Vulnerabilidades

by Miguel Solinas

Departamento de Computación

Julio XX22

Ministerio de Desarrollo Productivo Argentina

UTD Unidades de Transformación Digital

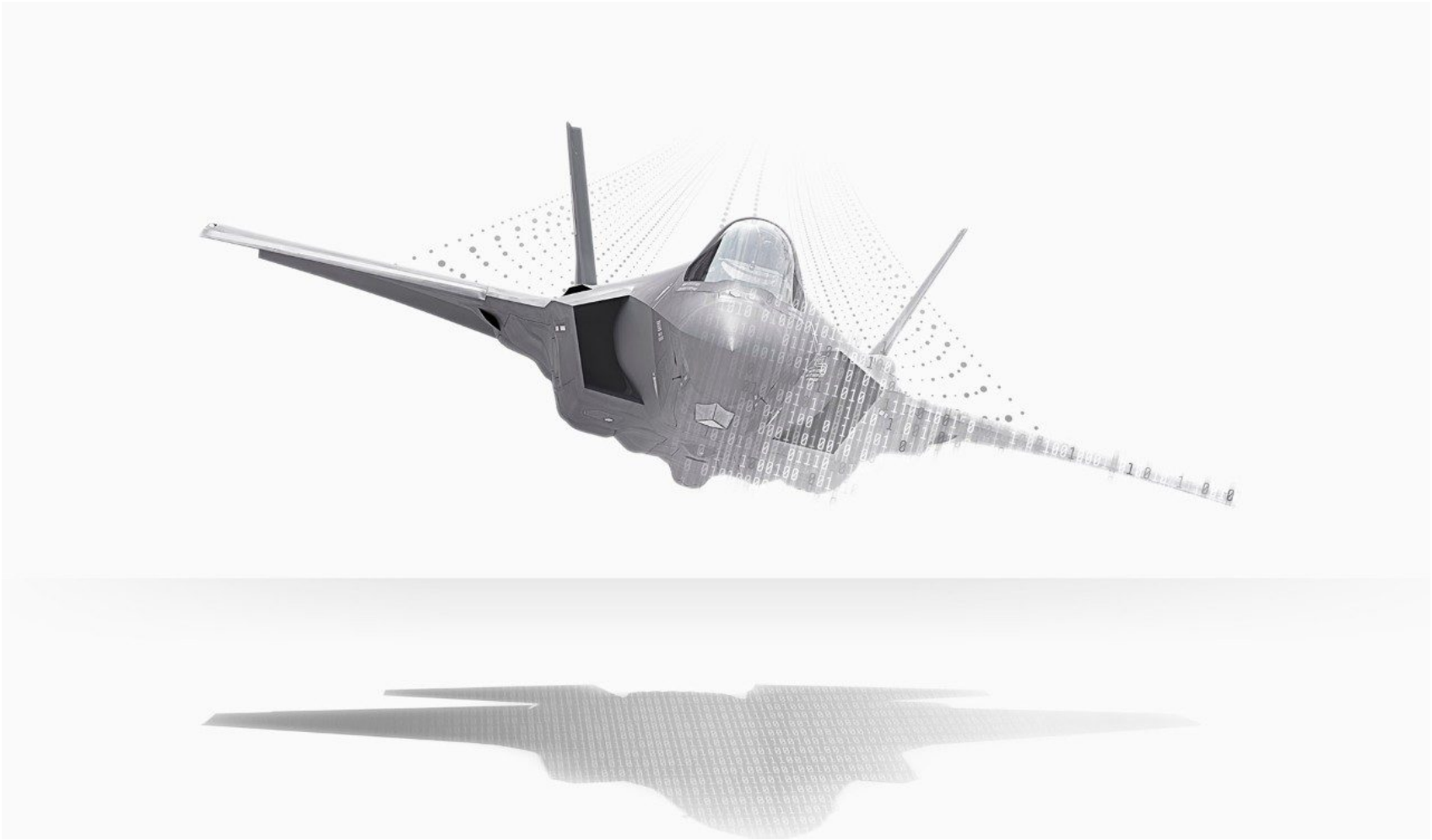
FCEFyN FACULTAD DE CIENCIAS EXACTAS, FÍSICAS y NATURALES

SECRETARÍA DE EXTENSIÓN

Houston, tenemos un problema.!!

El software tiene vulnerabilidades

Bueno, pero no todo es software en el ciberespacio. Ohhhhh...!!



El software tiene vulnerabilidades

¿ Por qué tiene vulnerabilidades el software ?

El mercado marca el ritmo

Llegar primero ha sido y es la premisa. Release o muerte..!!

El software tiene vulnerabilidades

¿ Por qué tiene vulnerabilidades el software ?

El mercado marca el ritmo

Llegar primero ha sido y es la premisa. Release o muerte..!!

Los arquitectos de software

Poco pueden hacer cuando toda la organización es devota del mercado. Quizás esté bien que así lo sea. Peeero...

El software tiene vulnerabilidades

¿ Por qué tiene vulnerabilidades el software ?

El mercado marca el ritmo

Llegar primero ha sido y es la premisa. Release o muerte..!!

Los arquitectos de software

Poco pueden hacer cuando toda la organización es devota del mercado. Quizás esté bien que así lo sea. Peeero...

Si hubiera o hubiese herramientas

Algunas se han construido, pero no han evolucionado al ritmo de otras.

El software tiene vulnerabilidades

¿ Por qué tiene vulnerabilidades el software ?

El mercado marca el ritmo

Llegar primero ha sido y es la premisa. Release o muerte..!!

Los arquitectos de software

Poco pueden hacer cuando toda la organización es devota del mercado. Quizás esté bien que así lo sea. Peeero...

Si hubiera o hubiese herramientas

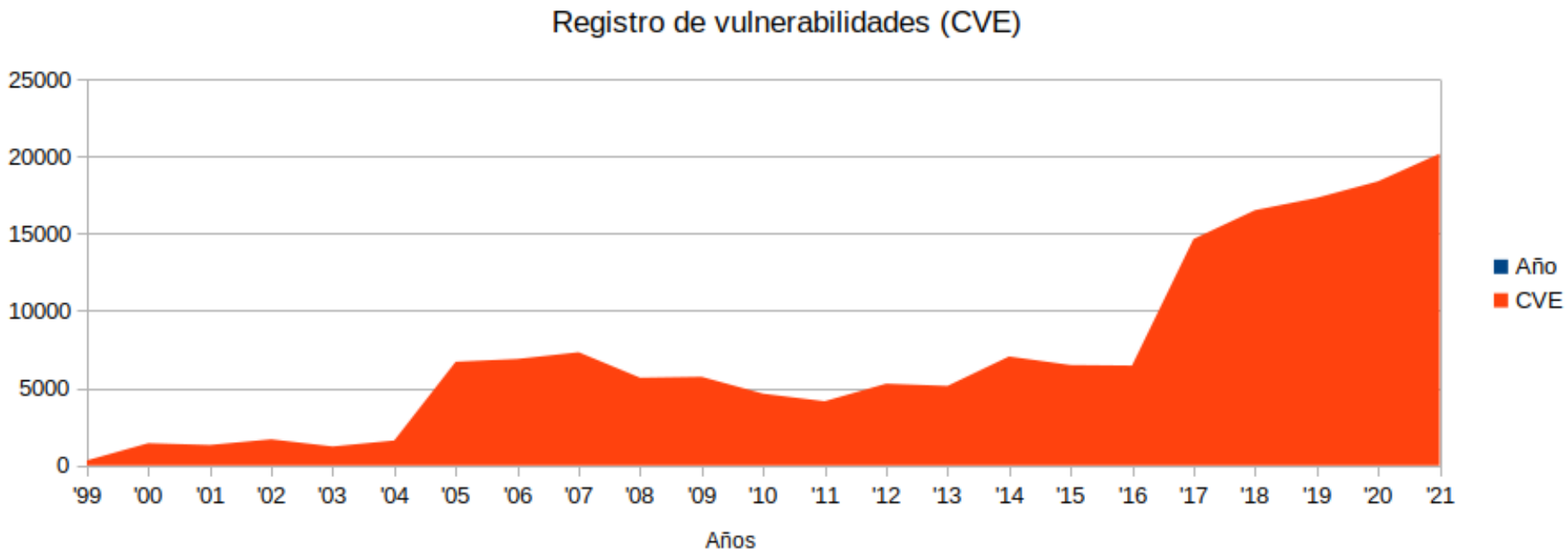
Algunas se han construido, pero no han evolucionado al ritmo de otras.

¿ Y la academia qué dice ?

En el año 2010 presenté mi informe de Maestría **Elicitación y trazabilidad de requerimientos utilizando patrones de seguridad** y desde al menos 10 años atrás ya existían propuestas de mejoras.

Vulnerabilidades (CVE)

El concepto original de lo que luego se convertió en la lista de Common Vulnerabilities and Exposures **(CVE)** fue presentado en enero de 1999. Desde ese año se llevan registradas mas de 166.000 vulnerabilidades.



Ref.:Metrics Published CVE Records

Vulnerabilidades (CWE™)

Hoy existe un "conocimiento" contenido en la terna **CVE**, Common Weakness Enumeration **(CWE)** y Common Attack Pattern Enumerations and Classifications **(CAPEC)** que intenta consolidarse como una tabla periódica de exposiciones.

1000 - Research Concepts

- Improper Access Control - *(284)*
- Improper Interaction Between Multiple Correctly-Behaving Entities - *(435)*
- Improper Control of a Resource Through its Lifetime - *(664)*
- Incorrect Calculation - *(682)*
- Insufficient Control Flow Management - *(691)*
- Protection Mechanism Failure - *(693)*
- Incorrect Comparison - *(697)*
- Improper Check or Handling of Exceptional Conditions - *(703)*
- Improper Neutralization - *(707)*
- Improper Adherence to Coding Standards - *(710)*

Ref.:CWE VIEW: Research Concepts

Conceptos de amenaza, vulnerabilidad, riesgo

¿ Te has sentado alguna vez sobre una silla de tres patas ? Hay direcciones en las cuales no es conveniente descargar el peso.!!

Amenaza

Toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información.

Conceptos de amenaza, vulnerabilidad, riesgo

¿ Te has sentado alguna vez sobre una silla de tres patas ? Hay direcciones en las cuales no es conveniente descargar el peso.!!

Amenaza

Toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información.

Vulnerabilidad

Debilidad o fallo en un sistema de información que pone en riesgo su seguridad pudiendo permitir que un atacante comprometa la integridad, disponibilidad o confidencialidad de la información.

Conceptos de amenaza, vulnerabilidad, riesgo

¿ Te has sentado alguna vez sobre una silla de tres patas ? Hay direcciones en las cuales no es conveniente descargar el peso.!!

Amenaza

Toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información.

Vulnerabilidad

Debilidad o fallo en un sistema de información que pone en riesgo su seguridad pudiendo permitir que un atacante comprometa la integridad, disponibilidad o confidencialidad de la información.

Riesgo

Está asociado a una probabilidad de que se produzca un incidente de seguridad, haciéndose efectiva una amenaza que aprovecha una vulnerabilidad, de este modo causando pérdidas o daños.

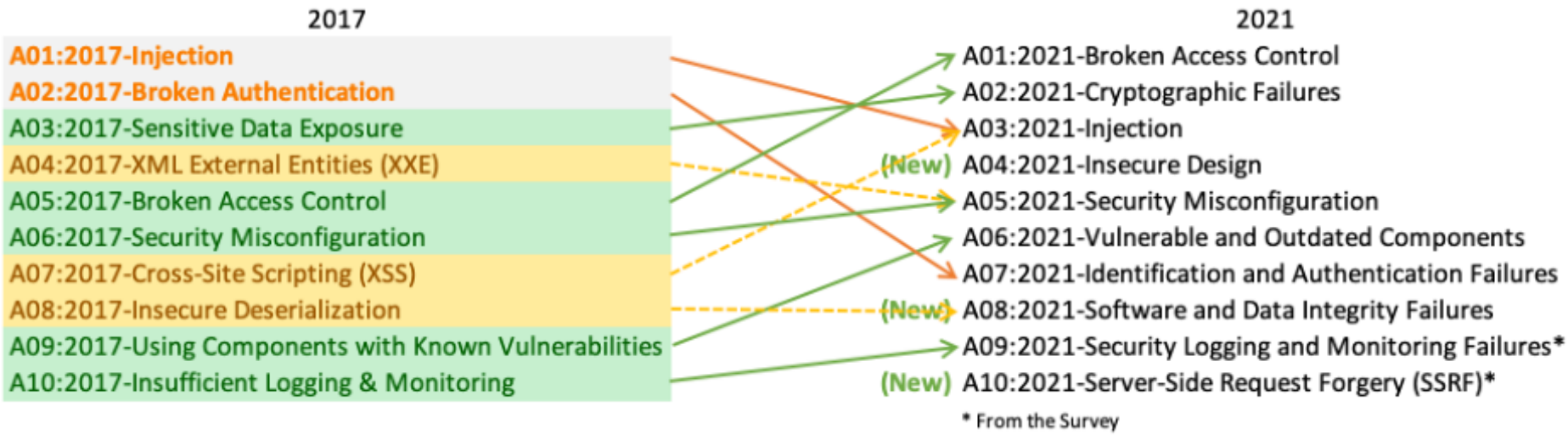
Open Web Application Security Project (OWASP)

Fundación sin fines de lucro que trabaja para mejorar la seguridad del software con proyectos de software de código abierto liderados por la comunidad, cientos de capítulos locales en todo el mundo, decenas de miles de miembros, conferencias educativas y capacitación de líderes, la Fundación OWASP es una de las fuentes para que los desarrolladores y tecnólogos protejan la web.

Ref.: OWASP

OWASP Top 10

Podemos ver que en el TOP 10 no hay muchos cambios, sin embargo aparecen nuevas categorías interesantes.!!



Ref.: OWASP TOP 10

OWASP Top 10 Nuevas categorías 2021

Insecure Design

Enfocada en los riesgos relacionados con fallas de diseño. Si realmente queremos **"movernos a la izquierda"** como industria, necesitamos más modelos de amenazas, patrones y principios de diseño seguros y arquitecturas de referencia.

OWASP Top 10 Nuevas categorías 2021

Insecure Design

Enfocada en los riesgos relacionados con fallas de diseño. Si realmente queremos **"movernos a la izquierda"** como industria, necesitamos más modelos de amenazas, patrones y principios de diseño seguros y arquitecturas de referencia.

Software and Data Integrity Failures

Se centra en aspectos relacionadas con actualizaciones de software, datos críticos y pipelines de CI/CD sin verificar integridad.

OWASP Top 10 Nuevas categorías 2021

Insecure Design

Enfocada en los riesgos relacionados con fallas de diseño. Si realmente queremos **"movernos a la izquierda"** como industria, necesitamos más modelos de amenazas, patrones y principios de diseño seguros y arquitecturas de referencia.

Software and Data Integrity Failures

Se centra en aspectos relacionadas con actualizaciones de software, datos críticos y pipelines de CI/CD sin verificar integridad.

Server-Side Request Forgery

Las fallas de SSRF ocurren cada vez que una aplicación web obtiene un recurso remoto sin validar la URL proporcionada por el cliente. Permite que un atacante obligue a la aplicación a enviar una solicitud manipulada a un destino inesperado, incluso cuando está protegida por un firewall, VPN u otro tipo de lista de control de acceso a la red (ACL).

Diseño inseguro en un contexto de CI/CD

Hoy, a mi entender, es la madre de todas las batallas.!!

Recomendaciones

- Establecer y utilizar un ciclo de vida de desarrollo seguro con profesionales de AppSec para ayudar a evaluar y diseñar controles relacionados con la seguridad y la privacidad.

Diseño inseguro en un contexto de CI/CD

Hoy, a mi entender, es la madre de todas las batallas.!!

Recomendaciones

- Establecer y utilizar un ciclo de vida de desarrollo seguro con profesionales de AppSec para ayudar a evaluar y diseñar controles relacionados con la seguridad y la privacidad.
- Establezca y use una biblioteca de patrones de diseño seguros o componentes listos para usar.

Diseño inseguro en un contexto de CI/CD

Hoy, a mi entender, es la madre de todas las batallas.!!

Recomendaciones

- Establecer y utilizar un ciclo de vida de desarrollo seguro con profesionales de AppSec para ayudar a evaluar y diseñar controles relacionados con la seguridad y la privacidad.
- Establezca y use una biblioteca de patrones de diseño seguros o componentes listos para usar.
- Utilice un modelo de amenazas para autenticaciones críticas, controles de acceso, lógica empresarial y flujos de claves.

Diseño inseguro en un contexto de CI/CD

Hoy, a mi entender, es la madre de todas las batallas.!!

Recomendaciones

- Establecer y utilizar un ciclo de vida de desarrollo seguro con profesionales de AppSec para ayudar a evaluar y diseñar controles relacionados con la seguridad y la privacidad.
- Establezca y use una biblioteca de patrones de diseño seguros o componentes listos para usar.
- Utilice un modelo de amenazas para autenticaciones críticas, controles de acceso, lógica empresarial y flujos de claves.
- Integre los controles de seguridad en las historias de usuario

Diseño inseguro en un contexto de CI/CD

Hoy, a mi entender, es la madre de todas las batallas.!!

Recomendaciones

- Establecer y utilizar un ciclo de vida de desarrollo seguro con profesionales de AppSec para ayudar a evaluar y diseñar controles relacionados con la seguridad y la privacidad.
- Establezca y use una biblioteca de patrones de diseño seguros o componentes listos para usar.
- Utilice un modelo de amenazas para autenticaciones críticas, controles de acceso, lógica empresarial y flujos de claves.
- Integre los controles de seguridad en las historias de usuario
- Escriba pruebas unitarias y de integración para validar que todos los flujos críticos sean resistentes al modelo de amenazas. Compile casos de uso y casos de uso indebido para cada nivel de su aplicación.

Diseño inseguro en un contexto de CI/CD

Hoy, a mi entender, es la madre de todas las batallas.!!

Mas recomendaciones

- Utilice firma digital o mecanismos similares para verificar que el software o los datos provengan de la fuente esperada y no hayan sido alterados.
- Asegúrese de que librerías y dependencias se consuman de repositorios confiables. Si su organización tiene un perfil de mayor riesgo, considere alojar un repositorio interno, conocido, que esté examinado.
- Asegúrese de que haya un proceso de revisión de cambios de código y configuración para minimizar la posibilidad de que se introduzcan códigos o configuraciones maliciosos en su proceso de software.

Si alguien tiene una propuesta, bienvenida es...

¿ Algunas buenas ideas ?

Evaluemos estas

- Dejemos de utilizar software..!!
- Desconectemos nuestros software de internet.

Si alguien tiene una propuesta, bienvenida es...

¿ Algunas buenas ideas ?

Evaluemos estas

- Dejemos de utilizar software..!!
- Desconectemos nuestros software de internet.
- Tenemos nuestros propios data center, no utilizamos la nube.
- Desarrollamos nuestras propias soluciones.

Si alguien tiene una propuesta, bienvenida es...

¿ Algunas buenas ideas ?

Evaluemos estas

- Dejemos de utilizar software..!!
- Desconectemos nuestros software de internet.
- Tenemos nuestros propios data center, no utilizamos la nube.
- Desarrollamos nuestras propias soluciones.
- ...
- ¿ Han escuchado hablar de pasivo tecnológico ?
- ...

Si alguien tiene una propuesta, bienvenida es...

¿ Algunas buenas ideas ?

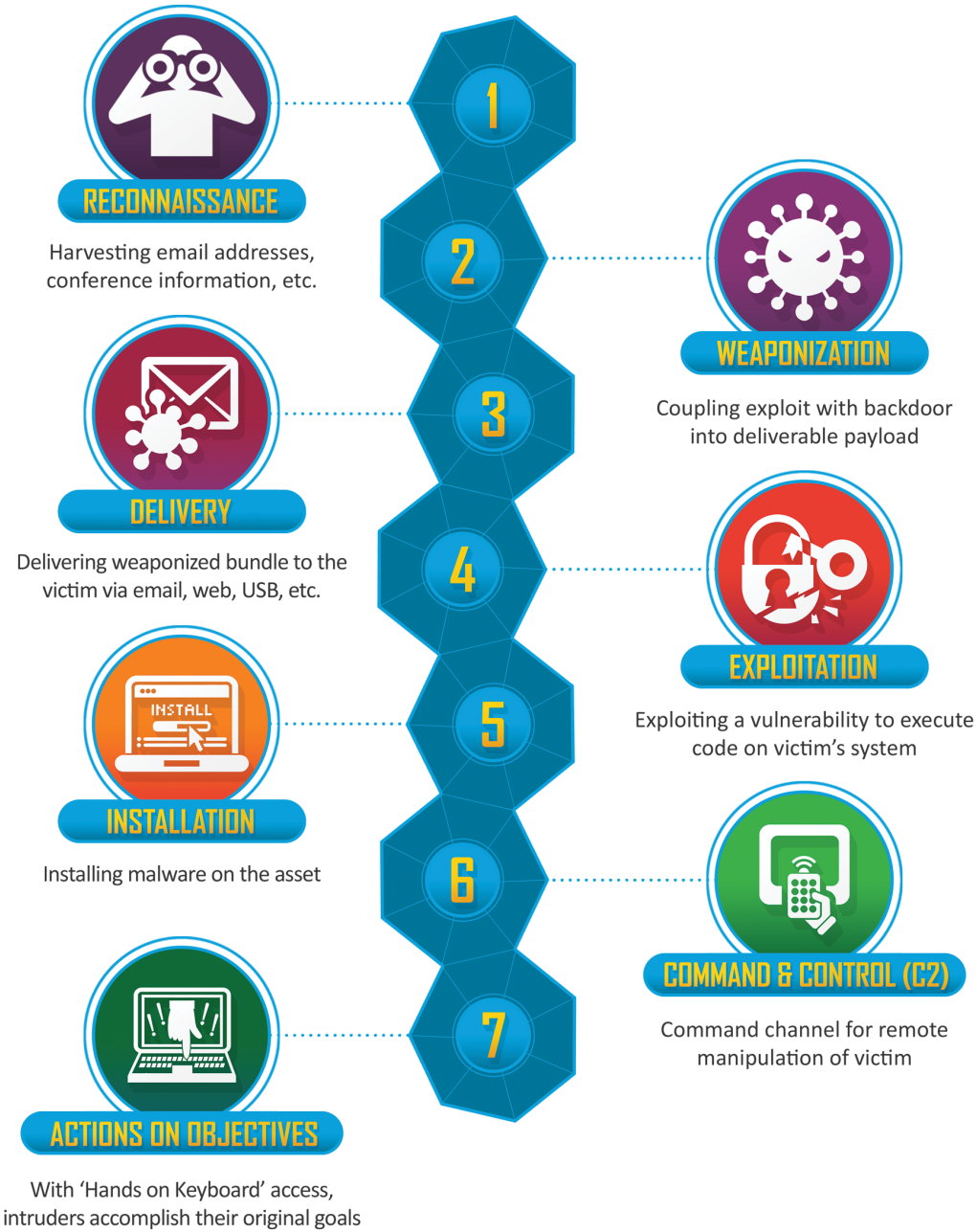
Evaluemos estas

- Dejemos de utilizar software..!!
- Desconectemos nuestros software de internet.
- Tenemos nuestros propios data center, no utilizamos la nube.
- Desarrollamos nuestras propias soluciones.
- ...
- ¿ Han escuchado hablar de pasivo tecnológico ?
- ...
- ¿ Cómo se desarrolla una acción ofensiva ?

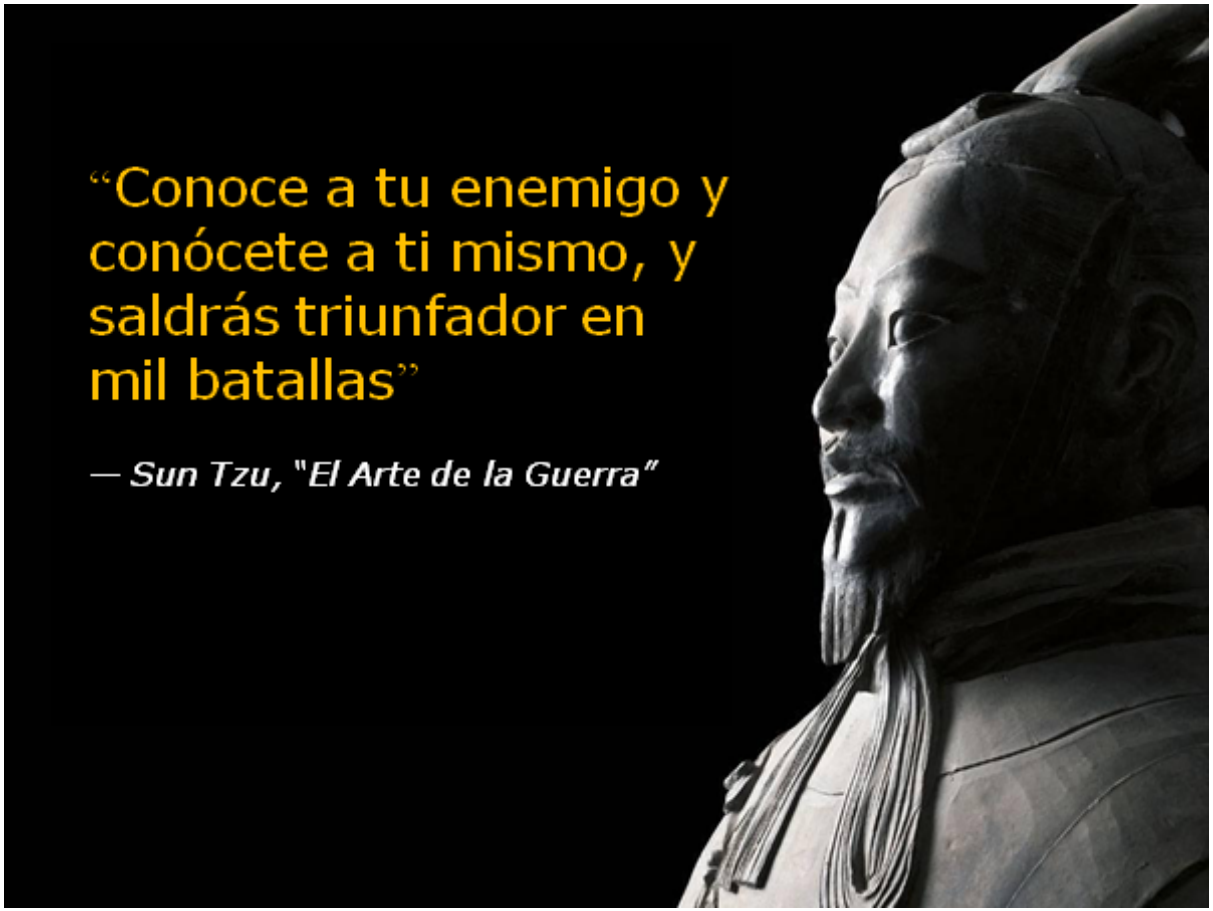
The Cyber Kill Chain

¿ Cómo se desarrolla una acción ofensiva ?

by Lockheed Martin



Debemos anticipar las acciones ofensivas



¿ Cómo mejorar nuestra resiliencia a las acciones ofensivas en el ciberespacio ?

Muchas gracias