ESPECIAL

"Hack&News"

DE Tecnología & Sentido Común

ESPECIAL
AGOSTO
2024

ESPECIAL

"Hack&News"

DE Tecnología & Sentido Común

EDITA
Business, Technology & Best Practices, S.L.
Av. San Onofre, 20
46930-Quart de Poblet (Valencia)
Teléfono: 96 109 44 44
Fax: 96 109 44 45
https://tecnologiaysentidocomun.com
soluciones@businessandcompany.com

Miguel Angel Arroyo

Miguel Ángel Arroyo es consultor de seguridad de la información, con certificación CISA de ISACA y 15 años de experiencia en el mundo de la ciberseguridad. Experiencia en auditorías de seguridad e implantación de SGSI (ISO/IEC 27001). Desempeña la labor de Director de Ciberseguridad, liderando la estrategia de seguridad para la gestión de riesgos IT. Es Responsable del Comité de Cordoba y Co-Líder del Grupo de Expertos de Seguridad en la Asociación itSMF España. Profesor en varios másteres de ciberseguridad (UCLM, Universidad de Sevilla y Universidad de Córdoba). Es autor del blog hacking-etico.com, fundador de Hack&Beers y ponente en congresos de ciberseguridad de ámbito nacional.

LinkedIn:
https://www.linkedin.com/in/miguel-angel-arroyo-moreno

ISSN 2951-8180

Escuela de Gobierno
eGob®
https://escueladegobierno.es

LIVE STREAMING

Sesión de Formación y Certificación en:

Sistema de Gestión de la Inteligencia Artificial

0

Director Académico:

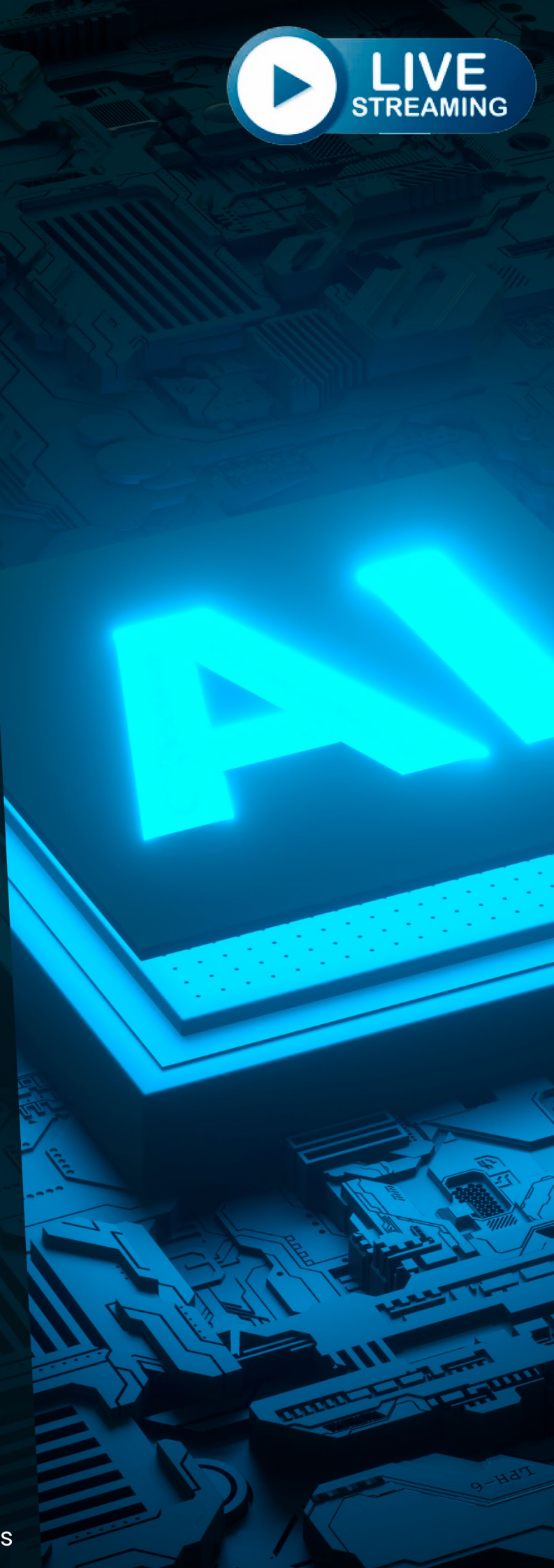
Javier Peris

- Duración 5 horas
- Sesión única
- Miércoles de 16:00 a 21:00 horas
- En Directo y en Remoto
- Basado en la norma ISO 42001:2023
- Examen de Certificación Incluido
- Certificación ISO 42001 Leader
- Plazas limitadas

MPPM® MGEIT® eGob®

Miércoles 10 de Abril

+ 34 96 109 44 44
campus@escueladegobierno.es



ESPECIAL AGOSTO 2024

#TYSC
TECNOLOGIA Y SENTIDO COMUN

índice
DE CONTENIDOS

https://tecnologiaysentidocomun.com

índice

#TYSC

Premios recibidos

Premio 2016 a la Difusión de los Valores de la Gestión y Gobierno TI

El Foro de Profesionales de la Gestión del Servicio en España itSMF otorga a «Tecnología y Sentido Común» el Galardón 2016 a la Difusión de los Valores de la Gestión y Gobierno de Tecnologías de la Información.

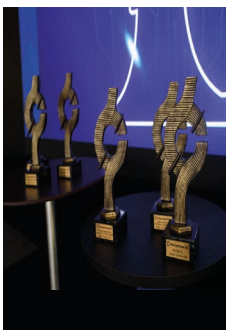
itSMF ESPAÑA

Premio Medio de Comunicación 2018 de la Asociación Profesional Española de Privacidad

La Junta Directiva de la Asociación Profesional Española de Privacidad durante su VI Congreso Nacional de Privacidad APEP celebrado en Madrid otorga el Premio Medio de Comunicación 2018 a Tecnología y Sentido Común #TYSC

apep

Tecnología y Sentido Común "Premio Sapiens" Medio de Comunicación 2022



El Colegio Oficial de Ingeniería Informática de la Comunidad Valenciana entregó el Premio Sapiens Medio de Comunicación 2022 a nuestra Revista "Tecnología y Sentido Común #TYC". El Colegio Oficial de Ingeniería Informática de la Comuni- dad Valenciana COIICV alabó tanto la gran labor de difusión que viene realización Tecnología y Sentido Común desde hace siete temporadas como su capacidad de adaptación y resiliencia adaptándose a nuevos formatos con los que continuar en su labor de evangelización en Buenas Prácticas al conjunto de los profesionales a pesar de la alerta sanitaria con nuevos formatos que partiendo de un programa de Radio y Podcast han permitido seguir llevando su mensajes a través de la Revista Mensual, o el informativo televisivo "El Semanal" de Tecnología y Sentido Común.

COLEGIO OFICIAL DE INGENIERÍA INFORMÁTICA DE LA COMUNITAT VALENCIANA

Premio 2022 ESET al Periodismo y Divulgación eb Seguridad Informática

VI Premios ESET Periodis- mo y Divulgación: Tecnología y Sentido Común Premiada en la Categoría Blogs por el Articulo de Ricard Martínez "Seguridad en el Smartphone".
Los Premios ESET apuestan por la educación y la concienciación de la sociedad en materia de ciberseguridad, y los medios de comunicación son esenciales en este cometido.
Los periodistas y divulgadores son fundamentales para difundir el conocimiento necesario que permita a los usuarios disfrutar de la tecnología de una manera más segura.
Estos VI Premios ESET pretenden fomentar la divulgación de la ciberseguridad.

eset

Agradecimiento de la Asociación Valenciana de Informática Sanitaria AVISA

La Asociación Valenciana de Informática Sanitaria AVISA durante las XIV Jornadas Técnicas que bajo el título "20 Años Implantando TIC en Sanidad" se celebraron en Benidorm en febrero de 2024 hizo entrega de su agradecimiento a Tecnología y Sentido Común por su apoyo y visibilidad a la profesión.

AVIS@ ASOCIACIÓN VALENCIANA DE INFORMÁTICA SANITARIA

Escuela de Gobierno

eGob®

https://escueladegobierno.es

Curso de Doble Certificación en:

Gestión Documental y Gestión del Conocimiento

ISO 30301:2021
ISO 30401:2021

Dirección Académica:
Javier Peris

- Dos formatos para tu comodidad
- Opción A: Remoto en Directo
- Opción B: Virtual con Tutoría
- Basado en las Últimas Normas ISO
- Exámenes de Certificación Incluidos
- Certificación ISO 30300 Leader
- Certificación ISO 30401 Leader
- Solicita tu admisión

MPPM® MGEIT® eGob®

Próxima Convocatoria en Directo
Septiembre 2024

Solicita tu admisión en:

+ 34 96 109 44 44
admisiones@escueladegobierno.es

Automatización de la respuesta ante amenazas

A lo largo de esta temporada de la sección de Hack&News hemos hablado en diferentes artículos sobre amenazas, gestión de riesgos y la importancia de contar con un proceso de inteligencia en amenazas que permitiera a la organización disponer de información de valor para tomar las mejores decisiones en el tratamiento de los riesgos, ya sea para disminuir la probabilidad de que las amenazas se puedan materializar o el impacto en caso de que ocurriera el evento de la dicha amenaza.

La proliferación de estas amenazas hace que sea mucho más complicado identificarlas, protegerse ante ellas, detectar un evento de amenaza, responder ante ellas o, en el peor de los casos, recuperarse de un incidente provocado por alguna de estas amenazas.

Precisamente, en el párrafo anterior, hemos repasado las cinco funciones del marco de trabajo de ciberseguridad del **NIST** (*National Institute of Standards and Technology*); **Identificación, Protección, Detección, Respuesta y Recuperación**. En este artículo vamos a centrar en la función de respuesta, enfatizando la importancia de automatizar dicha respuesta en la medida de lo posible, porque sería prácticamente imposible e ineficiente atender a cada una de ellas de manera manual.

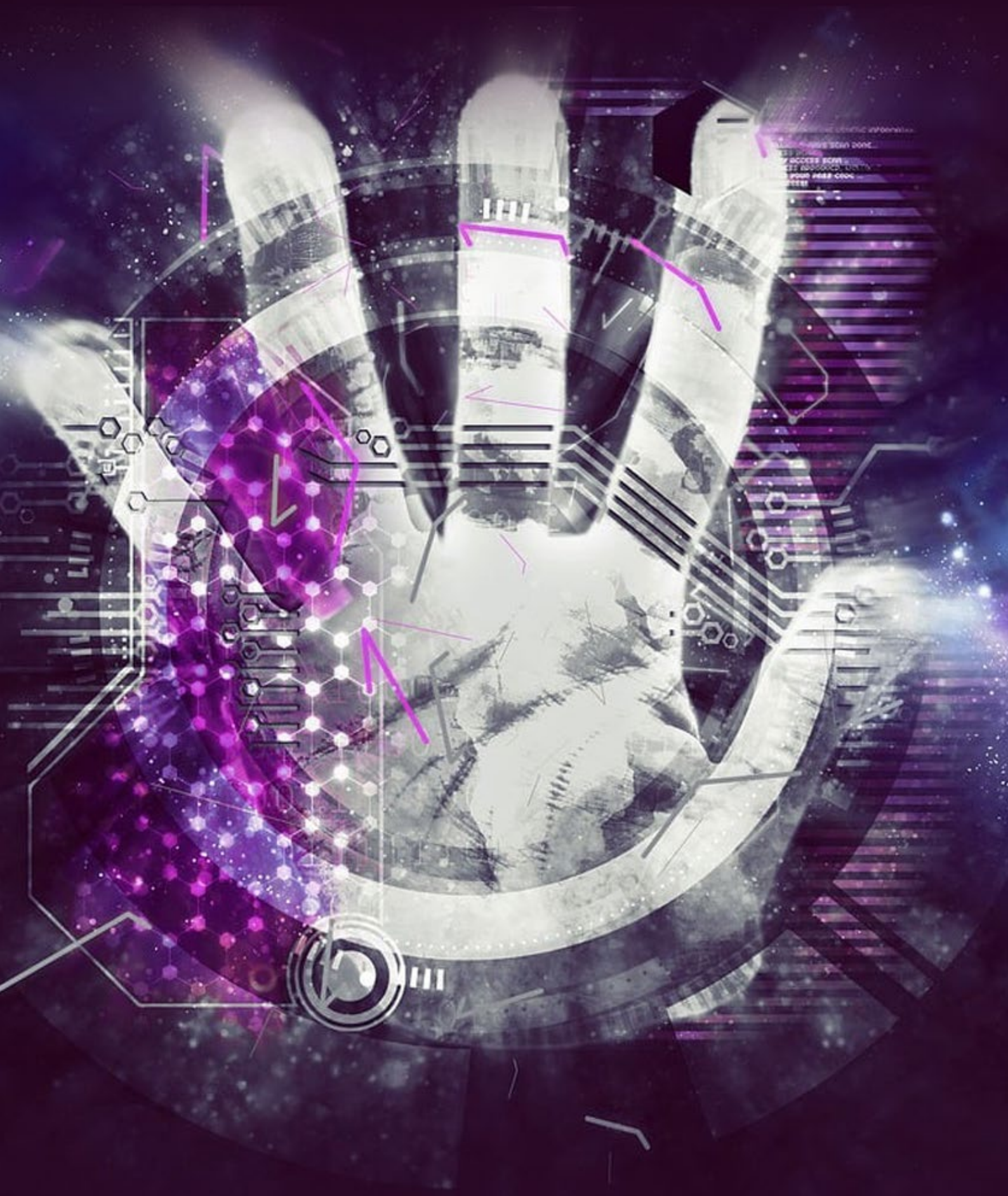
Afortunadamente, en la actualidad el mercado nos ofrece diferentes soluciones para la respuesta automatizada ante amenazas, aportando más eficacia y eficiencia en esta tarea. Esto no implica que el "ojo clínico" del analista vaya a separar de esta tarea, pero podría quedar en un segundo plano, para verificar la alerta, descartar un falso positivo, detectar un posible falso negativo, identificar posibles errores en el proceso o posibles oportunidades de mejora de este.

Uno de los ejemplos más claro de este tipo de soluciones son las herramientas antimalware (contra código malicioso) que, como sabréis, ha sufrido un importante cambio y evolución. Entre los cambios más importantes de esta evolución se podrían destacar dos. Por un lado, la integración de la inteligencia artificial para basar la detección de amenazas en el análisis de comportamiento, en lugar de hacerlo basándose en firmas (patrones) del código malicioso. Por otro lado, incluir la capacidad de respuesta ante amenazas.

Las soluciones de tipo **EDR** (*Endpoint Detection & Response*) son el mejor ejemplo de este tipo de soluciones. Esta evolución del antivirus tradicional permite, no solo detectar, sino también responder ante la amenaza, basándose en unas "recetas" (playbooks) previamente configuradas. Este tipo de soluciones a su vez han ido evolucionando, y un ejemplo claro son las soluciones de tipo **XDR** (e*Xtended Detection & Response*), que extienden la funcionalidad de los EDR para incluir también, por ejemplo, las cargas de trabajo de la nube.

Pero esta automatización de la respuesta ante amenazas no se queda solo en el puesto

CONTINÚA EN PRÓXIMA PÁGINA



de trabajo o servidor. Esta misma funcionalidad la podemos encontrar en otro tipo de soluciones más orientadas a detectar amenazas en la red. En este caso estaríamos hablando de soluciones **NDR** (*Network Detection & Response*), y que tienen como objetivo detectar actividades maliciosas en las comunicaciones de red y responder ante este tipo de amenazas.

El proceso de automatización de la respuesta ante amenazas se puede complementar con otras soluciones, como son los **SIEM** (*Security Information and Event Management*) para la recolección de logs y eventos de seguridad y la correlación de estos o las soluciones de tipo **SOAR** (*Security Orchestration Automation and Response*) que, como su nombre indica, permitiría "orquestar" y automatizar la respuesta ante amenazas.

En un escenario ideal en una organización, además de contar con soluciones de detección y respuesta como los EDR, XDR o NDR, los registros y eventos de seguridad serían recolectados y correlacionados por el SIEM, y en caso de detectar algún tipo de amenaza, notificar al SOAR para que se comunique con algún mecanismo de seguridad, como puede ser un cortafuegos, y crear una regla de seguridad en éste para bloquear cierto tráfico de la red.
Por ejemplo, imaginemos que un EDR ha detectado una amenaza en un equipo, lo cual generaría una alerta que sería recogida por el SIEM, y éste a su vez notificaría al SOAR para que se comunique con el cortafuegos y no permitiera que el equipo afectado pueda establecer una conexión con el exterior (para prevenir posible fuga de información). Esto es solo un ejemplo muy simple de la capacidad que tienen este tipo de soluciones y que aportarían mucho valor en las actividades de detección y respuesta ante amenazas.

Como siempre, espero que el artículo sea de vuestro agrado, interés y os pueda resultar útil.

¡Nos leemos!

Escuela de Gobierno

eGob®

https://escueladegobierno.es

Curso de Doble Certificación en:

Inteligencia Estratégica y Gestión de la Innovación

ISO 56002:2019
ISO 56006:2021

Dirección Académica:
Javier Peris

- Dos formatos para tu comodidad
- Opción A: Remoto en Directo
- Opción B: Virtual con Tutoría
- Basado en las Últimas Normas ISO
- Exámenes de Certificación Incluidos
- Certificación ISO 56002 Leader
- Certificación ISO 56006 Leader
- Solicita tu admisión

MPPM® MGEIT® eGob®

Próxima Convocatoria en Directo
Septiembre

Solicita tu admisión en:

+ 34 96 109 44 44
campus@escueladegobierno.es

Estructurando nuestras contramedidas con D3FEND

Comenzamos una nueva temporada en Hack&News, con nuevos contenidos que espero que disfrutéis tanto como yo he disfrutado creándolos. Durante la temporada pasada se habló mucho sobre gestión de riesgos, lo que para mí es la piedra angular del proceso de gestión de la seguridad de la información en cualquier organización, independientemente de su tamaño o naturaleza. Piedra angular porque la fase de evaluación de riesgos nos va a permitir a identificar las amenazas que pueden poner en peligro nuestros sistemas de información, calculando el riesgo en base a la probabilidad de que se materialicen y su posible impacto.

Por lo tanto, al final todo gira en torno a la identificación de las amenazas, evaluación de estas y la implantación de medidas de defensa que permitan defendernos ante estas amenazas, reduciendo o mitigando su riesgo. Obviamente, no termina aquí nuestro trabajo para la protección de nuestros sistemas de información, por ejemplo, querremos mejorar continuamente nuestros procesos y para ello deberemos medir la eficacia y eficiencia de los mecanismos de seguridad implantados. Pero para este artículo, nos vamos a centrar en la identificación de las amenazas, y concretamente, en cómo defendernos ante ellas.

En artículos anteriores hemos hecho varias referencias al proceso de inteligencia en amenazas (CTI, Cyber Threat Intelligence), también a MITRE ATT&CK, una magnífica herramienta para conocer y entender las diferentes tácticas, técnicas y procedimientos (TTP) utilizados por los atacantes. MITRE ATT&CK nos proporciona un modelo ofensivo con una estructura clara con información de las distintas técnicas (amenazas) que pueden poner en peligro nuestros activos.

CONTINÚA EN PRÓXIMA PÁGINA

Una vez identificados los diferentes TTP que pueden afectar a nuestra organización, a nuestros artefactos digitales (activos), es el momento de tomar decisiones e implantar medidas para contrarrestar estas técnicas. En primera instancia, podemos acudir al mercado de la ciberseguridad, con miles de fabricantes dispuestos a ofrecernos su gama de productos.

No siempre es fácil identificar la solución perfecta para combatir una amenaza concreta. La misma funcionalidad está presente en diferentes productos, de diferentes fabricantes. Los productos evolucionan, nos invaden/encantan los acrónimos (FW, IPS, IDS, WAF, NAC, AV, EPP, EDR, XDR, NDR, MDR, SIEM, SOAR, UBA, UEBA, ZTA, SASE, CASB…), lo que dificulta realmente decidir en qué invertir nuestro presupuesto en ciberseguridad, un presupuesto que no es infinito y que suele rondar el 10% del total del presupuesto de IT en una organización.

Una buena opción es empezar por el marco de trabajo de la ciberseguridad de NIST, con las cinco funciones básicas de la ciberseguridad: Identificar, Proteger, Detectar, Responder y Recuperar. Ubicar posibles soluciones del mercado en cada una de estas funciones puede ser una buena aproximación.

La otra opción, y pensando en estructurar bien nuestras contramedidas, es utilizar un marco de trabajo similar al ATT&CK de MITRE, pero en este caso con técnicas (defensivas), es decir, con controles / medidas de seguridad / contramedidas para contrarrestar eficazmente las técnicas ofensivas del ATT&CK.

Todo "queda en casa" porque estamos hablando de otra herramienta de MITRE, con menos recorrido en años que ATT&CK, pero que, si sabemos utilizarla bien, nos puede resultar de gran ayuda. Se trata de **MITRE D3FEND**.

MITRE y la **NSA** lanzaron D3FEND con la intención de proporcionar un modelo defensivo, organizado en funciones y que tiene como objetivo principal correlacionar medidas de defensa con las técnicas ofensivas de ATT&CK.

D3FEND nos puede ayudar a decidir dónde invertir nuestro presupuesto. Una vez identificadas las técnicas ofensivas, amenazas o debilidades que pueden poner en peligro nuestros activos de información, podemos identificar las medidas a implantar para contrarrestarlas. Para ello, D3FEND nos proporciona una matriz, similar a las que nos ofrece ATT&CK, categorizadas por tácticas, y cada táctica con un conjunto de técnicas, prácticamente de la misma manera que lo hace ATT&CK con sus matrices de técnicas ofensivas.

La propuesta de MITRE es relacionar estos dos modelos, ofensivo (ATT&CK) y defensivo (D3FEND), introduciendo el artefacto digital (activo) como centro de la relación. Por un lado, ATT&CK **produce** técnicas ofensivas que pueden poner en peligro el artefacto digital y, por otro lado, D3FEND **observa** mediante técnicas defensivas posibles acciones ofensivas sobre el activo (artefacto digital).

Veamos un caso práctico para entender mejor esta relación. Existen técnicas ofensivas para explotar un servicio o ejecutar una escalada de privilegios, concretamente en ATT&CK podemos encontrar la técnica "*Exploitation for Privilege Escalation - T1068*". Pues bien, esta técnica tiene la capacidad de modificar un artefacto digital, en este caso un proceso. Para contrarrestar esta técnica ofensiva, D3FEND ofrece diferentes técnicas defensivas para detectar estas técnicas, concretamente estaríamos hablando de la técnica "*D3-PCSV (Process Code Segment Verification)*", que tiene como finalidad verificar el segmento de código de ejecución del proceso, y controlar posibles cambios en memoria de este proceso, que puedan ser utilizados para escalar privilegios de un usuario en el sistema.

Esto es solo un pequeño ejemplo del potencial que tiene MITRE D3FEND, un **complemento** perfecto para nuestro MITRE ATT&CK y que nos permite diseñar un modelo defensivo para estructurar mejor nuestras contramedidas.

Como siempre, espero que el artículo sea de vuestro agrado, interés y os pueda resultar útil.

¡Nos leemos!

Escuela de Gobierno
eGob®
https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Gobierno del Tiempo y Gestión de la Productividad

Director Académico:
Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación TSG4® Yellow Belt
- Certificación UNE 71404 Executive
- Módulo 1: MasterGEIT®
- Módulo 1: MasterPPM®

MPPM® MGEIT® eGob®

Del 15 al 23 de marzo

+ 34 96 109 44 44
campus@escueladegobierno.es

Ransomware: del perfilado a la protección

INTRODUCCIÓN

Tal y como ya hemos mencionado en otros artículos de esta sección todo gira en torno a la gestión de riesgos, y para que este proceso sea lo más eficaz y eficiente posible, tendremos que volcar muchos esfuerzos en la evaluación de riesgos, y concretamente en entender las amenazas que nos rodean y pueden poner en peligro nuestros sistemas de información. No nos podemos defender de algo que no conocemos. Necesitamos saber cómo piensan los atacantes, que tácticas y técnicas utilizan, en resumen, obtener información de calidad que nos permita tomar las mejores decisiones para defendernos ante esas amenazas.

En un artículo anterior de esta sección ya hemos hablado sobre el perfilado de las amenazas, y pusimos como ejemplo el perfilado de una amenaza de tipo ransomware. **NIST** (*National Institute of Standards and Technology*) publica unos informes a los que denomina **NISTIR** (*NIST Interagency or Internal Reports*), y uno de estos informes, concretamente el **NISTIR 8374** habla sobre la gestión de riesgos del ransomware. Gran parte de este informe se basa en estudiar el perfil de este tipo de amenazas, relacionarlo con las funciones básicas del **CSF** (*Cyber Security Framework*) de **NIST** (*Identificar, Proteger, Detectar, Responder y Recuperar*) y proponer una serie de medidas para reducir o mitigar el riesgo de que un ransomware se pueda materializar en una organización.

POSIBLES CONTROLES DE SEGURIDAD

El informe nos proporciona una tabla detallada de posibles controles de seguridad que podemos utilizar, categorizados en las funciones básicas del CSF de NIST, y con subcategorías y referencias para segregar mejor la información y sea más fácil al lector del informe entender qué controles pueden resultar más eficaces para su organización a la hora de protegerse frente al ransomware.

A la hora de proponer posibles controles de seguridad, el documento toma como referencia diferentes marcos de trabajo y normas. Por un lado, identifica posibles controles de la **ISO/IEC 27001 (Anexo A)**, para reducir o mitigar el riesgo, y por otro lado la publicación **NIST SP 800-53**, una magnífica referencia para la seguridad de la información y que nos proporciona un amplio catálogo de controles de seguridad.

Finalmente, la tabla se completa con una columna donde se explica cómo aplica estas medidas a la hora de gestionar el riesgo que el ransomware pueda suponer.

AMPLIANDO CON CONTROLES MÁS TÉCNICOS

Los que estéis familiarizados con los controles de la ISO/IEC 27001 (Anexo A) y del NIST SP 800-53, sabréis que estas referencias no profundizan mucho en el aspecto técnico (sobre todo el Anexo A de la ISO/IEC 27001). Nos proporciona una guía y una muy buena base para poder definir nuestra estrategia de seguridad a la hora de afrontar los riesgos.

CONTINÚA EN PRÓXIMA PÁGINA

En la industria de la ciberseguridad, existen muchos repositorios y marcos de trabajo que nos proporcionan controles de seguridad con un detalle mucho más técnico. Como ejemplo, podríamos hablar de **CIS Controls** o del propio **MITRE D3FEND**, al que ya le hemos dedicado un artículo en esta sección.

El perfilado de la amenaza del ransomware que nos proporciona NIST con su informe NISTIR 8374 es muy interesante y útil, y creo que el complemento perfecto a la tabla que nos proporciona el informe sería la correlación de controles más técnicos para afrontar y defendernos eficazmente ante esta y cualquier otra amenaza.

Para entenderlo mejor, veamos un ejemplo basándonos en la tabla del perfilado de la amenaza que nos facilita el informe NISTIR 8374. Supongamos que queremos implantar un control, concretamente tecnología para la protección del sistema de información. En el informe aparece como "*Protective Technology*", con el código PR.PT (PR de Protección, del CSF de NIST). Una de las acciones recomendadas en este apartado es la de aplicar el **principio de mínimo privilegio** (*PoLP, Principle of Least Privilege*), y para ello el informe propone varios controles de la ISO/IEC 27001 (Anexo A) como, por ejemplo, el control **A.9.1.2** o los controles **AC-3 y CM-7** del NIST SP 800-53.

El complemento a estos controles, más genéricos, serían los controles técnicos de CIS Controls, o técnicas defensivas de MITRE D3FEND. En este último caso, podemos aplicar la técnica defensiva D3-UAP, que hace referencia a la gestión de los permisos de usuarios, para garantizar que los usuarios tienen solo los permisos que realmente necesitan para realizar sus tareas diarias en el entorno corporativo.

RESUMEN

Esto es solo un pequeño ejemplo de la aplicación del perfilado de una amenaza, la identificación de controles genéricos de seguridad propuestos por la industria como ISO/IEC 27001 (Anexo A) o NIST SP 800-53 y la aplicación de controles de seguridad más específicos (y técnicos) basados en otras referencias de la industria como CIS Controls, o más concretamente, MITRE D3FEND, del que ya hemos hablado en otro artículo, y seguiremos tratando en esta sección.

Como siempre, espero que el artículo sea de vuestro agrado, interés y os pueda resultar útil.

¡Nos leemos!

Escuela de Gobierno

eGob®

https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Análisis de Negocio y Gestión por Procesos

Director Académico:

Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación BPA Leader
- Certificación BPM Executive
- Módulo 2: MasterGEIT®
- Módulo 2 MasterPPM®

MPPM® MGEIT® eGob®

Del 5 al 13 de abril

+ 34 96 109 44 44
campus@escueladegobierno.es

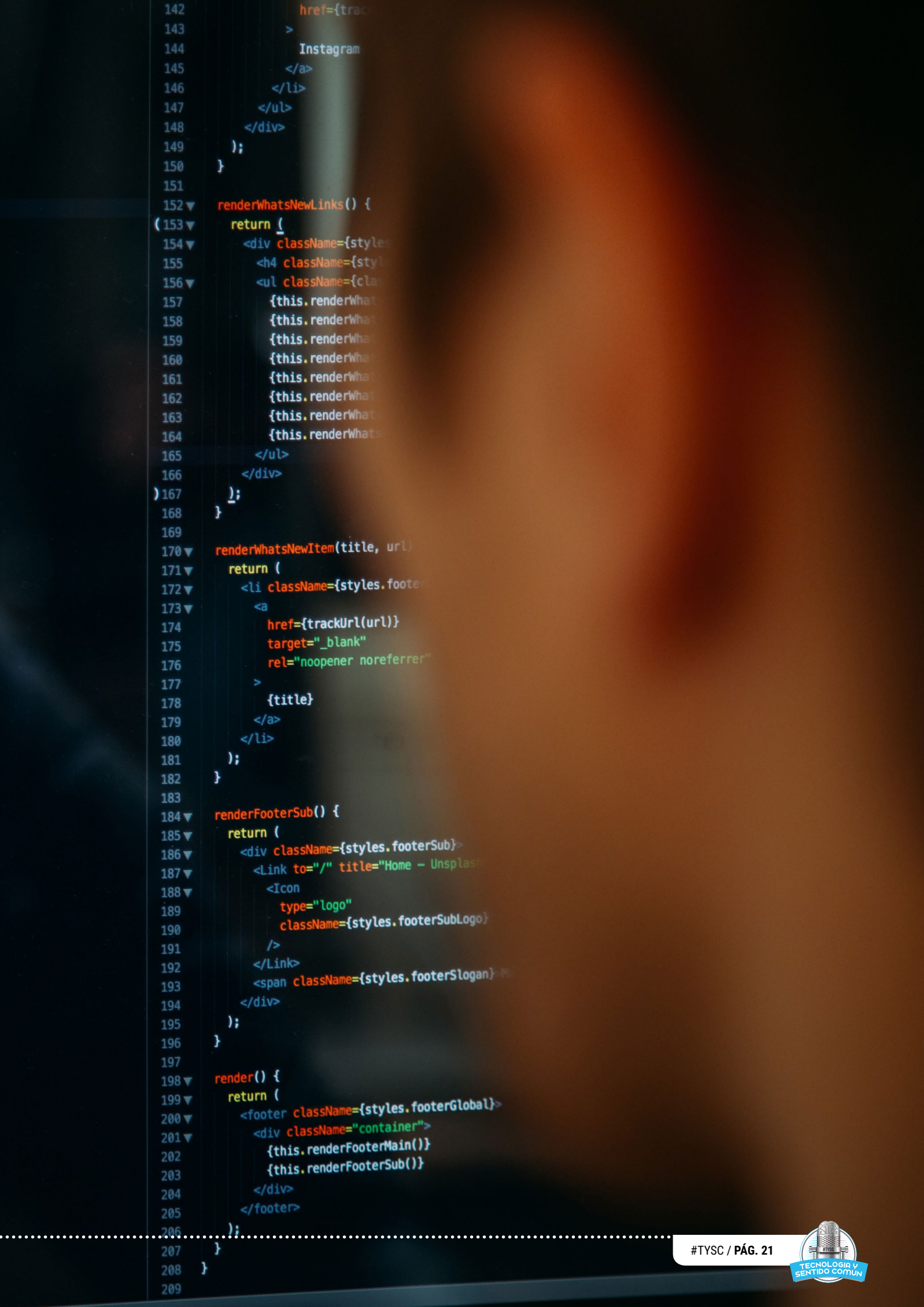
Perfiles profesionales en el mundo de la ciberseguridad

Introducción

No es la primera vez, ni será la última, que hablamos de la complejidad de la situación actual en referencia a las amenazas cibernéticas y al cibercrimen en general. El hecho de que el cibercrimen mueva tantísimo dinero supone una motivación más para los ciberdelincuentes. Unos grupos de ciberdelincuentes cada vez más profesionalizados, con más y mejores recursos, con estructuras organizativas que ya las quisieran muchas PYME en España, con conocimientos cada vez avanzados y con herramientas cada vez más especializadas.

Por otro lado, nos encontramos con la incesante adopción de la tecnología en los procesos diarios de cualquier organización. Ya sea tecnología de la información, cada vez más presente en cualquier organización, independientemente de su tamaño o naturaleza, o tecnología de la operación, como por ejemplo en entornos industriales. Sea cual sea la tecnología empleada, la integración de ésta ya conlleva unos riesgos que cada organización tendrá gestionar, ya que la tecnología de manera inherente se expone a posibles vulnerabilidades, así como a amenazas que puedan explotar dichas vulnerabilidades. A esto hay que añadir, que los entornos tecnológicos de las organizaciones son cada vez más complejos con usuarios deslocalizados, con la integración de servicios en la nube o la convergencia del mundo IT (Tecnología de la Información) con el mundo OT (Tecnología de la Operación).

CONTINÚA EN PRÓXIMA PÁGINA



```
                href={trac
              >
                Instagram
              </a>
            </li>
          </ul>
        </div>
      );
    }

    renderWhatsNewLinks() {
      return (
        <div className={styles
          <h4 className={styl
          <ul className={clas
            {this.renderWhat
            {this.renderWha
            {this.renderWha
            {this.renderWha
            {this.renderWha
            {this.renderWha
            {this.renderWha
            {this.renderWhats
          </ul>
        </div>
      );
    }

    renderWhatsNewItem(title, url)
      return (
        <li className={styles.foote
          <a
            href={trackUrl(url)}
            target="_blank"
            rel="noopener noreferrer"
          >
            {title}
          </a>
        </li>
      );
    }

    renderFooterSub() {
      return (
        <div className={styles.footerSub}>
          <Link to="/" title="Home — Unsplas
            <Icon
              type="logo"
              className={styles.footerSubLogo}
            />
          </Link>
          <span className={styles.footerSlogan}>M
        </div>
      );
    }

    render() {
      return (
        <footer className={styles.footerGlobal}>
          <div className="container">
            {this.renderFooterMain()}
            {this.renderFooterSub()}
          </div>
        </footer>
      );
    }
  }
```

Carrera de fondo en desventaja

Ante esta situación, lo que está claro es que los ciberdelincuentes siempre nos van a llevar ventaja en esta carrera de fondo que es la ciberseguridad. Son estos grupos de ciberdelincuentes los que marcan la tendencia en cuanto al descubrimiento y explotación de vulnerabilidades, desarrollando nuevas tácticas, técnicas y procedimientos para comprometer los sistemas de información de las organizaciones a través de las tecnologías que éstas van incorporando a su infraestructura.

En el lado defensivo, las personas que en las organizaciones se dedican a diseñar las estrategias de ciberseguridad, definir los planes de seguridad o ejecutar los procedimientos de ciberseguridad suelen "ir a rebufo", como en la Fórmula 1. Al igual que en la Fórmula 1, cuanto más cerca estés del coche de delante (los ciberdelincuentes), mejor, ya que estaremos al tanto de nuevas vulnerabilidades, amenazas y técnicas de explotación.

Perfiles especializados de ciberseguridad

El problema es que, mientras los ciberdelincuentes cuentan en "*boxes*" con un grupo nutrido y bien armado, en la mayoría de las organizaciones, el número de "*ingenieros y mecánicos*" es bastante limitado en cuanto a número. Pero el problema no es solo de números, también de la especialización de estos "ingenieros y mecánicos".

Lo que intento explicar con este símil con la Fórmula 1, es que con la situación tan compleja que estamos viviendo y con tecnologías tan diferentes que coexisten en nuestras organizaciones, lo que conlleva a nuevas vulnerabilidades y nuevos tipos de amenazas, necesitamos perfiles especializados de ciberseguridad en esas nuevas tecnologías. No podemos pedirle a un Administrador Senior de Sistemas, que además de configurar de manera seguridad los servidores Windows Server 2019, también esté capacitado para configurar de manera segura el entorno en la nube en Azure, desarrolle de manera segura una aplicación, o configure de manera segura el SCADA del entorno industrial.

Las posibles vulnerabilidades y amenazas específicas de un entorno cloud, no tienen nada que ver con lo que nos podemos encontrar en entornos "*on-premise*". Se necesita de un perfil especializado capaz de identificar los riesgos del entorno cloud, entender qué vulnerabilidades les puede afectar, qué probabilidad hay que se puedan explotar y qué impacto tendría. Para ello, este perfil especializado necesitará conocer y entender las amenazas específicas de un entorno cloud.

En entornos industriales, esta especialización es todavía mucho más necesaria, porque la tecnología de la operación, aunque la tendencia es la convergencia entre IT y OT, es totalmente diferente a la tecnología de la información, otro tipo de vulnerabilidades, otro tipo de amenazas, y, por lo tanto, otro tipo de riesgos.

Esta identificación de perfiles especializados en ciberseguridad no aplica solo a perfiles de seguridad defensiva, también aplica a perfiles de seguridad ofensiva como pueden ser los pentesters. Aquí la diferencia más clara la podemos encontrar entre perfiles especializados en evaluar la seguridad de sistemas y redes y perfiles especializados en evaluar la seguridad de una aplicación. Mientras que el primero requiere de conocimientos específicos en sistemas operativos, redes, vulnerabilidades y amenazas específicas de estos entornos, el segundo requiere de conocimientos de desarrollo, vulnerabilidades y amenazas específicas de una aplicación.

En resumen, para que la protección de nuestros sistemas de información sea la más eficaz y eficiente posible, necesitamos de perfiles especializados, ya sea internos o contratados a terceros.

Como siempre, espero que el artículo sea de vuestro agrado, interés y os pueda resultar útil.

¡Nos leemos!

Escuela de Gobierno
eGob®
https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Gestión de Proyectos

OpenPM² (PjM) + ISO 21502

Director Académico:
Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación OpenPM² (PjM) Executive
- Certificación ISO 21502 Leader
- Módulo 3: MasterGEIT®
- Módulo 3 MasterPPM®

MPPM® MGEIT® eGob®

Del 19 al 27 de abril

+ 34 96 109 44 44
campus@escueladegobierno.es

Reflexiones de un CISO

Siendo el último artículo del año me ha parecido oportuno enfocarlo desde la reflexión, desde la reflexión de un CISO en base a lo vivido durante este 2023, en cuanto a preocupaciones, sensaciones y recomendaciones.

Preocupaciones

Como la gran mayoría de los que estáis leyendo este artículo, la mayor preocupación como CISO es que la información de una organización esté bien protegida. Las noticias que nos llegan continuamente desde nuestros entornos y medios de comunicaciones no son nada optimistas. Cuando no hablan de un ciberataque a una empresa de tu sector, hablan de nuevas técnicas y herramientas utilizadas por los ciberdelincuentes capaces de evadir nuestras medidas de seguridad.

A esto hay que añadirle la actual situación geopolítica, con diferentes conflictos activos, y que nos trae un panorama de ciberguerras bastante complejo, con ataques a infraestructuras críticas de los estados que están inmersos de manera directa en dichos conflictos, incluso aquellos que, de alguna manera más indirecta, también lo están y sufren este tipo de ataques.

CONTINÚA EN PRÓXIMA PÁGINA

Lo único positivo de estas preocupaciones en materia de ciberseguridad, es que obligan al CISO y a la organización a estar en permanente estado de alerta, sin tiempo a la relajación, y adoptar una postura de seguridad más proactiva, basada en la gestión continua del riesgo.

Sensaciones

A pesar de la complejidad de la situación, son sensaciones positivas en cuanto a que hay ciertos tipos de ataques cuya efectividad por parte del ciberdelincuente han disminuido. *¿No os da la sensación de que cada vez hay menos casos de ransomware?* Ojo, no me refiero al número de ataques, aunque posiblemente también haya disminuido, pero creo que las organizaciones están cada vez más preparadas ante este tipo de ataques, tanto desde el punto de vista de la prevención, con la formación y concienciación de los usuarios, como desde la propia protección, detección y respuesta a través de mecanismos como los antivirus (EDR, XDR, …) o los SIEM (*Security Information and Event Management*).

Las organizaciones apuestan cada vez más por la monitorización de sus eventos de seguridad, lo que les ayuda a detectar a tiempo cualquier amenaza o incidente de seguridad, siendo cada vez más habitual encontrar soluciones de tipo SIEM para monitorizar dichos eventos o incluso organizaciones que contratan un SOC (Centro de Operaciones de Seguridad) externo.

Mención especial a los estándares, normativas y directivas de seguridad. Las organizaciones empiezan a mostrar interés por estándares como ISO/IEC 27001, y otras, por obligación, porque les aplica adecuarse a reglamentos o directivas como el Esquema Nacional de Seguridad (ENS) o NIS2.

Recomendaciones

Como he mencionado ya en otros artículos, es fundamental gestionar el riesgo de manera continua. La ciberseguridad no es un acto puntual en el tiempo. Como proceso crítico dentro de cualquier organización, se tiene que ejecutar de manera sistemática.

El proceso crítico dentro de la ciberseguridad es la gestión de riesgos, y a su vez, la evaluación de estos riesgos es una de las tareas más importantes. Implantar un programa de inteligencia de amenazas (*CTI, Cyber Threat Intelligence*) ayudará a las organizaciones a entender cómo piensan y actúan los adversarios, qué técnicas y herramientas utilizan, y esta información les permitirá analizar mejor las amenazas, la probabilidad de que se materialicen y el impacto en caso de que esto ocurra. Es decir, podrán evaluar de una manera mucho más eficaz los riesgos, lo que repercutirá de manera muy positiva en el tratamiento de dichos riesgos.

Por último, y no menos importante, se recomienda disponer de un Sistema de Gestión de Seguridad de la Información y un Sistema de Gestión de Continuidad de Negocio, basado en estándares como ISO/IEC 27001 o ISO 22301, respectivamente. Los sistemas de gestión son herramientas que van a permitir a las organizaciones a planificar, ejecutar, controlar y mejorar los diferentes procesos de seguridad de la información o continuidad de negocio en las organizaciones, tomando como referencia las buenas prácticas de estos estándares, independientemente de que el objetivo final sea la certificación o no. Lo realmente importante es estar bien protegido y poder garantizar la continuidad del negocio.

La certificación de estos estándares tiene que ser una consecuencia de las buenas prácticas implantadas. Recuerda, "*cumplimiento no es lo mismo que cumplo y miento*".

Como siempre, espero que el artículo sea de vuestro agrado, interés y os pueda resultar útil.

¡Nos leemos!

Escuela de Gobierno
eGob®
https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Gestión de Programas

OpenPM² (PgM) + ISO 21503

Director Académico:
Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación OpenPM² (PgM) Executive
- Certificación ISO 21503 Leader
- Módulo 4: MasterGEIT®
- Módulo 4 MasterPPM®

MPPM® MGEIT® eGob®

Del 3 al 11 de mayo

+ 34 96 109 44 44
campus@escueladegobierno.es

Evento de Cierre de Temporada 2024 de las Revistas Tecnología y Sentido Común y Stakeholders.news

El 19 de julio de 2024, las revistas Tecnología y Sentido Común y Stakeholders.News celebraron el Cierre de su novena y tercera temporada respectivamente con un interesante evento en la sede de UNE Asociación Española de Normalización, en Madrid.

En una tradición que se inició el pasado año 2023, las revistas Tecnología y Sentido Común y Stakeholders.News prepararon un cierre de temporada a la altura tanto de la calidad de sus contenidos como del nivel de sus colaboradores. Con la inestimable colaboración de UNE Asociación Española de Normalización, el día 19 de julio de 2024 se reunió en Madrid un granado grupo de profesionales, entre los que estaban algunos de los colaboradores de nuestras revistas.

El evento comenzó con una bienvenida a cargo de Paloma García, Directora de Programas de Normalización y Grupos de Interés de UNE, y de Javier Peris, Director de las revistas Tecnología y Sentido Común y Stakeholders.News, en el que agradecieron a los presentes su asistencia, sobre todo a aquellos afectados por el incidente global en sistemas de información de grandes compañías de todo tipo que se dio en esa fecha.

CONTINÚA EN PRÓXIMA PÁGINA

Evento Protagonista

Tras la bienvenida, se dio paso al ponente principal del evento, Ramsés Gallego, primer español (y tercer europeo) en ser nombrado para el "Hall of Fame" de ISACA internacional, evento que tuvo lugar en este 2024. Renombrado conferenciante, deleitó al público asistente con su charla "De Gestionar a Gobernar …. con 'G' de Ganar", en la que glosó las bondades de dar ese salto hacia el gobierno de las Tecnologías de la Información, sobre todo en los aspectos relacionados con la ciberseguridad. Ciertamente, un lujo contar con él para el evento.

CONTINÚA EN PRÓXIMA PÁGINA

Evento Protagonista

El siguiente acto fue la mesa redonda con cinco de los autores que colaboran con la revista Tecnología y Sentido Común en el que participaron: Alejandro Aliaga líder de la seccion “Radio Security”, Renato Aquilino líder de la sección “Marcos y Normas”, Marlon Molina líder de la seccion “Es Tendencia”, Marcos Navarro líder de la seccion Ai Robot” que a partir de la proxima temporada pasará a llamarse “Ai Futuro” y Manuel Serrat líder de la seccion “Futuro y Seguridad”.

Durante la mesa redonda de Tecnologia y Sentido Común, estos cinco representantes respondieron a las preguntas del presentador y director de la revista, Javier Peris, acerca de los contenidos de la temporada que terminaba, y de qué se podía esperar de sus secciones en cuanto a contenidos y novedades en la décima temporada de la revista.

Alejandro Aliaga centró su intervención en recordad que el objetivo de su sección “Radio Security” es concienciar a los lectores de que existen vectores de ataque no convencionales asociados con las comunicaciones inalámbricas, y que, por la evolución tecnológica, es difícil que éstos se reduzcan.

Por su parte, Renato Aquilino, en su sección “Marcos y Normas” ha centrado sus contenidos en poner de manifiesto el gap existente entre las normas y quienes las escriben, frente a quienes las han de convertir en realidad en las organizaciones, algo que resulta extremadamente complejo en algunos casos.

Por lo que respecta a Marlon Molina, con su sección “Es Tendencia”, ha tratado de contar a los lectores en esta temporada que termina los temas que, mes a mes, han atraído la atención del sector por diferentes motivos.

Marcos Navarro anunció que su sección, a partir de la décima temporada, cambiaba de enfoque y de nombre, para explicar cómo es la vida en 2024, sólo dentro de diez años, gracias a tecnologías como la Inteligencia Artificial y la Robótica.

En cuanto a Manuel Serrat, explicó que con su sección “Futuro y Seguridad” ha tratado de poner el foco en aquellos aspectos de la evolución tecnológica que pueden suponer algún tipo de riesgo, y concienciar a los lectores para evitarlos.

CONTINÚA EN PRÓXIMA PÁGINA

Evento Protagonista

Finalizada esta mesa redonda, se llevó a cabo la segunda Mesa Redonda, que contó con cuatro de los colaboradores de la revista Stakeholders.News: Juan Manuel Domínguez líder de la Seccion "Organizaciones Resilientes", Luis Morán líder de la sección "Personas y Procesos", José Antonio Puentes líder de la seccion "Tendiendo Puentes" y Juan Jesús Urbizu líder de la seccion "Tecno-transformación".

Dada la temática de la revista, fundamentalmente dirigida a aquellos profesionales de la gestión de proyectos, programas y portfolios y áreas conexas, las preguntas para los participantes en la mesa redonda se centraron en poner de relieve la necesaria aplicación de estándares y buenas prácticas en cada uno de los ámbitos que tratan las diferentes secciones de la revista.

Juan Manuel Domínguez, a través de su sección "Organizaciones Resilientes", expuso aspectos tales como que, en Japón, con aproximadamente 120 millones de habitantes, hay 45.000 empresas centenarias, frente a las poco más de 5.000 que existen en España con 48 millones de habitantes.

Luis Moran comentó algunos de los temas que había tratado durante esta tercera temporada en su sección "Personas y Procesos", y avanzó alguna de las cuestiones que va a tratar en la cuarta temporada de la revista.

José Antonio Puentes (sección "Tendiendo Puentes") compartió con los presentes algunas vivencias personales, relacionadas con las dificultades que la gestión de proyectos enfrenta en determinadas organizaciones.

Por último, Juan Jesús Urbizu, que estas temporadas ha escrito en su sección "Tecno Transformación", apuntó algunas de las cuestiones más relevantes a las que se enfrenta el gestor de proyectos, programas y portfolios en relación con la digitalización de las organizaciones, y más desde la irrupción para el gran público de los sistemas de inteligencia artificial.

CONTINÚA EN PRÓXIMA PÁGINA

Tras las dos mesas redondas, Javier Peris anunció el nombramiento de los tres embajadores de la revista Stakeholders.News en Hispanoamérica más concretamente en Puerto Rico, Uruguay y El Salvador.
En Puerto Rico contaremos cada mes con la participacion de Nesty Delgado en Uruguay contaremos con Daniel Sorokins y en el pais de la eterna sonrisa "El Salvador contaremos con Luis Guardado quienes fueron nombrados y serán a partir de ahora Embajadores de Stakeholders.news.

Los actos de cierre de temporada terminaron con la entrega de los premios Tecnología y Sentido Común y Stakeholders. News, en esta ocasión en su edición de 2024.

El "Premio Tecnología y Sentido Común 2024" recayó en el Consejo General de Colegios Profesionales de Ingeniería Informática (CCII), por su aportación al progreso de la sociedad de la información, el impulso al desarrollo ético de los avances tecnológicos y la defensa y promoción de la ingeniería en informática. El premio fue recogido por José García Fanjul, secretario del CCII y vicedecano del Colegio Oficial de Ingenieros en Informática del Principado de Asturias.

Por otro lado, el "Premio Stakeholders.News 2024" fue otorgado a la Agencia para la Administración Digital de la Comunidad de Madrid, por haberse convertido en referente en la innovación y digitalización de la administración pública y por su compromiso con el cumplimiento y la excelencia del servicio al ciudadano. Este premio fue recogido por Zaida Sampedro Préstamo, subdirectora general de Transformación y Gestión del Cambio de la Agencia para la Administración Digital de la Comunidad de Madrid.

Al terminar el acto, todos los presentes pudieron disfrutar de un magnífico networking alrededor de un espectacular catering que se sirvió en las mismas instalaciones de UNE, con lo que se dio por cerrada la temporada de ambas revistas. ¡Nos vemos en septiembre!

Hace mucho tiempo que hablas.

¿Pero hace cuánto no dialogas?

Somos una organización global de beneficio para la comunidad cuya misión es crear normas para contribuir a la construcción de un mundo más seguro, sostenible y competitivo.

Creamos espacios de colaboración neutrales e inspiradores en los que compartir conocimiento para desarrollar, a través del diálogo y el consenso, normas que sirvan a los intereses de toda la sociedad y que movilicen a los que apuestan decididamente por la excelencia empresarial y la conciencia social.

UNE Normalización Española

Progreso compartido

une.org

Cumpliendo con la inteligencia en amenazas

Introducción

En esta sección de Hack&News ya hemos hablado en varias ocasiones de la inteligencia en amenazas, y de la importancia de implementarla en la organización para ayudar a que el proceso de gestión de riesgos, concretamente la evaluación, sea más eficaz, a través del conocimiento profundo de las amenazas, con información de valor, que permitan a las organizaciones tomar las mejores decisiones para el tratamiento de los riesgos derivados de estas amenazas.

Pocos marcos de controles de seguridad hacían referencia de manera específica a la inteligencia en amenazas, al hecho de disponer de un programa de inteligencia en amenazas. Salvo NIST (*National Institute of Standards and Technology*), que sí hace referencia a un control como es *PM-16: Threat Awareness Program*, el resto de los marcos de controles no hacían una referencia específica, y algunos siguen sin hacerlo.

Inteligencia en amenazas en la nueva versión ISO/IEC 27001:2022

Antes de focalizarnos en el control específico, recordemos que tenemos nueva versión de esta Norma ISO, y con significantes cambios respecto a su versión anterior (2013). En la versión 2013 podíamos contabilizar hasta 114 controles, que se dividían en dominios (14) y objetivos de control (35). En esta nueva versión, se han fusionado más de 50 controles y se han añadido 11 nuevos controles. La versión 2022 agrupa los controles en; controles de personas, controles físicos, controles tecnológicos y controles organizacionales.

Lo que no ha cambiado es el enfoque del sistema de gestión de seguridad de la información, basada en el riesgo; en su evaluación y en su tratamiento. En este sentido, cobra especial importancia uno de los nuevos controles incluidos en esta versión 2022 y que precisamente hace referencia a la inteligencia en amenazas.

En la nueva versión del Anexo A de las ISO/IEC 27001:2022 podemos encontrar el control **A 5.7 – Inteligencia en amenazas**, y que precisamente viene cubrir este aspecto que tanto hemos mencionado en esta sección de Hack&News.

Este control precisamente focaliza en que las organizaciones deben disponer de información de valor, inteligencia, sobre amenazas que pueden poner en peligro sus sistemas de información. Para ello, de manera periódica, deberán consultar frameworks como MITRE ATT&CK o informes de fabricantes y organizaciones gubernamentales que hayan investigado los comportamientos de los **Grupos APT** (*Advanced Persistent Threats*), es decir,

CONTINÚA EN PRÓXIMA PÁGINA

nuestros posibles adversarios. Esto nos permitirá saber qué motivaciones tienen, cómo piensan y cómo actúan, conociendo cuáles son sus **tácticas, técnicas y procedimientos (TTP)**, permitiéndonos identificar cuáles son las medidas de seguridad que pueden responder de una manera más eficaz y eficiente ante estas técnicas empleadas por este tipo de adversarios.

La organización, en base a su tecnología y vulnerabilidades, tendrá que determinar la probabilidad de que este tipo de amenazas puedan materializarse e impactar en la organización, e implantar las medidas de seguridad oportunas para mitigar o reducir el riesgo de dichas amenazas.

Como prácticamente todo en ciberseguridad, esto se debe realizar a través de un proceso, que permita de manera sistemática la planificación, ejecución, monitorización y mejora de las tareas necesarias para cubrir esta necesidad, y ya de paso, cumplir con este control de la nueva versión 2022 de la ISO/IEC 27001.

Y ojo, ya no es por el cumplimiento de la norma, es por la propia seguridad y continuidad de negocio de las organizaciones. El cumplimiento de un control o la certificación de una Norma ISO tiene que ser la consecuencia de las buenas prácticas implantadas en una organización, en este caso en el contexto de la seguridad de la información o la continuidad de negocio.

Hay que destacar que este nuevo control no se ha categorizado como un control tecnológico, sino como un control organizacional. Y tiene todo el sentido del mundo, ya que la inteligencia en amenazas se debe de abordar desde los tres niveles funcionales de una organización; el nivel estratégico para tomar decisiones de alto nivel en base a la información recibida, el nivel táctico para gestionar el programa de inteligencia en amenazas y reportar al nivel estratégico y el nivel operativo para la ejecución de las operaciones necesarias y planificadas previamente por el nivel táctico.

Personalmente, creo que es un gran acierto la inclusión de este control, ya que servirá para concienciar a las organizaciones de la necesidad de disponer de un programa de inteligencia de amenazas y que les ayudará a protegerse mejor ante sus posibles adversarios.

Como siempre, espero que el artículo sea de vuestro agrado, interés y os pueda resultar útil.

¡Nos leemos!

Escuela de Gobierno

eGob®

https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Service Management FitSM + ISO 20000

Director Académico:

Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación FitSM Executive
- Certificación ISO 20000 Leader
- Módulo 5 MasterGEIT®
- Módulo 5 MasterPPM®

MPPM® MGEIT® eGob®

Del 17 al 25 de mayo

+ 34 96 109 44 44
campus@escueladegobierno.es

La tecnología frente a las personas y procesos

Ya en otros artículos de esta sección hemos hablado sobre la importancia de considerar el tridente personas, procesos y tecnología a la hora de gestionar la seguridad de la información en nuestras organizaciones. No se trata solo una cuestión de seguridad, la gestión adecuada, y coordinada, de estos tres elementos favorecerá la eficacia y eficiencia de los servicios prestados por la organización, ya sea a clientes o de manera interna.

Centrándonos en la seguridad de la información, la tecnología está ahí, para bien o para mal. Afortunadamente son muchos más los beneficios que nos aporta la tecnología, no solo en el ámbito de las organizaciones, también a la propia sociedad. Pero, como bien sabéis, el uso de estas tecnologías también conlleva de manera intrínseca unos riesgos. A esto hay que unirle que el número de amenazas existentes es cada vez mayor y más difíciles de detectar.

Por si no fuera suficiente con el ingenio y recursos con los que cuentan los ciberdelincuentes para desarrollar amenazas cada vez más peligrosas, la penetración de la Inteligencia Artificial (IA) en nuestras vidas ha permitido a estos ciberdelincuentes desarrollar otras técnicas de ataque.

CONTINÚA EN PRÓXIMA PÁGINA

Uno de los ejemplos más recientes y del que se están conociendo ya casos reales que están afectando a algunas organizaciones, es la utilización de la técnica Deep Fake para la suplantación de identidades. Esta técnica de IA utiliza algoritmos de aprendizaje para la creación de diferentes recursos multimedia como pueden ser imágenes, vídeos o audios falsos, muy realistas y que dificultan distinguirlos de recursos reales.

Los ciberdelincuentes están empezando a usar esta técnica para engañar a sus víctimas a través de la ingeniería social, suplantando la identidad de personas de la organización, especialmente personas con cargos importantes, como pueden ser directores generales o directores financieros. Ya se han dado casos en la que los atacantes han conseguido engañar a sus víctimas a través de un vídeo falso en el que el supuesto director financiero de la organización solicitaba la realización de una transferencia.

Es un ejemplo más de que los adversarios van un paso por delante, porque mientras ellos desarrollan o utilizan este tipo de técnicas para atacar a las organizaciones, la tecnología que debería de identificar y defendernos de estas técnicas o no existen o no están aún suficientemente maduras para ser totalmente eficaces ante estos ataques.

Y aquí es donde cobra mayor relevancia el hecho de que a nivel de seguridad de la información, a nivel de cómo proteger nuestros sistemas de información, las personas, los procesos y la tecnología deben ir de la mano. *¿No existe aún una tecnología capaz de identificar Deep Fakes durante una videollamada*? Quizás la solución la tengamos más cerca de lo que nos pensamos; personas y procesos.

No todas las soluciones a nuestros problemas de ciberseguridad son de índole tecnológico, la capacitación y formación de las personas es crucial para una protección efectiva y eficiente. Si además contamos con procesos y procedimientos que nos sirven como medida organizativa para reducir o mitigar riesgos, mucho mejor. En el caso de las técnicas con *Deep Fake*, la organización podría implantar un procedimiento mediante el cual, a partir de un importe concreto, las transferencias no puedan ser ordenadas sin el consentimiento de dos o más personas. O si las peticiones se hacen a través de algún medio como videollamada o por teléfono, a la persona que ordena la transferencia se le solicitará un factor de autenticación, como puede ser un código enviado a su móvil. Este ejemplo concreto dificultaría que el fraude se consumara ya que los ciberdelincuentes deberían tener acceso también al móvil del ordenante.

Esto es solo un simple ejemplo de que no todo se soluciona con tecnología, y que la instauración y aplicación de las buenas prácticas en seguridad de la información, por parte de las personas y los procesos, también ayudará a las organizaciones a reducir la probabilidad de ser víctimas de este tipo de ataques.

Políticas de mínimo privilegio, segregación de responsabilidades y controles de accesos son solo algunos ejemplos de medidas de seguridad que son realmente efectivas. Y no son nuevas. Son principios y políticas que ya aparecían en modelos de seguridad hace más de 40 años, como son los modelos de *Bell-Lapadula, Biba o Brewer-Nash*, y en los cuales se basa mucha tecnología de la industria de la ciberseguridad que hoy conocemos.

Como siempre, espero que el artículo sea de vuestro agrado, interés y os pueda resultar útil.

¡Nos leemos!

Escuela de Gobierno

eGob®

https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Seguridad de la Información

CSX + ISO 27001

Director Académico:

Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación CSX Executive
- Certificación ISO 27001 Leader
- Módulo 6: MasterGEIT®

MGEIT® eGob®

Del 7 al 15 de junio

+ 34 96 109 44 44
campus@escueladegobierno.es

Seguridad en aplicaciones móviles con OWASP MAS

En nuestra revista ya se ha hablado alguna vez de OWASP (Open Web Application Security Project), un proyecto sin ánimo de lucro que tiene como objetivo ofrecer a la comunidad una serie de recursos para ayudar a las organizaciones a que sus aplicaciones sean más seguras, para ello ofrece diferentes recursos tanto para desarrolladores como para auditores de seguridad.

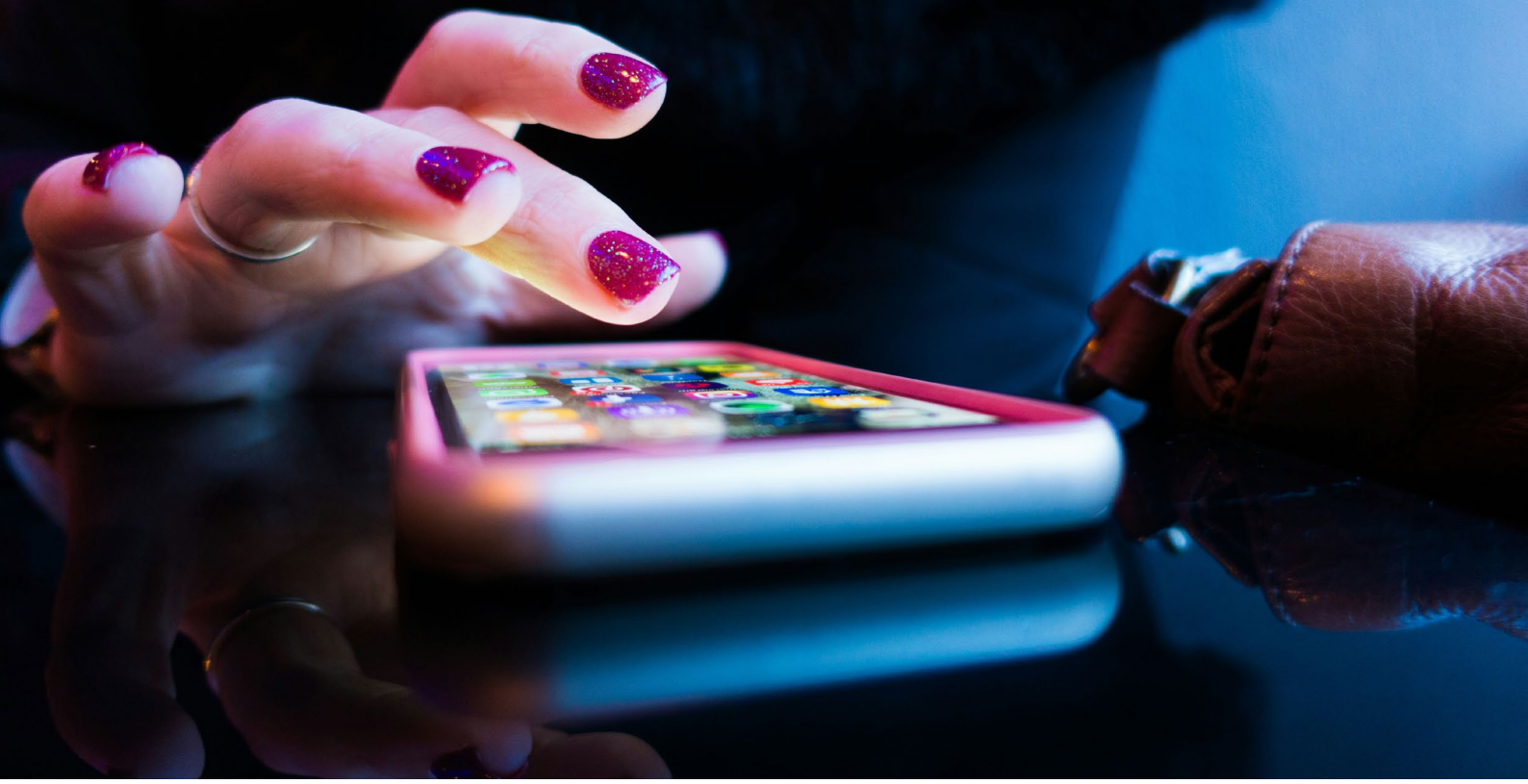
Los desarrolladores pueden utilizar OWASP para aplicar un **Ciclo de Vida del Desarrollo de Software Seguro** *(S-SDLC, Security Software Development Life Cycle)*, que es un enfoque que permite aplicar controles de seguridad en las distintas etapas del ciclo de desarrollo, evitando que el software se ponga en producción con vulnerabilidades, lo que significaría un importante riesgo para la organización, adoptando una postura de seguridad más proactiva en lugar de una postura reactiva.

Desde su inicio OWASP estaba focalizado sobre todo en la seguridad de aplicaciones web, sin embargo, en los últimos años han ido apareciendo diferentes proyectos dentro de OWASP para abarcar la seguridad en otros contextos, como puede ser el **IoT** *(Internet of Things* o Internet de las Cosas*)* o las aplicaciones móviles, que es precisamente el objeto de este artículo.

Hoy en día llevar un teléfono móvil en el bolsillo implica llevar un *miniordenador* en el bolsillo, con su software, como es el propio sistema operativo del dispositivo o las diferentes aplicaciones instaladas en el mismo. El software (y el hardware) está expuesto a vulnerabilidades, a fallos y deficiencias del desarrollo que pueden ser explotadas por agentes maliciosos y comprometer la información almacenada, procesada o transmitida desde el dispositivo móvil.

CONTINÚA EN PRÓXIMA PÁGINA


0.01K/s
23:18
23:18
96%
NOV 9
Facebook
Chrome
YouTube
VSCO
Gmail
Music
Maps
Gallery
Mi Home



La utilización de los dispositivos móviles, ya sean personales o corporativos, en los ámbitos profesionales es cada vez mayor. Esta situación requiere prestar una atención especial a este tipo de dispositivos y sus aplicaciones. Por ello, en las organizaciones tenemos que garantizar el uso seguro de estos dispositivos por parte de los usuarios, pero también que las aplicaciones utilizadas sean seguras. Y aquí es donde un proyecto como **OWASP MAS** (*Mobile Application Security*) puede ayudar a garantizar la seguridad en las aplicaciones.

El proyecto MAS, siguiendo la filosofía OWASP, ofrece un conjunto de recursos para ayudar a los desarrolladores de aplicaciones móviles a producir aplicaciones, ya sean Android o iOS, más seguras. Entre los diferentes recursos ofrecidos por MAS, destacaría tres; **OWASP MASVS, OWASP MASTG y OWASP MAS Checklist**.

OWASP MASVS (*Mobile Application Security Verification Standard*) se puede considerar como un estándar para la seguridad en aplicaciones móviles. Dirigido sobre todo a desarrolladores que quieran aplicar seguridad desde el diseño y en las diferentes etapas del desarrollo de la aplicación. La web de OWASP MAS ofrece una página específica de este recurso donde podemos encontrar un pequeño repositorio de los distintos grupos de controles de seguridad a tener en cuenta en el proceso de desarrollo. También tenemos la opción de descargarnos la guía en PDF.

OWASP MASTG (Mobile Application Security Testing Guide) es una guía más orientada para la evaluación de la seguridad de las aplicaciones móviles y es ideal para llevar a cabo una auditoría de seguridad técnica de una aplicación móvil, ya sea Android o iOS. Describe los procesos que hay que ejecutar para verificar la existencia de los controles definidos en el MASVS, y en caso de existencia, evaluar su madurez. La guía en PDF está disponible en la web de OWASP MAS.

Finalmente, **OWASP MAS Checklist** es una lista de verificación en Excel que nos puede servir como herramienta de soporte a la hora de auditar las aplicaciones móviles. Contempla los diferentes grupos de controles de seguridad incluidos en el MASVS y puede resultar útil para garantizar la completitud y alcance de los controles, así como para guardar los resultados de las auditorías y poder compararlos en el tiempo, para ir evaluando el progreso en la seguridad de las aplicaciones auditadas.

Estos tres recursos de OWASP nos pueden ayudar a crear nuestra propia metodología de auditoría de aplicaciones móviles, ya que tenemos por un lado el conjunto de controles a auditar (MASVS), una guía que explica los procesos a ejecutar (MASTG) y una lista de verificación para garantizar que son cubiertos todos los controles y guardar resultados para su comparación. Obtener resultados comparables y repetibles, es uno de los principios más importantes a la hora de usar una metodología para llevar a cabo una auditoría de seguridad.

Como siempre, espero que el artículo sea de vuestro agrado, interés y os pueda resultar útil.

¡Nos leemos!

Escuela de Gobierno
eGob®
https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Continuidad de Negocio

BCI + ISO 22301

Director Académico:
Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación BCI Executive
- Certificación ISO 22301 Leader
- Módulo 7: MasterGEIT®

MGEIT® eGob®

Del 5 al 13 de julio

+ 34 96 109 44 44
campus@escueladegobierno.es


750
1000
990
PLUIE
REGEN

Evaluando la eficacia de nuestro SGSI

En anteriores artículos ya hemos visto la importancia de hacer un **seguimiento** y llevar un control del SGSI (Sistema de Gestión de Seguridad de la Información) para verificar que estamos alcanzando los objetivos de seguridad marcados.

Como en otros ámbitos de la vida, no todo es sí o no, blanco o negro, aprobado o suspenso... Desde el negro hasta el blanco tenemos diferentes tonalidades de grises, y este símil nos puede ayudar a entender que, aunque se alcance una meta, hay muchas formas de hacerlo, los que nos lleva también posiblemente a diferentes niveles de eficiencia a la hora de lograr dicha meta.

Nuestro SGSI ha de ser **evaluado periódicamente**, y no me refiero solo a las auditorías internas o externas de nuestro sistema, me refiero al rendimiento. Podríamos decir que el rendimiento es la proporción que surge entre los medios empleados para obtener algo y el resultado que se consigue. En el mundo de la gestión de la seguridad siempre está la duda en cuánto tiempo, recursos y esfuerzo tenemos que dedicarle a nuestro SGSI para garantizar la protección de nuestros sistemas, que detectamos y respondemos bien ante amenazas y finalmente, en caso de incidente de seguridad, tengamos la capacidad de recuperarnos en el menor tiempo posible.

En este artículo nos vamos a centrar en la **eficacia del sistema**, en cómo podríamos medir y evaluar la eficacia de los procesos de seguridad y controles implantados. A estas alturas, espero que todos tengamos claro que el primer paso es medir; recordad que *no podemos mejorar lo que no medimos*. Una vez obtenidos los datos de las mediciones tendremos que evaluar esa información para verificar que estamos cumpliendo los objetivos, y en caso contrario, identificar el motivo del desvío o no consecución y definir un plan de acciones correctivas para corregir la situación.

Disponer de un **programa de medición** nos puede facilitar esta tarea, ya que nos ayuda a dar respuesta a preguntas que nos pueden surgir, tales como:

- *¿Qué tenemos medir?*
- *¿Cómo lo vamos a medir?*
- *¿Quién lo va a medir?*
- *¿Con qué periodicidad se va a medir?*

CONTINÚA EN PRÓXIMA PÁGINA

Antes de comenzar a diseñar nuestro programa de medición, sería bueno aplicar aquello de *"divide y vencerás"*. No podemos pretender empezar con un programa que abarque todos los procesos y controles de seguridad. Pensad que los sistemas de gestión, no solo el de seguridad de la información, tienen unos **niveles de madurez** y, por lo tanto, lo lógico y más eficaz sería empezar por un número determinado de procesos y controles, no importa que sea un número pequeño. Lo importante es diseñar un programa de medición, que será escalable y permitirá la inclusión de nuevos procesos y controles a medir, conforme el sistema de gestión vaya adquiriendo madurez.

Consultad vuestro listado de procesos de seguridad; **gestión de activos, gestión de riesgos, gestión de vulnerabilidades, formación y concienciación, seguridad operativa, control de accesos, gestión de identidades**, etc. Haced una selección de dos o tres procesos (se recomienda empezar por uno de los procesos que tenga menos complejidad) y comenzad a diseñar vuestro programa de medición. Vuestro programa puede empezar siendo una simple tabla de Excel, eso sí, aseguraros que incorpore campos para guardar datos que dan respuesta a las preguntas que hemos planteado anteriormente.

Por ejemplo, la tabla inicial de nuestro programa de medición podría incorporar los siguientes campos:

•**Proceso / Control:** Hace referencia al proceso o control al que pertenece la medición.

•**Responsable:** Persona o equipo responsable de la ejecución de la medición (se podría ampliar con una tabla RACI de responsabilidades)

•**Recursos:** Qué recursos serán necesarios para llevar a cabo la medición

•**Indicador:** Dato o conjunto de datos observados para la medición.

•**Método de cálculo:** Indica cómo se calcula el valor del indicador (se recomienda utilizar fórmulas que den un valor porcentual).

•**Valor Objetivo:** Valor que nos sirve como referencia, como umbral, para saber si nuestro valor obtenido (indicador).

•**Periodicidad:** Con qué frecuencia o periodicidad se llevarán a cabo las mediciones.

•**Observaciones:** Campo para añadir observaciones si fuera necesario.

Una vez diseñada la tabla de nuestro programa de medición, incluimos los datos necesarios de los dos o tres procesos / controles que hayamos seleccionado. El proceso de formación y concienciación puede ser un buen ejemplo por el que empezar. Por ejemplo, se podría medir el porcentaje de usuarios que están recibiendo formación en materia de ciberseguridad. En este caso, el **método de cálculo** podría ser: número de usuarios que reciben formación / número de usuarios totales.

En este artículo se ha presentado un ejemplo muy básico de un programa de medición que nos ayudara con la **mejora continua de nuestro SGSI**, pero puede servir como base para ir mejorando el programa e ir escalándolo a un mayor número de procesos, y más complejos.

Como siempre, espero que el artículo sea de vuestro agrado, interés y os pueda resultar útil.

¡Nos leemos!

Escuela de Gobierno

eGob®

https://escueladegobierno.es

Curso de
Doble Certificación

Gobierno de I&T

COBIT + ISO 38500

Director Académico:

Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación COBIT Executive
- Certificación ISO 38500 Leader
- Módulo 8: MasterGEIT®

MGEIT® eGob®

Del 6 al 14 de septiembre

+ 34 96 109 44 44
campus@escueladegobierno.es

Necesitamos un SIEM, ¿por dónde empezamos?

En esta sección ya hemos nombrado en varias ocasiones cómo está aumentando considerablemente el número de amenazas emergentes y la complejidad que supone identificarlas, protegerse ante ellas y detectarlas. Afortunadamente, las organizaciones disponen también de un amplio catálogo que ofrecen los fabricantes de productos de seguridad para seleccionar e implantar medidas de seguridad que les ayuden en estas labores.

Soluciones como cortafuegos y antivirus (con sus diferentes evoluciones tipo EDR o XDR) forman parte de la infraestructura tecnológica de cualquier organización, o al menos, así debería ser, independientemente del tamaño o naturaleza de ésta. Sin embargo, la situación actual obliga a que las organizaciones tengan una mayor visibilidad de lo que está ocurriendo en su organización, no solo en la red corporativa, sino también en su perímetro, en su infraestructura de la nube o con sus usuarios y sedes remotas.

Los componentes de los sistemas de información generan una gran cantidad de registros de actividad (logs) y eventos de seguridad. Dependiendo del tipo de componente, esta cantidad puede ser mayor o menor y la calidad de la información también puede variar. Desde las impresoras, hasta los servidores o cortafuegos, pasando por los equipos de sobremesa, portátiles o electrónica de red, como switches, puntos de acceso y routers, generan registros de actividad y eventos de seguridad.

Es importante diferenciar entre registros de actividad o logs y eventos de seguridad. Los registros hacen referencia a cualquier tipo de actividad en un sistema, mientras que los eventos de seguridad, tal y como su nombre indica, se centran exclusivamente en eventos que tengan que ver con algún aspecto de la seguridad. Podríamos decir que los eventos de seguridad son un subconjunto de los registros de actividad (logs).

CONTINÚA EN PRÓXIMA PÁGINA

Desde el punto de vista de la seguridad de la información, es importante que la organización tenga visibilidad de la actividad de los sistemas de información, sobre todo de aquella actividad sospechosa o maliciosa, intentando evitar los puntos ciegos en la infraestructura que les impida ver y controlar actividades de agentes maliciosos con la antelación suficiente para responder de una manera eficaz y mitigar o reducir el riesgo de impacto negativo en la seguridad de la información.

Herramientas como los SIEM (*Security Information and Event Management*) ayudan a las organizaciones a tener una visibilidad de la actividad de los sistemas, pero no solo eso, sino que además aportan la capacidad de detectar actividad sospechosa o maliciosa en las fuentes monitorizadas. Una de las claves para que este proceso de monitorización de eventos de seguridad sea eficaz es la correcta selección de las fuentes a monitorizar con el SIEM.

En este punto es posible que a algún lector se le ocurra la respuesta *"Pues todas las fuentes, Miguel Ángel"*, y no iría mal encaminado, pero hay que tener en cuenta que los presupuestos de ciberseguridad no son ilimitados, y el coste de este tipo de soluciones dependen de la cantidad de información que reciban y tengan que procesas, es decir, del número de eventos que tienen que tratar, concretamente eventos por segundo (EPS). Cuantos más EPS mayor será el coste, no solo tecnológico en cuanto a los recursos (CPU, memoria, almacenamiento, etc.) que necesite el SIEM, sino también en cuanto al coste de operación, porque se necesitarán más personas para atender los eventos de seguridad y las posibles alertas que se puedan generar.

Esta cuestión supone en muchos casos un rechazo por parte de las organizaciones a la hora de implantar un SIEM en su organización y optan por continuar con sus consolas de cortafuegos y antivirus, que hoy en día son insuficientes, porque quedan puntos ciegos sin cubrir.

La buena noticia es que no se trata del todo o nada, ya que este tipo de soluciones suelen ser bastante flexibles y escalables, en el sentido de que se puede comenzar con unas pocas fuentes iniciales (las más críticas), e ir incorporando nuevas fuentes según el presupuesto lo permita y la circunstancia lo requiera. Por ejemplo, para comenzar, una organización podría empezar monitorizando las fuentes de seguridad de su cortafuegos, consola antimalware, controladores de dominio, sistema de backup y su Microsoft 365 o Google Workspace, si lo tuviera.

Una vez implantado el proceso de monitorización de eventos de seguridad con un SIEM, paulatinamente se pueden ir añadiendo nuevas fuentes, actualizar los casos de uso y establecer indicadores que permitan medir el proceso y mejorarlo.

Como siempre, espero que el artículo sea de vuestro agrado, interés y os pueda resultar útil.

¡Nos leemos!

Escuela de Gobierno
eGob®
https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Gobierno Corporativo COSO + ISO 37000

Director Académico:
Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación COSO Executive
- Certificación ISO 37000 Executive
- Módulo 10: MasterGEIT®
- Módulo 1:0 MasterPPM®

MPPM® MGEIT® eGob®

Del 22 al 30 de noviembre

+ 34 96 109 44 44
campus@escueladegobierno.es

Analizando los comportamientos de nuestros adversarios

En artículos anteriores de esta sección ya hemos mencionado la importancia de contar con un programa de inteligencia en amenazas dentro de la organización ya que es la única forma de poder hacer una evaluación eficaz del riesgo e implantar medidas de seguridad que reduzcan la probabilidad de que una amenaza se materialice o que, en caso de materializarse, reducir su posible impacto. El objetivo siempre es el mismo; reducir el riesgo.

A través de artículos o informes de fabricantes especialistas en inteligencia en amenazas podemos aprender a identificar los comportamientos de los adversarios, analizarlos y extraer conclusiones interesantes en relación a las tácticas, técnicas y procedimientos (TTP) utilizados por estos adversarios, una información que resultará muy útil a la hora de elaborar un programa de seguridad o plan de tratamiento para dar respuesta a las técnicas ofensivas usadas, ya que incluirán técnicas defensivas más eficaces en base a la información de valor (inteligencia) obtenida durante el proceso.

CONTINÚA EN PRÓXIMA PÁGINA

El enfoque aquí propuesto es basándonos en los comportamientos, que serán las tácticas utilizadas por los adversarios. MITRE ATT&CK, del cual ya hemos hablado en esta sección, cuenta con diferentes matrices para agrupar las tácticas y técnicas ofensivas utilizadas.

Tomaremos como ejemplo la matriz ENTERPRISE, y las 12 tácticas que van desde el "*Acceso inicial*" (INITIAL ACCESS) hasta el "*Impacto*" (IMPACT).

La idea es que, a través de la información facilitada por los analistas en los diferentes artículos e informes que comparten podamos ir identificando las diferentes fases que han ido ejecutando durante su ataque, intentando plasmarlas en un orden cronológico y alineándolo con el famoso CYBER KILL CHAIN (*ciber cadena de la muerte*).

Veamos un pequeño ejemplo para entender el enfoque y cómo extraer la información de valor que nos permita identificar tácticas y técnicas. Centrémonos en el siguiente extracto de un informe:

The vector of the infection, similarly to other APT28 / FancyBear attack, is a spear phishing email delivering a Word Office document with a significant name, often related to International Conferences or other events involving several countries. As expected, the document triggers a MACRO function able to extract a Microsoft Dynamic Link Library (DLL) which acts as downloader of a SkinnyBoy dropper (tdp1.exe) from a first dropurl.

En el extracto anterior se puede observar el nombre del grupo APT que estamos analizando, en este caso el APT28 o FancyBear. Como se puede ver, el acceso inicial se produce a través del envío de un *phishing* dirigido (*spear phishing*) con un documento adjunto. En las dos primeras frases del párrafo se puede extraer que para la táctica de INITIAL ACCESS, el grupo APT28 utilizaba *spear phishing*.

El phishing está etiquetado como la técnica T1566 (dentro de MITRE ATT&CK) y el *spear phishing* concretamente es una subtécnica, que dependiendo de si el correo incluye un adjunto o un enlace, se identifica de una manera diferente. En este caso, se trata de un *spear phishing* con adjunto, por lo tanto, estaríamos hablando de la subtécnica T1566.001.

El fichero adjunto incluye una macro capaz de extraer una librería DLL que actúa como herramienta para la descarga de otros ficheros maliciosos necesarios para continuar el ataque.

Esto es solo un pequeño ejemplo como, a partir de informes compartidos por fabricantes y analistas independientes, podemos extraer información muy valiosa que, tras ser debidamente procesada, nos puede ayudar a tomar las mejores decisiones a la hora de implantar medidas eficaces de seguridad.

En este sentido, el propio MITRE ATT&CK nos propone, por cada técnica, diferentes mecanismos para la detección de la técnica y su mitigación. Información que puede ser completada si además de MITRE ATT&CK utilizamos MITRE D3FEND para identificar técnicas ofensivas para contrarrestar las técnicas ofensivas identificadas.

En el ejemplo que acabamos de ver, y para la subtécnica de *spear phishing* con adjunto, algunas medidas de seguridad recomendadas puede ser la capacitación y concienciación de usuarios para identificar correos maliciosos, bloquear correos entrantes con adjuntos que puedan contener macros, aplicar el principio de mínimo privilegio para los usuarios o la segmentación de las redes para minimizar el impacto en caso de que se llegue a ejecutar el código malicioso.

Como siempre, espero que el artículo sea de vuestro agrado, interés y os pueda resultar útil.

¡Nos leemos!

Escuela de Gobierno

eGob®

https://escueladegobierno.es

Curso de Doble Certificación en:

Gestión de Beneficios y Gestión de Portafolios

P4MGO!® BfM Leader
P4MGO!® PfM Leader

Dirección Académica:
Javier Peris

- Dos formatos para tu comodidad
- Opción A: Remoto en Directo
- Opción B: Virtual con Tutoría
- Metodología P4MGO!®
- Exámenes de Certificación Incluidos
- Certificación P4MGO!® BfM Leader
- Certificación P4MGO!® PfM Leader
- Solicita tu admisión

MPPM® MGEIT® eGob®

Próxima Convocatoria en Directo
Octubre 2024

Solicita tu admisión en:

+ 34 96 109 44 44
admisiones@escueladegobierno.es

P4MGO!

NUEVOS MASTERS

Escuela de Gobierno eGob®
admisiones@escueladegobierno.es
https://escueladegobierno.es