Apuntes SinCara

Modulo 01

- El CIO (Director de Información), es el gerente de sistemas o director de tecnologías de la información (responsable de TI). Reporta directamente al CEO, y se encarga directamente de las estrategias de la organización que están alineadas con la tecnología de la información para lograr los objetivos planificados.
    - El CSO (Chief Security Officer) es el responsable de la seguridad de la organización. Al CSO a veces se le denomina responsable de seguridad corporativa.
    - El CISO (Director de Seguridad de la Información) es el director de seguridad de la información. Básicamente es un rol desempeñado a nivel ejecutivo y su función principal es la alineación de la seguridad de la información con los objetivos del negocio. De esta forma se garantiza en todo momento que la información de la empresa está protegida con seguridad.
    - https://www.incibe.es/protege-tu-empresa/blog/ceo-ciso-cio-roles-ciberseguridad
    - https://rafeeqrehman.com/2024/03/31/ciso-mindmap-2024-what-do-infosec-professionals-really-do/ - CISO Mindmap 2024. ¿Qué hacen realmente los profesionales InfoSec?
        - https://rafeeqrehman.com/wp-content/uploads/2024/03/CISO_MindMap_2024-2.png - El Mindmap a máxima resolución
- https://www.hornetsecurity.com/es/knowledge-base/cyber-kill-chain/ - Cyber Kill Chain
- TTP: Las técnicas son las herramientas utilizadas, la táctica es la forma de combinar esas herramientas para hacer un determinado trabajo y el procedimiento es la guía a seguir para hacer el trabajo.
- IoC:
    - Es la descripción de un incidente de ciberseguridad, actividad y/o artefacto malicioso mediante patrones para ser identificado en una red o endpoint pudiendo mejorar así las capacidades ante la gestión de incidentes.
    - https://es.wikipedia.org/wiki/Indicador_de_compromiso - IoCs
- Attacks = Motive (Goal) + Method (TTP) + Vulnerability
- https://ichi.pro/es/modelo-de-diamante-de-analisis-de-intrusion-233418583446217 - Modelo Diamante de análisis de intrusión
- https://blog.segu-info.com.ar/2023/11/el-modelo-diamante-vs-mitre-att.html - El modelo diamante vs MITRE ATT&CK
- Information Assurance (IA):
    - Es la práctica de asegurar la información y gestionar los riesgos relacionados con el uso, el procesamiento, el almacenamiento y la transmisión de la información.
    - La garantía de la información incluye la protección de la integridad, la disponibilidad, la autenticidad, el no repudio y la confidencialidad de los datos de los usuarios.
    - La IA abarca no sólo las protecciones digitales sino también las técnicas físicas. Estas protecciones se aplican a los datos en tránsito, tanto en forma física como electrónica, así como a los datos en reposo.
- Cyber Threat Intelligence (CTI):
    - Cyber Threat Intelligence es el arte de convertir los datos en inteligencia sobre amenazas informáticas para prevenir ataques
    - https://www.welivesecurity.com/la-es/2021/11/08/que-es-cyber-threat-intelligence/
- Threat Modeling (Modelado de Amenazas):
    - La elaboración de modelos de amenazas es un proceso mediante el cual se pueden identificar y enumerar las posibles amenazas, como las vulnerabilidades estructurales o la ausencia de protecciones apropiadas, y se puede dar prioridad a su mitigación.
    - El propósito de la modelización de amenazas es proporcionar a los defensores un análisis sistemático de los controles o defensas que deben incluirse, dada la naturaleza del sistema, el perfil del atacante probable, los vectores de ataque más probables y los bienes más deseados por un atacante.
    - https://www.flu-project.com/2014/06/el-modelado-de-amenazas-parte-i.html

    - https://www.flu-project.com/2014/06/el-modelado-de-amenazas-parte-ii.html
    - https://www.flu-project.com/2014/06/el-modelado-de-amenazas-parte-iii.html
    - https://blog.segu-info.com.ar/2023/01/desarrollo-seguro-mediante-el-modelado.html
- Legislación:
    - https://blog.segu-info.com.ar/2020/08/apis-con-certificacion-pci-dss-rgpd-y.html - PCI DSS
        - https://www.pcihispano.com/ - PCI DSS Hispano
        - https://blog.segu-info.com.ar/2022/04/pci-dss-v40-y-la-proteccion-de-scripts.html - PCI DSS v4.0
        - https://blog.segu-info.com.ar/2022/06/analisis-de-pci-dss-v40.html - Análisis de PCI DSS v4.0
        - https://www.incibe.es/protege-tu-empresa/blog/pagos-linea-mas-seguros-pci-dss-version-40 - v4.0
    - https://es.wikipedia.org/wiki/ISO/IEC_27000-series - La serie ISO/IEC 27000 de normas son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC).
    - https://www.uprm.edu/p/cpshi/ley_hippa - HIPAA
    - https://www.ineaf.es/tribuna/que-es-la-ley-sox-y-para-que-sirve/ - SOX
        - Aunque la Ley SOX es una normativa estadounidense, afecta a empresas españolas que operan en los mercados financieros de Estados Unidos, y también a proveedores de empresas reguladas por SOX.
        - https://es.wikipedia.org/wiki/Digital_Millennium_Copyright_Act - DMCA
    - FISMA:
        - La certificación FISMA es un requisito para muchos contratos con el gobierno de Estados Unidos, siendo un marco diseñado para proteger al gobierno de los Estados Unidos contra los ataques a la ciberseguridad y los desastres naturales que pongan en riesgo los datos confidenciales, las operaciones y los activos.
        - Obliga a implementar y soportar controles de seguridad de TI uniformes, definidos por el Instituto Nacional de Normas y Tecnología (NIST), permitiendo entre otras cosas, que los contratistas trasladen, de manera segura y confidencial, sus aplicaciones indispensables a la nube, ambientes de hospedaje administrados y que contraten a proveedores de SaaS que cumplan con las disposiciones de la ley FISMA.
- Normas ISO serie 27k:
    - http://iso27000.es/ - El portal de ISO 27001 en Español
    - http://iso27000.es/iso27000.html - Normas ISO 27k
    - https://normaiso27001.es/ - Otro portal que habla de las ISO 27k
    - https://t.me/iso27001hispano - Canal de Telegram con las ISO 27k
    - https://www.enac.es/ - ENAC certifica en España. Entidad Nacional de Acreditación en España.
- https://blog.segu-info.com.ar/2019/11/penetration-testing-vs-red-teaming-cual.html - Pentesting vs Red Teaming
- https://hackernoon.com/introducing-the-infosec-colour-wheel-blending-developers-with-red-and-blue-security-teams-6437c1a07700 - Los colores de la ciberseguridad: Blue, Red, Purple, Orange...
- https://eu.desmoinesregister.com/story/news/crime-and-courts/2019/09/11/men-arrested-burglary-dallas-county-iowa-courthouse-hired-judicial-branch-test-security-ia-crime/2292295001/ - El Incidente de Iowa
- https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/ - Historial de hackeos
    - https://blog.elhacker.net/2022/07/la-cadena-de-hoteles-marriott-es-hackeada-por-sexta-vez.html - La cadena de hoteles Marriott es hackeada por sexta vez
- https://www.bbc.com/mundo/noticias-internacional-53102950 - Ciberguerra entre estados
    - https://blog.segu-info.com.ar/2020/09/atacantes-norcoreanos-roban-millones-en.html - Atacantes norcoreanos roban millones en criptomonedas
- https://www.eluniversal.com.mx/techbit/diputados-aprueban-ley-iras-la-carcel-si-reparas-o-modificas-tus-dispositivos-electronicos - Ley mexicana que impide que puedas manipular tus propios dispositivos.
- https://www.youtube.com/results?search_query=atm+robbery - Robo de cajero
    - https://www.elmundo.es/espana/2022/12/28/63ac5f33fc6c8309128b4591.html - Y en Badajoz, con el mismo método
- IKEA hacking

- https://wiki.eth0.nl/index.php/LackRack - mesita rack
- https://www.impresoras3d.com/mesa-basica-de-ikea-para-crear-camara-cerrada-de-impresora-3d/
- https://ikeahackers.net/