Facultad Militar Conjunta

OBSERVATORIO ARGENTINO DEL CIBERESPACIO

Director del Proyecto: BM (R) Alejandro Moresi
Codirector: TC (R) Ing Carlos Amaya
Edición: Bib Alejandra Castillo

ISSN: 2718-6245
http://www.esgcffaa.edu.ar/esp/oac-boletines.php

AÑO 7 N° 52
Enero/Febrero/Marzo 2024

OAC Boletín de Enero-Febrero 2024

"El primero, el supremo, el más trascendental acto de juicio que el estadista y el comandante tienen que hacer es establecer mediante esa prueba el tipo de guerra en la que se embarcan; no confundirla con algo ajeno a su naturaleza, ni tratar de convertirla en ello.

Carl von Clausewitz, Sobre la guerra"

Tabla de Contenidos

El Observatorio Argentino del Ciberespacio (OAC), es un micro-sitio de la Facultad Militar Conjunta de las Fuerzas Armadas, editado y publicado por el Instituto de Ciberdefensa de las Fuerzas Armadas

URL: http://www.esgcffaa.edu.ar/esp/oac-boletines.php,.

Esta publicación mensual se encuentra inserta en el Nodo Territorial de Defensa y Seguridad de la Red Nacional de Nodos Territoriales (NT) de Vigilancia Tecnológica e Inteligencia Estratégica (VTeIE) del Ministerio de Ciencia, Tecnología e Innovación de la Nación y es administrado por el Centro de Estudios de Prospectiva Tecnológica Militar "Grl Mosconi" de la Facultad de Ingeniería del Ejército Argentino.

Nuestro objetivo se reafirma en la intención de llevar a la comunidad ciberespacial distintas perspectivas de este nuevo ambiente operacional, aportando novedades reportes e informes que permitan a la comunidad educativa y a la sociedad en general conocer más acerca del mismo.

ESTRATEGIA

Aplicación de IA al transporte

El Departamento de Transporte está asignando 15 millones de dólares en fondos federales para que las pequeñas empresas aprovechen los sistemas de inteligencia artificial y creen nuevas aplicaciones específicamente para el sector del transporte de EE. UU.

https://link.nextgov.com/click/34233554.63391/aHR0cHM6Ly93d3cubmV4dGdvdi5jb20vYXJ0aWZpY2lhbC1pbnRlbGxpZ2VuY2UvMjAyNC8wMi90cmFuc3BvcnRhdGlvbi1sYXVuY2hlcy0xNW0tYWktZWZmb3J0LWltcHJvdmUtdXMtc3RyZWV0LWluZnJhc3RydWN0dXJlLzM5Mzg3My8_b3JlZj1uZ2Zjd19mdHRfbmw/597b4680e661f0a4708b4c13B001fd171

El transporte lanza un esfuerzo de IA de 15 millones de dólares para mejorar la infraestructura de las calles de EE. UU. - Nextgov/FCW

¿Vale la Pena la Inteligencia Artificial

Las decisiones de estrategia de adquisición se basan en estudios de mercado. Y si bien las solicitudes de información pueden parecer a veces desalentadoras, los esfuerzos valen la pena. Theresa Terry, líder del equipo de la División de Adquisición de Servicios y Gestión de Categorías del Subsecretario Adjunto de la Fuerza Aérea dijo: "el poder de la IA podría potencialmente ocuparse de asuntos a nivel de superficie o acelerar ciertos procesos. "¿Pero reemplazar? Absolutamente no".

https://www.afcea.org/signal-media/ai-worth-buzz?utm_source=Informz&utm_medium=Email&utm_campaign=Informz%20Email&_zs=pIIVg1&_zl=HwLQ9
https://www.afcea.org/signal-media/data-sharing-impacts-human-health

Implicancia de la atribución lenta de ataques

Las demoras en la determinación de la atribución pueden tener efectos estratégicos, aquí se cita el caso de una organización de noticias le tomó cincuenta y cinco horas y veinticinco minutos publicar una atribución pública autorizada de los dos atentados suicidas del Estado Islámico en Kerman, Irán, que mataron al menos a noventa personas el 3 de enero de 2024. Durante ese tiempo, al menos un alto funcionario iraní culpó abiertamente a Israel por los ataques y pidió ataques de represalia inmediatamente después algunos periodistas estadounidenses simplemente repitieron las acusaciones iraníes, ofreciendo poca investigación adicional sobre los autores. Mientras tanto, la autoría de los ataques por parte del Estado Islámico fue cuestionada y debatida ampliamente.

https://mwi.westpoint.edu/fifty-five-hours-of-risk-the-dangerous-implications-of-slow-attack-attribution/

Guía de la Identidad Digital y la reputación Online

La identidad corporativa permite a las empresas diferenciarse de las demás, y esto, es también cierto en el mundo digital e interconectado actual. En este entorno, cobran especial importancia algunas características de la comunicación, en particular las relativas a la inmediatez, visibilidad, credibilidad, influencia y permanencia de la información. Por tanto, es cada vez más importante, la creación de una identidad digital corporativa, basada en una estrategia de comunicación sólida que les permita alcanzar una posición en entornos colaborativos en Internet, y comunicarse mejor con sus clientes, proveedores y público en general.

https://www.incibe.es/sites/default/files/contenidos/guias/doc/GU%C3%8DA_CIBERSEGURIDAD_EN_LA_IDENTIDAD_DIGITAL.pdf

CIBERDEFENSA

Filtración de datos de 1,32 billones de GB de datos militares por Hackers Ucranianos

El servicio ucraniano de radio difusión Hromadske informa que el grupo Blackjack probablemente tenga vínculos con el Servicio de Seguridad de Ucrania. Una fuente de las fuerzas del orden reveló al servicio que los intrusos robaron documentación técnica de unas 500 instalaciones del Ministerio de Defensa ruso. Los intrusos extrajeron más de 1,32 billones de GB de datos de los servidores de la Dirección General de Construcción Militar. Los datos robados son clasificados y cubren detalles de arsenales de armas, ubicaciones de complejos de misiles antiaéreos, cuarteles y diversos cuarteles generales de unidades. Esta información involucra instalaciones militares existentes y proyectadas en Rusia y territorios ocupados, indicando planes para nuevos proyectos de construcción y modernización.

https://essanews.com/ukrainian-hackers-reveal-russian-military-secrets-devastating-1-32-trillion-gb-data-leak,6986766622963329a

CIBERGUERRA

El escenario de todo en todas partes, todo a la vez

En EE.UU legisladores, directores del FBI, la NSA y la Agencia de Seguridad de Infraestructura y Ciberseguridad, advierten acerca de la actividad cibernética de China está yendo más allá del espionaje y el

robo de datos de la última década, direccionándose a ataques directos a la infraestructura crítica de Estados Unidos. Al respecto los miembros de la junta se refirieron al grupo de hackers Volt Typhoon está colocando malware en enrutadores de red y otros dispositivos conectados a Internet que, si se activa, podría interrumpir los servicios de agua, energía y ferrocarril, posiblemente causando un caos generalizado o incluso hiriendo y matando a estadounidenses.

https://www.defenseone.com/technology/2024/02/chinese-hacking-operations-have-entered-far-more-dangerous-phase-us-warns/393843/?oref=defenseone_today_nl&utm_source=Sailthru&utm_medium=email&utm_campaign=Defense%20One%20Today:%20February%2002%2C%202024&utm_term=newsletter_d1_today

El papel dominante de China en la producción de exploits

Para los actores de los estados-nación que atacan a sus adversarios en el ciberespacio, las vulnerabilidades sin parches en el software son como municiones.

El arte de la piratería se ha vuelto más sigiloso e inteligente con el paso de los años. Los piratas informáticos chinos pueden ocultar el código que utilizan para infiltrarse en sistemas en todo el mundo. Estas incluyen vulnerabilidades que los atacantes pueden utilizar para colarse en una red informática. Los exploits (ataque que aprovecha las vulnerabilidades de las aplicaciones) les permiten comenzar a robar datos una vez que están dentro. "Haga clic aquí". El artículo informa sobre cómo pueden hacer esto.

https://theworld.org/stories/2024-01-15/chinas-dominant-role-producing-hacking-bugs

CIBERCONFIANZA

Implementar confianza cero y la ciberseguridad

Implementar la confianza cero diseñada específicamente para mitigar las amenazas que enfrentan las agencias gubernamentales es un esfuerzo crítico y muy complejo. La confianza cero requiere comprender el almacenamiento de las agencias de datos, incluido el etiquetado de los datos, dónde residen, quién los posee, quién tiene acceso, si se han descargado (también conocido como gobernanza de datos) y los requisitos regulatorios y legales. El esfuerzo se complica aún más por una multitud de proveedores que afirman ofrecer confianza cero con un producto único para todos y argumentos de venta demasiado entusiastas.

Crear y mantener el entorno de confianza cero adecuado requiere una planificación coherente, nuevos procesos, recursos capacitados, un seguimiento eficaz de los esfuerzos de revisión continuos y los productos adecuados que se ajusten a sus requisitos únicos. Es la combinación de todos estos factores, más una estrategia comprobada de gestión del cambio (como observar, orientar, decidir, actuar o bucle OODA), lo que permite a las agencias establecer o mejorar su enfoque de seguridad centrado en datos de confianza cero.

https://www.afcea.org/signal-media/cyber-edge/upend-government-cybersecurity-zero-trust?utm_source=Informz&utm_medium=Email&utm_campaign=Informz%20Email&_zs=pIIVg1&_zl=8wLQ9

TECNOLOGÍA

Robots asesinos una preocupación ética

Los sistemas de armas autónomos, conocidos como "robots asesinos", que durante mucho tiempo han sido materia de ciencia ficción, están a punto de convertirse en realidad gracias al rápido desarrollo de la inteligencia artificial.

En respuesta, las organizaciones internacionales han intensificado los pedidos para que se limiten o incluso se prohíban directamente su uso. En noviembre, la Asamblea General de la ONU adoptó la primera resolución sobre estos sistemas de armas, que pueden seleccionar y atacar objetivos sin intervención humana.

Para arrojar luz sobre cuestiones legales y éticas que plantean, se entrevistó a personas de la Facultad de Derecho de Harvard

https://news.harvard.edu/gazette/story/2024/01/killer-robots-are-coming-and-u-n-is-worried/

CIBERFORENSIA

Informes de Vulerabilidades

En esta área hemos incorporado los informes semanales que proporciona la CISA (Cybersecurity & Infrastructure Security Agency) de los EEUU, estos boletines proporcionan un resumen de las nuevas vulnerabilidades que han sido registradas por la Base de Datos de Vulnerabilidad (NVD) del Instituto Nacional de Estándares y Tecnología (NIST).

2024

1. Vulnerabilidades semana del 22 de enero: https://www.cisa.gov/news-events/bulletins/sb24-029
2. Vulnerabilidades semana del 15 de enero https://www.cisa.gov/news-events/bulletins/sb24-022
3. Vulnerabilidades semana del 8 de enero https://www.cisa.gov/news-events/bulletins/sb24-017
4. Vulnerabilidades semana del 1 de enero https://www.cisa.gov/news-events/bulletins/sb24-008
5. Vulnerabilidades semana del 8 de enero https://www.cisa.gov/news-events/bulletins/sb24-017
6. Vulnerabilidades semana del 15 de enero https://www.cisa.gov/news-events/bulletins/sb24-022
7. Vulnerabilidades semana del 22 de enero https://www.cisa.gov/news-events/bulletins/sb24-029
8. Vulnerabilidades semana del 29 de enero https://www.cisa.gov/news-events/bulletins/sb24-036
9. Vulnerabilidades semana del 5 de febrero https://www.cisa.gov/news-events/bulletins/sb24-043
10. Vulnerabilidades semana del 12 de febrero https://www.cisa.gov/news-events/bulletins/sb24-051
11. Vulnerabilidades semana del 19 de febrero https://www.cisa.gov/news-events/bulletins/sb24-057-0

2023

12. Vulnerabilidades semana del 25 de diciembre https://www.cisa.gov/news-events/bulletins/sb24-002

13. Vulnerabilidades semana del 18 de diciembre https://www.cisa.gov/news-events/bulletins/sb23-360

Conclusiones acerca de las tecnologías multidominio y la amenaza híbrida

El medio de comunicación "El Confidencial" organizó la primera edición del foro Desafíos Defensa en Córdoba (España), centrada en el reto para la base industrial y tecnológica. Estas fueron las claves de un evento que dio cita a líderes industriales, militares y políticos, algunas de las interesantes conclusiones es la del teniente general José María Millán Martínez, jefe del CESTIC (Centro de Sistemas y Tecnologías de la Información y las Comunicaciones) apuntaba que el auténtico desafío yace en el cambio cultural necesario para afrontar esta nueva situación.

https://www.elconfidencial.com/espana/2024-02-04/foro-desafios-defensa-amenaza-hibrida-guerra-multidominio_3823290/

Sitio web: http://www.esgcffaa.edu.ar/esp/oac-boletines.php Nuestra dirección postal es:

** | Luis María Campos 480 - CABA - República Argentina | **

Nuestro correo electrónico:

|observatorioargentinodelciberespacio@conjunta.undef.edu.ar | *