Boletín informativo del Departamento de Productos y Tecnologías de Seguridad TIC del Centro Criptológico Nacional (CCN-PYTEC).

Boletín CCN-PYTEC nº22 - 02/2020

Novedades en el Catálogo de Productos STIC

RSA cualifica su producto NetWitness en la familia *"Sistemas de gestión de eventos de seguridad"* para ENS categoría ALTA (12/2019).

Sistemas de gestión de eventos de seguridad

NetWitness 11 es la solución de SIEM evolucionado, con capacidades de visibilidad completa gracias a su modelo de datos unificado pudiendo capturar *logs*, *netflow*, tráfico de red y *end point* de forma integrada, bajo un único motor de análisis y correlación avanzada. Además, incluye funcionalidades necesarias por un Centro del Operaciones de Ciberseguridad (SOC) para hacer frente a amenazas complejas

Forcepoint cualifica nuevos productos en la familia de *"Sistemas para prevención de fugas de datos"* para ENS categoría ALTA (12/2019).

El producto *Forcepoint On-Premise Security,* versión *8.*5, de la empresa Forcepoint ha sido incluido en el CPSTIC como producto cualificados para ENS categoría ALTA en la familia *de "Sistemas para prevención de fugas de datos".*

Sistemas para prevención de fugas de datos

Forcepoint On-Premise Security es una solución de prevención de fuga de datos en un organismo. Esta solución ofrece una alta escalabilidad de acuerdo con la estrategia del cliente para abordar el robo y la pérdida de datos.

Aruba cualifica nuevos productos en varias familias del CPSTIC (12/2019).

Aruba ha cualificado y aprobado su serie de productos *Mobility Controller* (7005, 7008, 7010, 7024, 7030, 7205, 7210, 7220, 7240, 7240XM) y *Virtual Mobility Controller* (MC-VA-50, MV-VA-250, MC-VA-1K) con el sistema operativo Aruba OS versión 8.2 en las siguientes familias del CPSTIC:

Dispositivos de Red Inalámbricos

Redes privadas virtuales: IPSec

Los *Mobility Controllers* (MC) y *Virtual Mobility Controllers* (VMC) de Aruba son *switches* inalámbricos (*appliance* físicos o virtuales) que proporcionan una amplia gama de servicios y características de seguridad que incluyen la movilidad de red inalámbrica y cableada, seguridad, administración centralizada, auditoría, autenticación, acceso remoto seguro, auto-chequeos de integridad y operación, filtrado de tráfico y funcionalidad de Gateway VPN.

Los puntos de acceso (AP) de ARUBA compatibles son: AP-203R , AP-203RP , AP-204 , AP-205 , AP-205H , AP-214 , AP-215 , AP-224 , AP-225 , AP-228 , AP-274 , AP-275 , AP-277 , AP-303H , AP-304 , AP-305 , AP-314 , AP-315 , AP-324 , AP-325 , AP-334 , AP-335.

Cisco cualifica nuevos productos en varias familias del CPSTIC (12/2019).

CISCO ha cualificado las siguientes series de dispositivos:

- Catalyst 3650 y 3850 con IOS XE 16.3
- Catalyst 9300 y 9500 con IOS XE 16.9
- *Catalyst 9200L y 9400* con *IOS XE 16.9*

Enrutadores

Switches

Los productos, que han sido incluidos en las familias de *"Enrutadores"y "Switches"*, son plataformas de enrutamiento y conmutación con capacidades de filtrado de tráfico OSI Capa 2 y Capa 3.

La empresa ARPA, EQUIPOS MÓVILES DE CAMPAÑA S.A.U. ha conseguido la aprobación de su producto SHATEM - SHELTER ARPA TEMPEST MULTIPROPOSITO en la familia de *"Armarios Apantallados"* del CPSTIC (01/2020).

Armarios apantallados

El contenedor *shelter* de la empresa ARMA, EQUIPOS MÓVILES DE CAMPAÑA S.A.U ha sido aprobado para su utilización en el despliegue de sistemas clasificados. Está destinado al alojamiento y/o operación de equipos informáticos, electrónicos, optrónicos de telecomunicaciones y asimilables para entornos CIS. Dispone de elementos de filtrado y protección EMI necesarios en acometidas de potencia, datos y servicios para disponer de apantallamiento intergral TEMPEST frente a emanaciones comprometedoras radiadas y conducidas.

Grupo ICA ha cualificado su producto LogICA Next Generation SIEM en la familia de *"Sistemas de gestión de eventos de seguridad"* del CPSTIC (01/2020).

La plataforma Next Generation SIEM LogICA, versión 5.7.1, ha sido cualificada e incluida en la familia de *"Sistemas de gestión de eventos de seguridad"*.

El producto permite a los analistas de ciberseguridad recopilar *logs* e información de seguridad, detectar ataques basados en anomalías y comportamientos desconocidos así como automatizar la respuesta ante incidentes.

Gestión de eventos de seguridad

EMSEC

Primer curso STIC de Seguridad de Emanaciones y TEMPEST (02/2020).

En el mes de febrero ha tenido lugar el primer curso STIC de Seguridad de Emanaciones y TEMPEST, dirigido a organismos de la Administración que por sus funciones necesitan disponer de los conocimientos necesarios para hacer frente a este tipo de amenazas. El curso de dos días de duración fue impartido por técnicos del laboratorio TEMPEST del Centro Criptológico Nacional y asistió personal del Ministerio de Defensa, Interior y Asuntos Exteriores, Unión Europea y Cooperación. Todos los organismos asistentes se han visto, o verán, implicados en alguno de los aspectos tratados durante el curso, ya sea en la protección de la información, la definición de requisitos de diseño, o la evaluación de instalaciones o plataformas en las que habitualmente se trabaja con información clasificada CONFIDENCIAL o superior.

Durante el curso, se hicieron demostraciones en directo de distintos medios de fuga de información en equipos aislados sin necesidad de tener acceso a los mismos, se analizaron los vectores de ataque que ofrecen estas tecnologías y se presentaron las contramedidas que dificultan la materialización de estos ataques.

Evaluación EF200 Twin Seat (02/2020).

A solicitud de NETMA (agencia OTAN para la gestión de los programas Eurofighter y Tornado), el CCN ha llevado a cabo la evaluación y certificación TEMPEST a nivel de plataforma de las nuevas radios embarcadas en los cazas eurofighter. La evaluación se realizó en las instalaciones de Airbus en Getafe con el apoyo del personal especialista en comunicaciones y TEMPEST-EMC de la empresa y en coordinación con el Ejército del Aire y la oficina de programa. Estas pruebas son necesarias para confirmar que los equipos de radio una vez instalados en la plataforma mantienen la certificación TEMPEST y no suponen un riesgo para la confidencialidad de la información procesada en la aeronave.

Comunicaciones Tácticas Seguras

Demostración sobre comunicaciones inalámbricas seguras al Regimiento de Transmisiones nº 21 del Ejército de Tierra (02/2020).

El pasado 26 de febrero, en el marco de los Planes de Experimentación del Ejército de Tierra, el CCN y la Jefatura CIS y Asistencia Técnica (JCISAT) del ET hicieron una demostración al Regimiento de Transmisiones nº 21 en Marines (Valencia) sobre el empleo seguro de tecnologías inalámbricas que, entre otras cosas, facilitan el despliegue rápido de los puestos de mando.

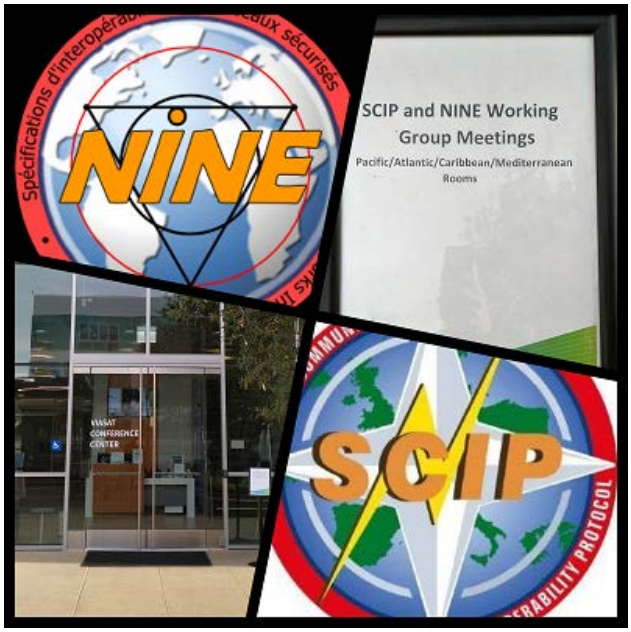
La demostración se centró en un escenario con una única infraestructura Wi-Fi que soportaba tres dominios de seguridad diferenciados, que reproducían los entornos de seguridad que se establecerían en un Puesto de Mando de Brigada:

- RESERVADO (RES),
- DIFUSIÓN LIMITADA (DL) y
- SIN CLASIFICAR (SC)

Para la protección de la confidencialidad de la información, se emplearon productos de cifra software (para DL) y hardware (para RES) recomendados por el CCN. Esta demostración tendrá continuidad en un ejercicio real del Regimiento de Transmisiones nº21, que tendrá lugar la semana del 30 de marzo en la provincia de Valencia.

Interoperabilidad

Participación española en los grupos de trabajo SCIP y NINE (01/2020).



La semana del 27 al 31 de enero, el CCN participó en la Tercera Reunión de los Grupos de trabajo para el desarrollo e implantación de los estándares de la OTAN para la protección de voz segura SCIP (Secure Communications Interoperability Protocol) y protección de transmisiónes IP NINE (Network and Information Infrastructure IP Network Encryption). Dentro de este marco, y en paralelo a las sesiones principales, se reunieron los “focus group”, de los que cabe destacar aquellos dedicados a la definición de perfiles especificos para comunicaciones radio (STaC-IS, “SCIP packet-based” y “NINE Tactical Radio Profile”) y el dedicado a la definición de un perfil para entornos FMN (“Federated Mission Networking”).

Durante las sesiones que se celebraron en Carlsbad (Estados Unidos), en las instalaciones de la empresa General Dynamics, el CCN presentó la evolución de la estrategia nacional para el

desarrollo de productos nacionales basados en estos estándares, y expuso los planes de de participación de la industria de cifra nacional en el ejercicio CWIX de este año, los cuales incluyen pruebas de interoperabilidad con productos nacionales que implementan los estándares STaC-IS y NINE. Asimismo está previsto el uso de un diodo nacional como dispositivo de intercambio seguro entre la red clasificada de CWIX y la red sin clasificar.

Formación y concienciación en seguridad

Productos STIC para la protección de información clasificada en el programa Horizonte 2020 (02/2020).

El pasado 19 de febrero tuvo lugar en la sede del CDTI (Centro para el Desarrollo Tecnológico Industrial) una jornada informativa sobre la protección de la Información Clasificada (IC) en los programas Horizonte 2020 y Horizonte Europa. Dicha jornada fue organizada por el propio CDTI y por la Oficina Nacional de Seguridad (ONS), y sirvió para presentar diversas cuestiones sobre cómo tratar la IC en dichos programas, las habilitaciones de seguridad que es necesario obtener, etc. La jornada contó con la asistencia de universidades, centros tecnológicos y empresas. Por su parte, el CCN presentó los diferentes productos STIC nacionales disponibles para proteger la IC de grado EU RESTRICTED y EU CONFIDENTIAL que se podrían manejar en los diferentes proyectos, los cuales están recogidos en el Catálogo de Productos STIC (CCN-STIC-105).

El reto de explicar la "Criptografía en el Mundo Real" a los alumnos del V Curso Avanzado de Ciberdefensa (02/2020).

El pasado mes de febrero, personal del CCN se desplazó hasta la Academia de Ingenieros de Hoyo de Manzanares para realizar la ponencia "Criptografía en el Mundo Real", perteneciente al módulo de Especialidades Criptológicas dentro del V Curso Avanzado de Ciberdefensa que organiza el Mando Conjunto de Ciberdefensa.

Durante la ponencia se hizo un recorrido por las aplicaciones y ejemplos de uso en el mundo real, tanto de la criptografía de clave secreta (tanto cifrado en serie como cifrado en bloque), como de la criptografía de clave pública.

Además, se introdujeron los conceptos de los bits cuánticos o qubits, la computación cuántica y la amenaza que supondría para nuestros sistemas de la información la construcción de un ordenador cuántico computacionalmente relevante, así como las difererencias entre criptografía cuántica y postcuántica.

Asimismo, se realizó una presentación de los productos de seguridad TIC actualmente aprobados para proteger infomación nacional clasificada, así como aquellos productos nacionales que han sido aprobados para proteger infomación OTAN clasificada y UE clasificada.

Contacto

Correo electrónico CCN-PYTEC	**ccn-pytec@cni.es**
Twitter	**@CCNPYTEC**
LinkedIn	**https://www.linkedin.com/company/CCN-PYTEC**
Catálogo CPSTIC	**Enlace web**