a través de la activación de una funcionalidad en los Firewalls PaloAlto, a través de los cuales se detecta, analiza y centraliza el tráfico de los dispositivos IoT/IoMT. Todo ello se gestiona y monitoriza por medio de una consola centralizada que es la que proporciona toda la información al respecto.

La solución se encarga de identificar en primer lugar los siguientes aspectos:

- Inventario de activos
    - Descubrimiento continuo de todos los dispositivos conectados, como servidores, PCs, portátiles, así como dispositivos no gestionados como IoT, IoMT y OT.
    - Identificar pasivamente el 90% de los dispositivos en menos de 48 horas usando Machine Learning con +50 atributos.
    - Compartir la visibilidad de IoMT.

  - Optimizar el coste de los dispositivos mediante la visibilidad del uso de los mismos.

- Estado de la protección de dispositivos.
  - Asegurarse que los dispositivos disponen de una solución de seguridad y que se encuentra actualizada.

- Gestión de vulnerabilidades
  - Mapear riesgos y vulnerabilidades con activos IoT/IoMT. Alertar cuando se descubren nuevas vulnerabilidades y entender el plan para mitigar el riesgo.
  - Detectar vulnerabilidades y compartirlas bidireccionalmente con soluciones de gestión de vulnerabilidades.
  - Gestionar continuamente el riego y medirlo para priorizar la respuesta.
  - Automatizar el examen de compliance con un informe de 1 click.

- Visibilidad de amenazas. Ganar visibilidad en amenazas asociadas con activos, como conexiones a IPs maliciosas, conexiones no seguras y anomalías de comportamiento.

- Segmentación de dispositivos. Perfilado de dispositivos y políticas de seguridad recomendadas Zero Trust. Integración en los Firewalls.

- Estado de parcheado. Identificar donde se están usando sistemas operativos fuera de soporte y donde se encuentran dispositivos vulnerables que debemos proteger.

- Aplicar políticas de mitigación del riesgo
  - Obtener políticas recomendadas Zero Trust para permitir el acceso y el comportamiento de dispositivos de confianza

  - Aplicar segmentación basada en el contexto reduciendo la superficie de ataque
  - Aplicar políticas de seguridad con 1 click.

- Prevenir amenazas conocidas
  - Proteger frente a exploits, spyware y otras amenazas conocidas.
  - Mejorar la respuesta ante incidentes añadiendo al SIEM el contexto de los dispositivos.

- Detección y respuesta ante amenazas desconocidas
  - Detectar amenazas Zero Day y actividad anómala
  - Bloquear amenazas de ficheros desconocidos y basados en web
  - Mantener información detallada sobre el incidente para la respuesta
  - Alertar ante la presencia de anomalías
  - Aplicar medidas de contención en caso de comportamientos maliciosos.

Repercusión para el ciudadano y las Administraciones.

Tanto para nuestro ciudadanos y pacientes, como para nosotros mismos, la solución tiene una repercusión muy importante para garantizar la seguridad en un uso creciente de los dispositivos y los datos que generan, reducir la exposición a riesgos y aplica nuestras políticas de seguridad para proteger los dispositivos contra todo tipo de amenazas.:

• Riesgo de salud del paciente. Se necesita mantener la seguridad del paciente con la disponibilidad IoMT y el control de riesgos.

• Riesgos de compliance. La visibilidad de IoMT limitada y la gestión manual de riesgos hace que sea complicada cumplir los requisitos de regulación

- Riesgo de seguridad. Visibilidad limitada, las vulnerabilidades sin parchear y la falta segmentación.

- Presión de rentabilidad. Se necesita asegurar la eficiencia de uso de los dispositivos IoMT.

Equipo de desarrollo y proveedores.

Equipo interno de la Unidad de Ciberseguridad del Área de Infraestructuras digitales de la Dirección General de Salud Digital.

Solución IoT Security – Palo Alto Networks.

Valoración económica.

En este caso tenemos que sumar el Licenciamiento de la, con soporte, capacitación y puesta en marcha de la solución junto con el coste del equipo humano interno y especializado, dependiente todo él de la Unidad de Ciberseguridad

Plazos de cumplimiento

El proyecto se ha planteado en el tiempo a través de un cronograma que finalizará en el segundo semestre del año en curso. La solución está desplegada en todos los Hospitales de la región, habiendo completado fases como asignación de licencias a los Firewalls, revisión de perfiles de Log forwarding, inicio de ingesta de datos, aprendizaje de redes y eventos y revisión de redes y perfiles de equipos detectados.

Las fases pendientes serán las relativas a la identificación de vulnerabilidades y varios tipos de riesgos, la revisión de las recomendaciones de reglas generadas por perfiles, la procedimentación de la gestión de eventos, el Gobierno de la

solución, la implantación de políticas recomendadas en modo auditoría sin Deny, el análisis del tráfico y la Implantación definitiva de políticas recomendadas.