Centro de
Investigación en
Computación

Introducción

Al análisis y detección de malware

Definitions

Research

Course

Análisis y Detección de Malware

Instructor

Acosta Bermejo Raúl

Lecture notes

2024-B
28 de agosto del 2024
Última actualizacioón

Instituto
Politécnico
Nacional

Table of contents (outline)

Tabla de contenido

1. Introducción
   - Conceptos básicos
   - Marco general
2. Estándares
   - 1ª parte
   - 2ª parte
3. Varios temas
   - Soluciones (Software/papers)

Conceptos Básicos

Definiciones

Conceptos

Definiciones

Malware

1. Malware or malicious software is any computer software intended to harm the host operating system or to steal sensitive data from users, organizations or companies.
2. Malware may include viruses, worms, trojan horses, and spyware that gathers user information without permission.
3. Taxonomias
    i. Tipos: Rootkits, botnets, Toyanos, etc.

Conceptos

Definiciones

Quien
Objetivo (target)
Daño

Amenaza / Threat

- NIST definition

  Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

- Wikipedia definition.

  It is a potential negative action or event facilitated by a vulnerability that results in an unwanted impact to a computer system or application. A threat can be either:

  - A negative "intentional" event: i.e. hacking: an individual cracker or a criminal organization.
  - An "accidental" negative event: e.g. the possibility of a computer malfunctioning, or the possibility of a natural disaster event such as an earthquake, a fire, or a tornado.
  - Otherwise a circumstance, capability, action, or event.

Conceptos

Definiciones

probability vs likelihood

Riesgo / Risk

Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización.

- NIST definition

  A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

- Actividades
  - Análisis: Identificar los riesgos.
  - Evaluación (*Risk assesment*): Calcular la probabilidad.
  - Gestión: Que hacer para prevenirlos, mitigarlos (elim)
- Estándares
  - MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), Versión 3.

Conceptos

Definiciones

Ataque / Attack

- NIST definition

  Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.

- Varias clasificaciones de los Tipos de ataque. La más sencilla:
  - Al sistema operativo.
  - A un error de configuración.
  - A una aplicación.
- Estándar
  - https://attack.**mitre**.org/ Muy completa (extensa)

Conceptos

Definiciones

Debilidad / Weakness

- NIST definition

  Defect or characteristic that may lead to undesirable behavior.
- Estándar
  - Uno de los más conocidos y completos:

    https://cwe.**mitre**.org/
  - La mayoría son en software pero tambien contempla en hardware, configuración, etc.

Conceptos

Definiciones

A flaw (defecto) is unintended functionality. This may either be a result of poor design or through mistakes made during implementation.

Vulnerabilidad / Vulnerability

- NIST definition

  Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

- NCSC definition

  It is a weakness in an IT system that can be exploited by an attacker to deliver a successful attack. They can occur through flaws, features or user error, and attackers will look to exploit any of them, often combining one or more, to achieve their end goal.

- Estándares
  - CVSS (Common Vulnerability Scoring System) creado por el NIST y aplicado en NVD (National Vulnerability Database).

    It is a method used to supply a qualitative measure of severity. CVSS is not a measure of risk. CVSS consists of three metric groups: Base, Temporal, and Environmental.

Conceptos

Definiciones

Vulnerability Vs Weakness

- Weaknesses and vulnerabilities are both states that indicate security risks.
- While weakness refers to an application error or bug, it may escalate to a vulnerability in cases where it can be exploited to perform a malicious action.
- The difference between a weakness and a vulnerability is the availability of a specific payload allowing it to be exploited.
- Once an exploit is available it is considered a confirmed vulnerability and as such it holds greater risk to the application security.

All vulnerabilities rely on weaknesses,

but not all weaknesses entail vulnerabilities.

Conceptos

Definiciones

Explotar, aprovechar / Exploit

- Es un programa informático, una parte de un software o una secuencia de comandos que se aprovecha de un error o vulnerabilidad para provocar un comportamiento no intencionado o imprevisto en un software, hardware o en cualquier dispositivo electrónico.
- Estos comportamientos incluyen, por lo general, la toma del control de un sistema, la escalación de privilegios, etc.
- Las vulnerabilidades de Día Cero (también conocidas como 0-day exploits) son las brechas de seguridad en el software desconocidas hasta el momento del ataque.

Conceptos

Definiciones

Jeopardizes
Daño (noun)
Comprometer (verb)

Incidente de Seguridad / Security Incident

- NIST definition

  An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

- Propiedades en Seguridad
  - Criptografía

    Confidentiality, Integrity, Authentication, Non-repudiation
    Cifrado F. Hash. Digital signatures **Implementaciones**
  - Infraestructura

    Availability

Accountability
Propiedad de un recurso del sistema que asegura que las acciones de una entidad del sistema puedan ser rastreadas sin ambiguedad, lo que la hace responsable de sus acciones.

Conceptos

Definiciones

Brecha de seguridad / Breach

- *It is any incident that results in unauthorized access to computer data, applications, networks or devices*.
- Una brecha de seguridad es “un incidente de seguridad que afecta a datos de carácter personal” y que, además, puede ocasionar la “destrucción, pérdida, alteración accidental o ilícita de los datos personales transmitidos, conservados o tratados, así como la comunicación o el acceso no autorizados a los mismos.” Fuente AEPD (España).
- Con independencia de si se ha originado como consecuencia de un accidente o si se trata de una acción intencionada y de que afecte a datos en formato digital o en formato papel.
- Un incidente puede tratarse, por ejemplo, de una infección con malware o un ataque DDOS. No supone el acceso a la red ni la pérdida de datos. Por lo tanto, no lo podemos considerar brecha de seguridad.

https://www.kaspersky.com/resource-center/threats/what-is-a-security-breach

Conceptos

Definiciones

Resumen

Los conceptos anteriores se relacionan de la siguiente forma:

Weakness => Vulnerability => Exploit => Security Incident => Security breach
=> Security Event
=> Threat

Conceptos

Definiciones

Criptografía Infraestructura
Implementaciones

Propiedades

- Confidencialidad / Cifrado[Cripto]
- Integridad / Funciones Hash[Cripto] (FH)
- Autenticación / Firmas digitales[Cripto] (FH y sistemas)

  Consistente en poder verificar que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. Violaciones de esta propiedad son la manipulación del origen o el contenido de los datos y en el caso de los usuarios o servicios se da la Suplantación de Identidad.

- Disponibilidad / Redundancia[Infra]

  Disposición de los servicios a ser usados cuando sea necesario. Ataques buscan la Interrupción del Servicio y su productividad.

- Trazabilidad / Bitacoras[Infra]

  Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento. La trazabilidad es esencial para analizar los incidentes, perseguir a los atacantes y aprender de la experiencia. La trazabilidad se materializa en la integridad de los registros de actividad.

Conceptos

Definiciones

Varios conceptos

- Cracking
  - Es un parche creado sin autorización del desarrollador del programa al que modifica cuya finalidad es la de modificar el comportamiento del *software* original.
  - Password cracking tools.
- Privilege escalation
  - It is the act of exploiting a bug, a design flaw, or a configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user.
  - *Jailbreaking* is defined as the act of removing limitations that a vendor attempted to hard-code into its software or services.

Conceptos

Definiciones

Varios conceptos

- Campaigns
  - An individual or group involved in malicious cyber activity is called a **Threat Actor**.
  - A set of activity (Incidents) carried out by Threat Actors using specific techniques (TTP) for some particular purpose is called a **Campaign**. Such activity might fit along the lines of stealing financial information from banking customers or targeting a particular business sector.
  - https://stixproject.github.io/documentation/idioms/campaign-v-actors/

Conceptos

Definiciones

Varios conceptos

- Policies / Políticas
  - Statements, rules or assertions that specify the correct or expected behavior of an entity.
  - For example, an authorization policy might specify the correct access control rules for a software component.
  - Other examples: Password policies.
- Security requirements / Requerimientos de software
  - .
- .

Conceptos

Definiciones

Servicios en la Nube

- Tipos
  - Software as a Service (SaaS) Aplicaciones
  - Platform as a Service (PaaS) Sistema Operativo, BD, etc
  - Infrastructure as a Service (IaaS) Hardware, Servidores, Switches
- Para el malware existe:
  - Malware as a Service (MaaS)
  - Ransomware a Service (RaaS)

Conceptos

Definiciones

Hacker

BlackHat

Ejemplos

- Lizard Squad

  4 cracker que atacaron la industria del Videojuego a partir del 2014 usando DDoS.
- Anonymous
  - http://www.anonops.net/
- Ciberactivismo

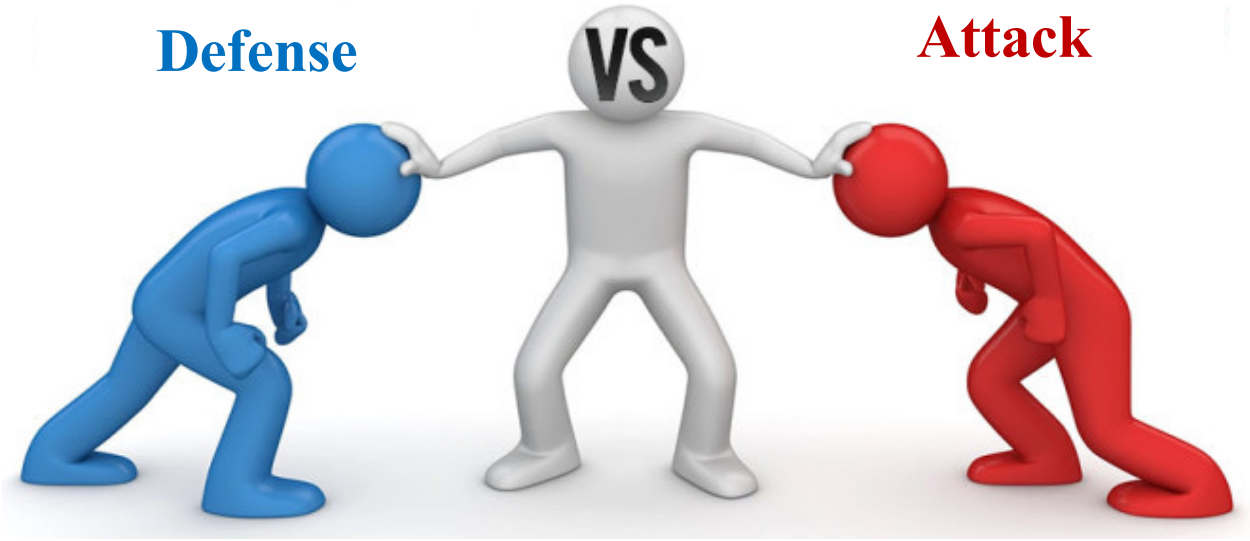
Introduction

Introducción

Marco general

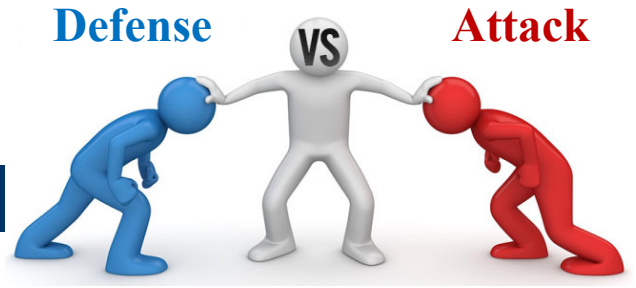
Introduction

Motivación



Introduction

Motivación



Attacks

- Diseño
  - Estrategía
  - Táctica
- Origen
  - Local
  - Remoto

Vulnerabilities
Vulnerabilidades
Por mal diseño o límites

⟺

Exploit
(explotar/aprovechar)
Code used to take advantage vulnerabilities in software code and configuration, usually to install malware.

Threat
Amenaza
Attack Vector

Malware

Trojans Virus Code injection

Introduction

Motivación

Eavesdrop / Scan
Escuchar a escondidas furtivamente

Local attacks

- Bugs
  - NULL pointer dereference bugs
  - Denial of Service Exploits (DoSE)
- System instability vulnerabilities
  - For example, Configuration
- To privilege escalation threats

Ataques en Red

From network:

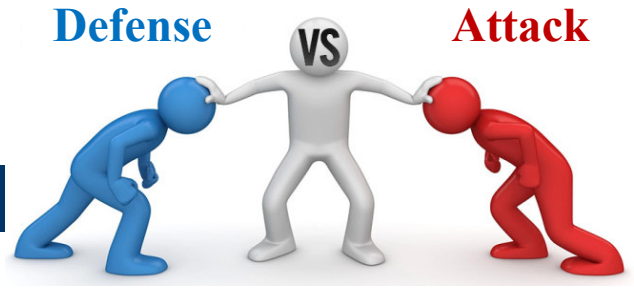
- Botnet
- DoS (Denial of Service) of Protocols

Several types:

- Trojans
- Backdoors

Introduction

Motivación



Defense

Some of the main thecniques used are:

- Trusted Computing Base (TCB)

  It is the set of all hardware, firmware, and/or software components that are critical to its security, in the sense that bugs or vulnerabilities occurring inside the TCB might jeopardize the security properties of the entire system.

- Static analysis of source code security
- Control-flow integrity (CFI).
- Dynamic Control-flow assertions (CFAs)

comprometer/poner en peligro

Introduction

Motivación

Database of Vulnerabilities

- CVE (Common Vulnerabilities and Exposures)
  - https://cve.mitre.org/
- Microsoft Security Bulletin
  - https://learn.microsoft.com/en-us/security-updates/
- MacOS X
  - https://support.apple.com/en-us/HT201222

Ver de Microsoft
MS17-023

Y luego su version
En la App

Introduction

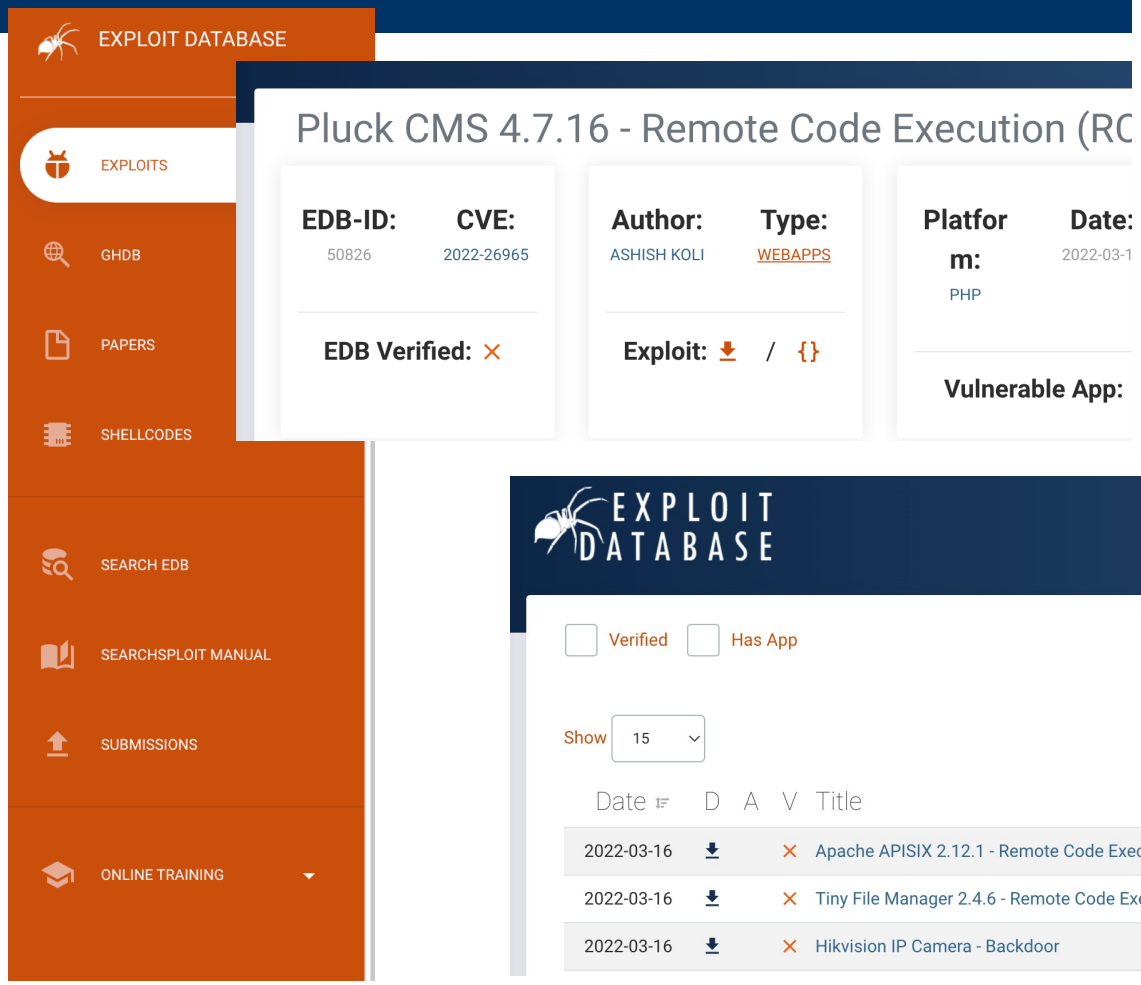
Motivación

Database of Exploits

- Exploit Database
  - https://www.exploit-db.com/
  - 45,095 exploits (15/mzo./2023)
- Metasploit
  - Version comercial
    https://www.rapid7.com/db/
  - Versón gratuita
    https://www.metasploit.com/download

Introduction

Motivación

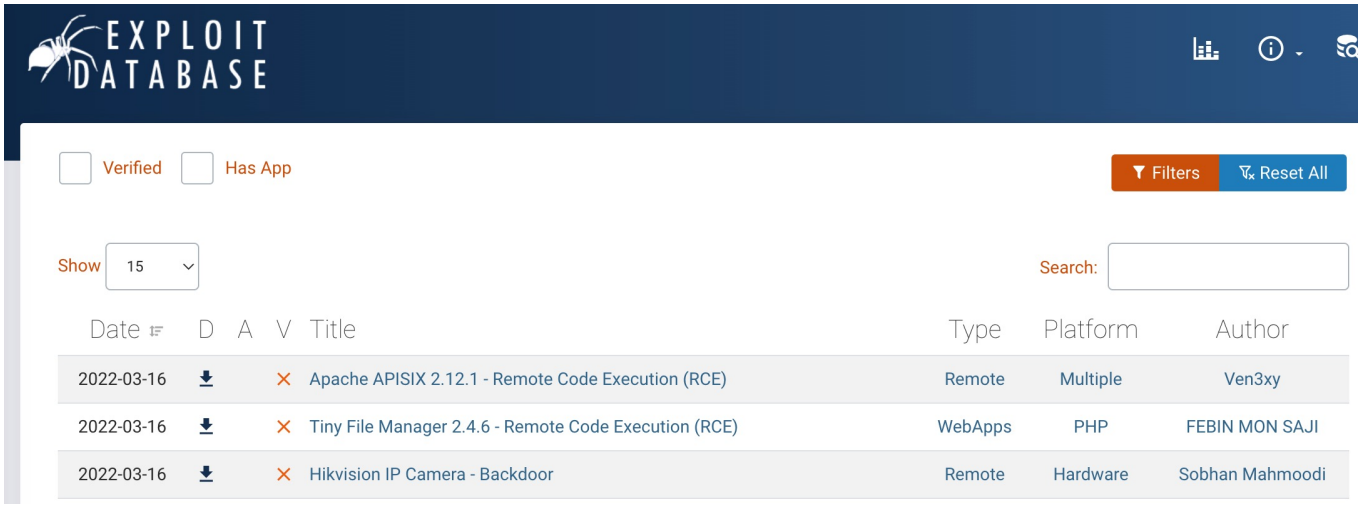



```
# Exploit Title: Pluck CMS 4.7.16 - Remote Code Execution (RCE) (Authentic
# Date: 13.03.2022
# Exploit Author: Ashish Koli (Shikari)
# Vendor Homepage: https://github.com/pluck-cms/pluck
# Version: 4.7.16
# Tested on Ubuntu 20.04.3 LTS
# CVE: CVE-2022-26965
# Usage : python3 exploit.py <IP> <Port> <Password> <Pluckcmspath>
# Example:  python3 exploit.py 127.0.0.1 80 admin /pluck
# Reference: https://github.com/shikari00007/Pluck-CMS-Pluck-4.7.16-Theme-

'''
Description:
A theme upload functinality in Pluck CMS before 4.7.16 allows an admin
privileged user to gain access in the host through the "themes files",
which may result in remote code execution.
'''


'''
Import required modules:
'''
import sys
import requests
import json
import time
import urllib.parse
import struct

'''
User Input:
'''
target_ip = sys.argv[1]
target_port = sys.argv[2]
password = sys.argv[3]
pluckcmspath = sys.argv[4]
```



Introduction

Bibliografía

Algunos links

- Cursos en Internet
  - http://securitytrainings.net/
  - http://opensecuritytraining.info/Training.html

- Libros
  - Android Hacker's handbook
  - Android Security Internals
  - A guide to Kernel exploitation
  - Books of Hacking Exposed Version 7, Malware & Rootkits
  - Hacking The art of exploitation
  - Malware Analyst's Cookbok and DVD
  - Practice Malware Analysis
  - Rootkits subverting the windows kernel
  - Moder malware for Dummies

Standars, Methodologies, etc.

Estándares de seguridad

1ª Parte

Standars

Introducción

SANS

- *SysAdmin Audit, Networking and Security Institute*
- Entrenamientos y certificaciones
  - GIAC certificaciones: caras pero las mejores.
  - En México hay escuelas parners.
- https://www.sans.org/
- Certificaciones
  - TODAS: https://www.sans.org/cyber-security-certifications
  - Malware: https://www.giac.org/certifications/reverse-engineering-malware-grem/

Standars

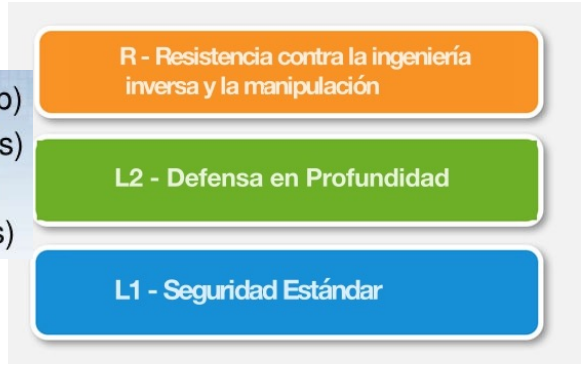
Introducción

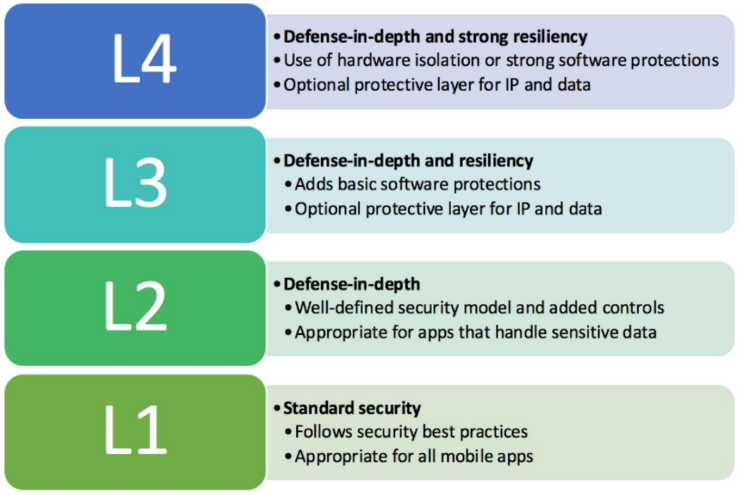
OWASP

- *Open Web Application Security Project*
  - OWASP Mobile Security Testing Guide

Ver 1.0

- MASVS-L1 (e.g. social media app)
- MASVS-L1+R (e.g. mobile games)
- MASVS-L2 (e.g. healthcare app)
- MASVS-L2+R (e.g. banking apps)





OWASP MASVS LEVELS

Links

- https://owasp.org/
- https://owasp.org/www-project-mobile-security-testing-guide/

Standars

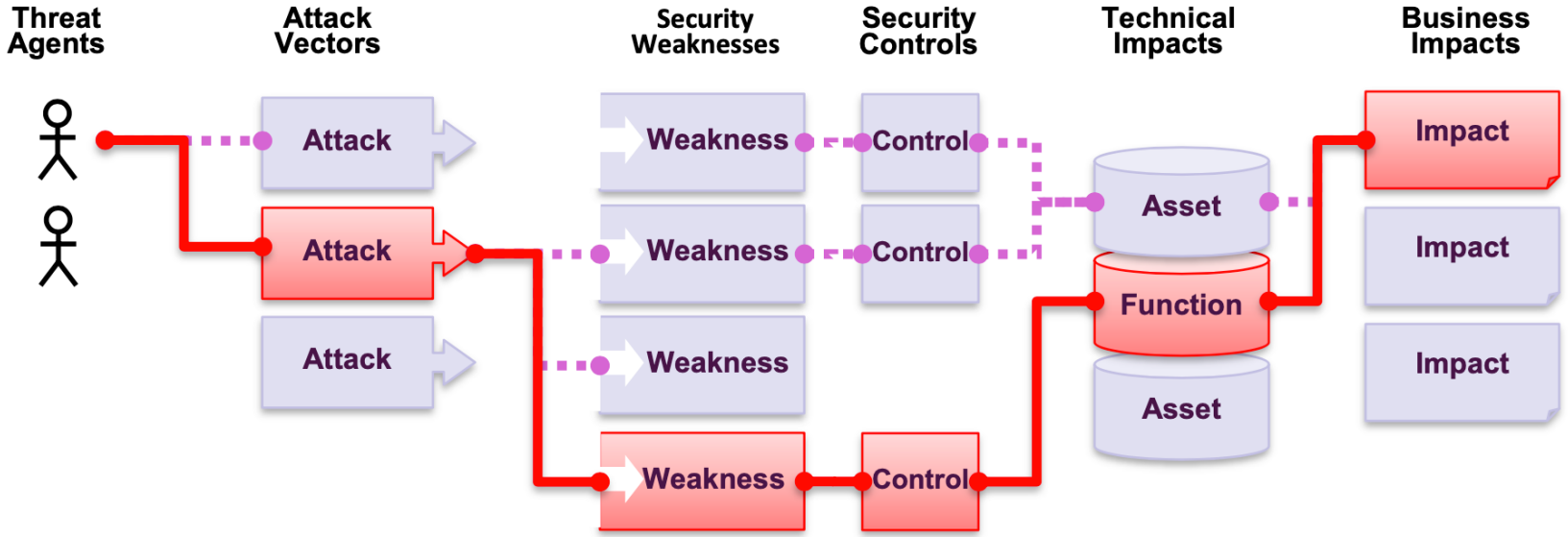
OWASP

Conceptos

Threat
Attacl Vector
Weakness
Security Control
Asset
Risk

What Are Application Security Risks?

Attackers can potentially use many different paths through your application to do harm to your business or organization. Each of these paths represents a risk that may, or may not, be serious enough to warrant attention.



Sometimes these paths are trivial to find and exploit, and sometimes they are extremely difficult. Similarly, the harm that is caused may be of no consequence, or it may put you out of business. To determine the risk to your organization, you can evaluate the likelihood associated with each threat agent, attack vector, and security weakness and combine it with an estimate of the technical and business impact to your organization. Together, these factors determine your overall risk.

Standars

Introducción

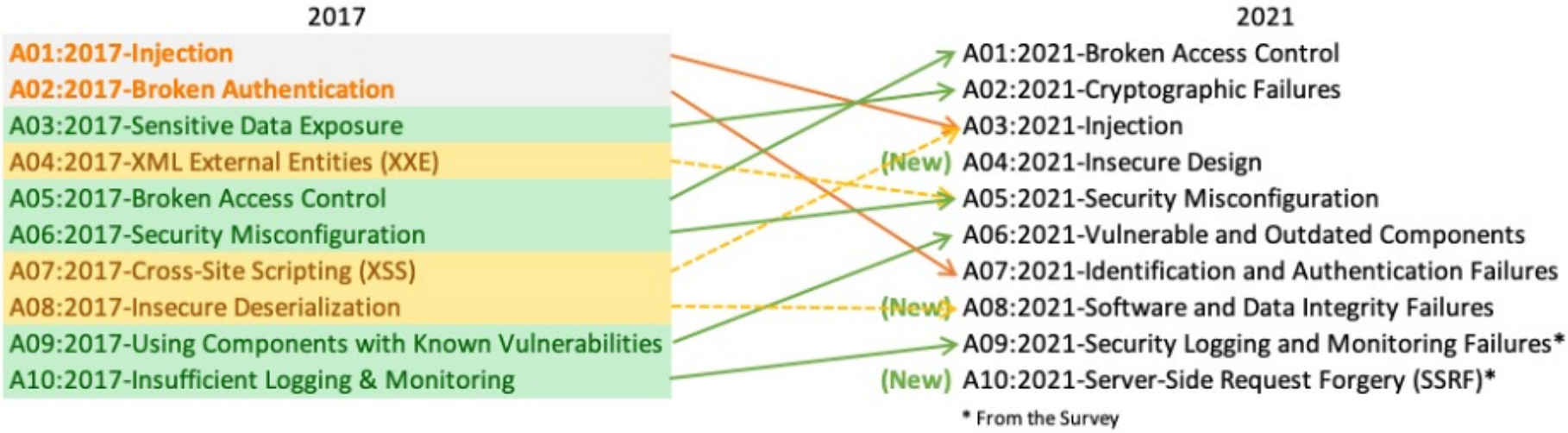
OWASP

OWASP Top 10 – 2013		OWASP Top 10 – 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

Standars

Introducción

OWASP



Standars

Introducción

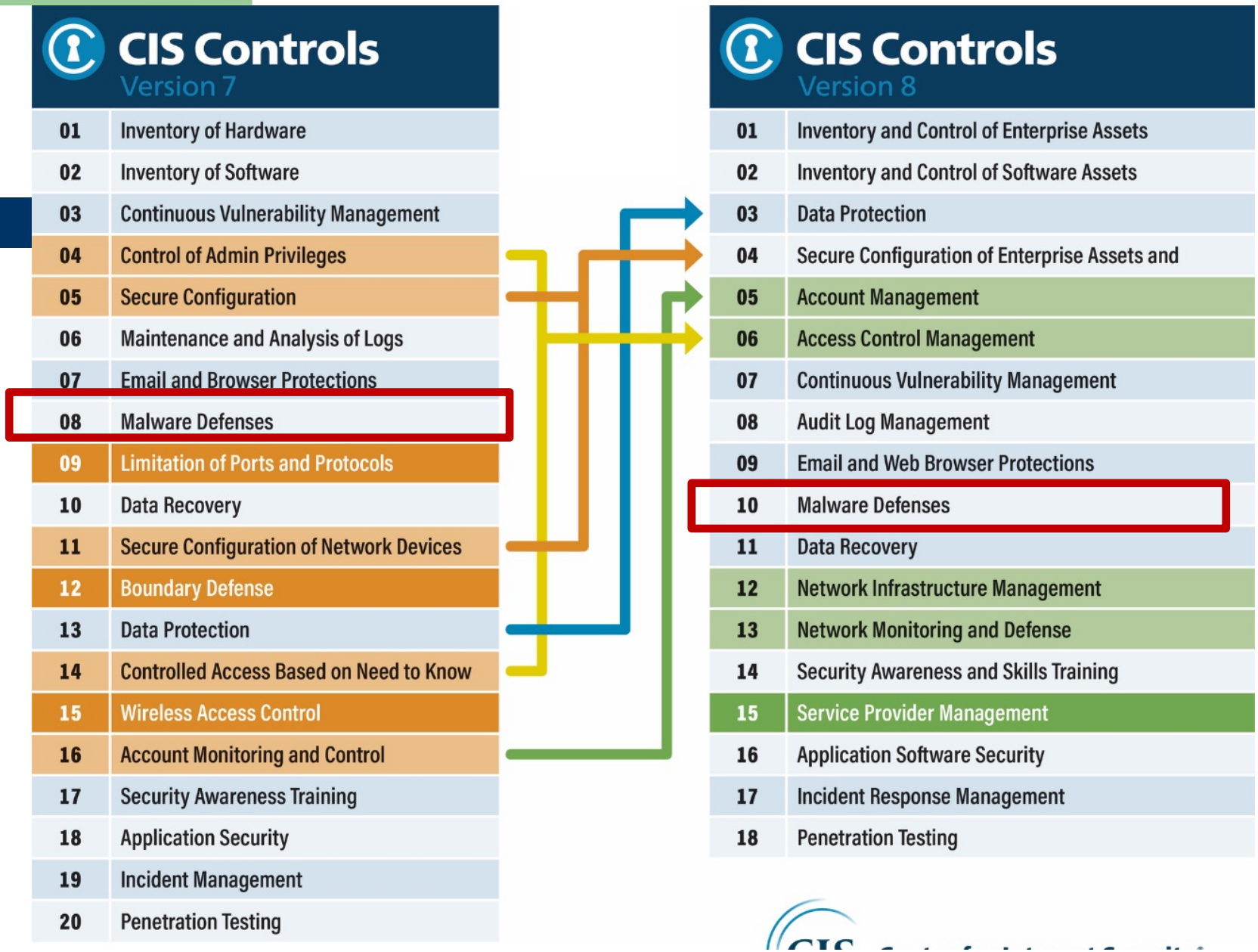
CIS

- *Critical Security Controls*
- Genera varios documentos y el más utilizado es:
  - CIS Critical Security Controls, ver 8.
- https://www.cisecurity.org/

Noticias importantes

- https://www.elfinanciero.com.mx/nacional/2022/02/22/sedena-presenta-fallas-en-su-ciberseguridad/

CIS



CIS Controls Version 7	
01	Inventory of Hardware
02	Inventory of Software
03	Continuous Vulnerability Management
04	Control of Admin Privileges
05	Secure Configuration
06	Maintenance and Analysis of Logs
07	Email and Browser Protections
08	Malware Defenses
09	Limitation of Ports and Protocols
10	Data Recovery
11	Secure Configuration of Network Devices
12	Boundary Defense
13	Data Protection
14	Controlled Access Based on Need to Know
15	Wireless Access Control
16	Account Monitoring and Control
17	Security Awareness Training
18	Application Security
19	Incident Management
20	Penetration Testing

CIS Controls Version 8	
01	Inventory and Control of Enterprise Assets
02	Inventory and Control of Software Assets
03	Data Protection
04	Secure Configuration of Enterprise Assets and
05	Account Management
06	Access Control Management
07	Continuous Vulnerability Management
08	Audit Log Management
09	Email and Web Browser Protections
10	Malware Defenses
11	Data Recovery
12	Network Infrastructure Management
13	Network Monitoring and Defense
14	Security Awareness and Skills Training
15	Service Provider Management
16	Application Software Security
17	Incident Response Management
18	Penetration Testing

Standars

CIS Controls

Standars

Introducción

CONTROL 10

Malware Defenses

SAFEGUARDS TOTAL	7	IG1	3/7	IG2	7/7	IG3	7/7

Overview

Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.

Why is this Control critical?

Malicious software (sometimes categorized as viruses or Trojans) is an integral and dangerous aspect of internet threats. They can have many purposes, from capturing credentials, stealing data, identifying other targets within the network, and encrypting or destroying data. Malware is ever-evolving and adaptive, as modern variants leverage machine learning techniques.

Malware enters an enterprise through vulnerabilities within the enterprise on end-user devices, email attachments, webpages, cloud services, mobile devices, and removable media. Malware often relies on insecure end-user behavior, such as clicking links, opening attachments, installing software or profiles, or inserting Universal Serial Bus (USB) flash drives. Modern malware is designed to avoid, deceive, or disable defenses.

Standars

Introducción

MITRE ATT&CK

- *Adversarial **T**actics, **T**echniques, and **C**ommon Knowledge*
- It is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.
- MITRE Corporation es una organización de investigación y desarrollo sin fines de lucro financiada con fondos federales encargada de idear soluciones para mantener a los Estados Unidos a salvo de diversas amenazas. Fue creada en el 2013.
- Tiene 3 categorías de nivel superior, dentro de las cuales hay matrices que describen las tácticas utilizadas por los atacantes, las técnicas que utilizan y las mitigaciones que las organizaciones pueden tomar para protegerse contra los atacantes para aumentar la ciberseguridad.
- https://attack.mitre.org/

Standars

Introducción

- La categoría Enterprise tiene una matriz de nivel superior que está disponible para ver en la página Enterprise Matrix. Tiene 14 subcategorías que incluyen diferentes números de técnicas y tácticas.

Standars

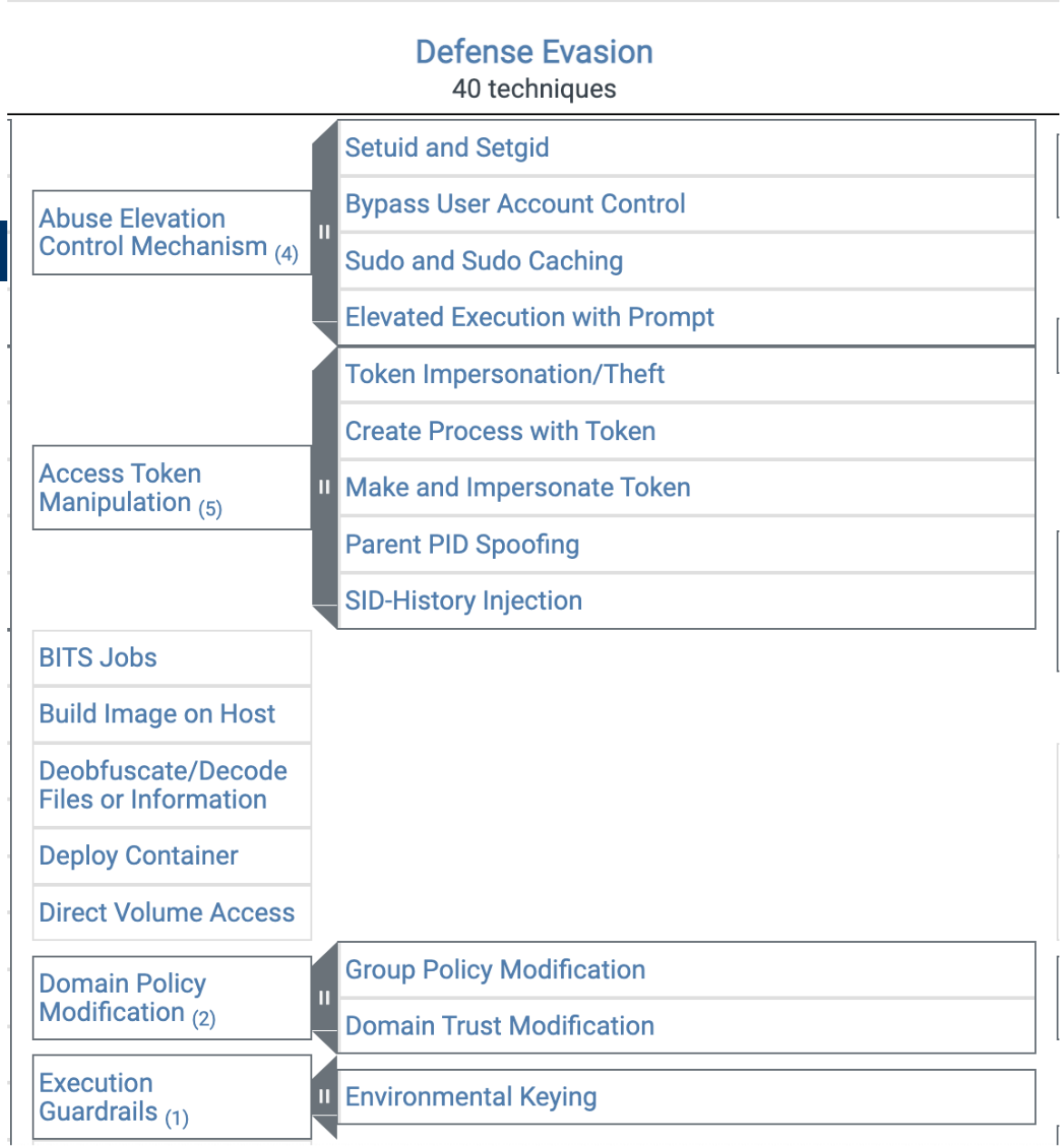
Introducción

Clasificación jerárquica

Deobfuscate/Decode Files or Inf

Adversaries may use Obfuscated Files or Information to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system.

One such example is use of certutil to decode a remote access tool portable executable file that has been hidden inside a certificate file. [1] Another example is using the Windows `copy /b` command to reassemble binary fragments into a malicious payload. [2]



Standars

CWE

Flaw: defecto, imperfección.

Common Weakness Enumeration

- It is a community-developed list of software and hardware weakness types that have security ramifications. It serves as a common language, a measuring stick for security tools, and as a baseline for weakness identification, mitigation, and prevention efforts.
- Weaknesses are flaws, faults, bugs, or other errors in software or hardware implementation, code, design, or architecture that if left unaddressed could result in systems, networks, or hardware being vulnerable to attack.
- The CWE List and associated classification **taxonomy** serve as a language that can be used to identify and describe these weaknesses in terms of CWEs.
- Example:

CWE-627: Dynamic Variable Evaluation

https://cwe.mitre.org/data/published/cwe_latest.pdf, 2,420 pags.

Standars

CWE CATEGORY: Bad Coding Practices

Category ID: 1006

Summary

Weaknesses in this category are related to coding practices that are deemed un
present in the application. These weaknesses do not directly introduce a vulnera
or maintained. If a program is complex, difficult to maintain, not portable, or sh
weaknesses are buried in the code.

Membership

Nature	Type	ID	Name
MemberOf	V	699	Software Developr
HasMember	B	478	Missing Default Ca
HasMember	B	487	Reliance on Packag
HasMember	B	489	Active Debug Code
HasMember	V	546	Suspicious Comme
HasMember	V	547	Use of Hard-coded
HasMember	B	561	Dead Code

CWE-627: Dynamic Variable Evaluation

Weakness ID: 627
Abstraction: Base
Structure: Simple

Presentation Filter: Complete

Description

In a language where the user can influence the name of a variable at runtime, if the variable na
to arbitrary variables, or access arbitrary functions.

Extended Description

The resultant vulnerabilities depend on the behavior of the application, both at the crossover po
the related variables or functions.

Alternate Terms

Dynamic evaluation

Relationships

Relevant to the view "Research Concepts" (CWE-1000)

Nature	Type	ID	Name
ChildOf	B	914	Improper Control of Dynamically-Identified Variables
PeerOf	B	183	Permissive List of Allowed Inputs

Relevant to the view "Software Development" (CWE-699)

Nature	Type	ID	Name
MemberOf	C	1006	Bad Coding Practices

Standars, Methodologies, Frameworks, etc.

Estándares de seguridad

2ª Parte

Standars

Introducción

ITIL

- .
- Vs ITSM

Security Model

Introducción

COBIT

- .

Security Model

Introducción

TOGAF

- .

Security Model

Introducción

SISM o SGS

Standard for Information Security Management,

En español tambien le llaman Sistema de Gestión de la Seguridad

- Definido el el ISO/IEC 27 mil
  - https://www.iso.org/isoiec-27001-information-security.html
- Obvio una empresa puede certificarse.

Grupos y Centros

De seguridad

Definiciones

Grupos y Centros

De seguridad

SOC

Security Operation Center, en español Centro de Operaciones de Seguridad

- Es el equipo responsable de garantizar la seguridad de la información y esta conformado por:
  - Una plataforma que permite la supervisión y administración de la seguridad del sistema de información a través de herramientas de recogida, correlación de eventos e intervención remota.
  - El **SIEM** (Security Information Event Management) es la principal herramienta del SOC ya que permite gestionar los eventos de un SI.
- Porque crear uno?
  - La creación y operación de un SOC es complicada y costosa. Las empresas los establecen por varias razones, tales como:
  - Proteger los datos confidenciales
  - Cumplir con las normas de la industria o las gubernamentales.

Grupos y Centros

De seguridad

1. Data collection & Correlation.
2. Proactive Detection of Malicious Activity
3. Security Monitoring
4. Incident Response
5. Compliance Management and Reporting

SOC

The 10 key functions performed:

1. Take Stock of Available Resources
2. Preparation and Preventative Maintenance
3. Continuous Proactive Monitoring
4. Alert Ranking and Management
5. Threat Response
6. Recovery and Remediation
7. Log Management
8. Root Cause Investigation
9. Security Refinement and Improvement
10. Compliance Management

Personas

- SOC manager
- Incident responders
- Analysts (levels 1, 2 and 3)
- Threat hunters
- Incident response manager(s).

El SOC reporta al CISO, quien a su vez reporta al CIO o al director del CEO.

Grupos y Centros

De seguridad

SOC

URLs

1. https://www.**oracle**.com/es/database/security/que-es-un-soc.html
2. https://www.**ibm**.com/topics/security-operations-center.
3. https://latam.**kaspersky**.com/enterprise-security/security-operations-center-soc
4. …

Servicios en la Nube

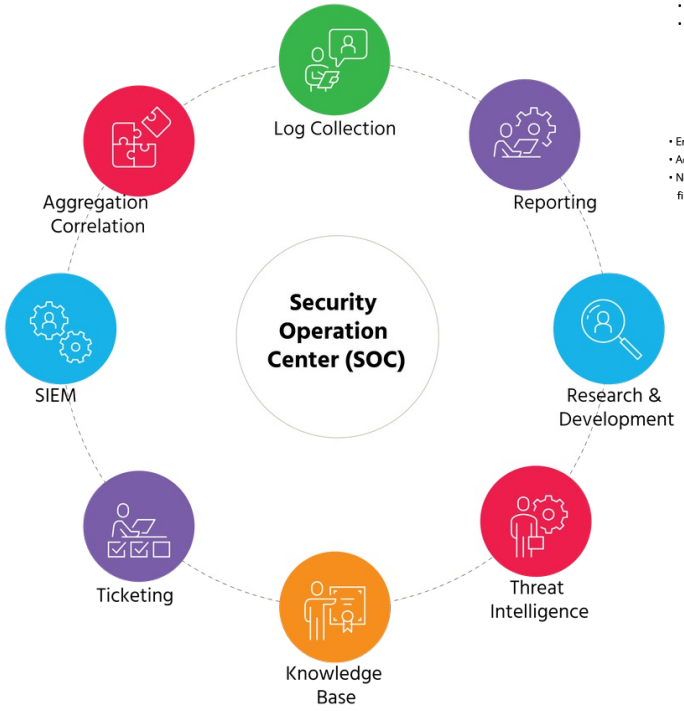
SOC-as-a-service

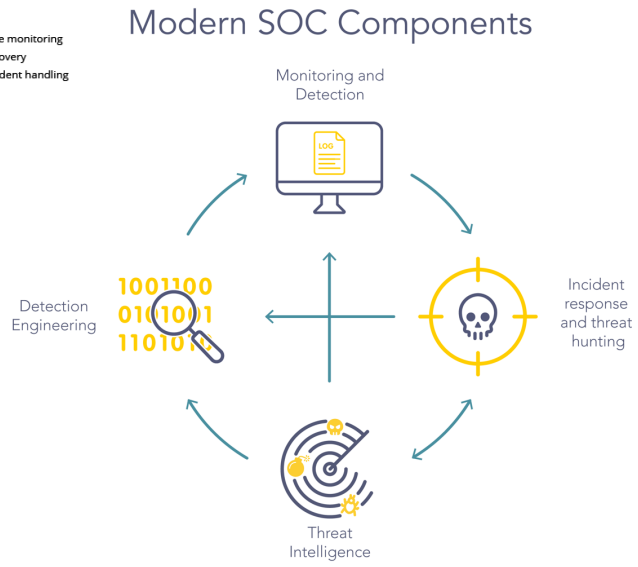
Grupos y Centros

De seguridad

SOC

C4 (Comando, Control, Comunicación y Cómputo
C4 municipal, C5 estatal





Grupos y Centros

De seguridad

NOC

Network Operations Center, en español Centro de Operaciones de Red

- Diferencias entre NOC y SOC.
  - SOC se enfoca en la seguridad de la información y los datos. Es de tipo Estratégico en el negocio.
  - NOC se enfoca en el monitoreo de la red de la empresa. Es de tipo Operativo.
- Dependiendo del Negocio de la empresa y su tamaño, pueden tenerse los 2 o solo el SOC.

Grupos y Centros

De seguridad

CERT
Para gobiernos, marca registrada en EU
CSIRT
Usado en Europa y sector no gov

CSIRT (por sus siglas en inglés)

Computer Security Incident Response Team

- En español ERIC
  - Equipo de Respuesta ante Incidentes Cibernéticos
- Referencias

  Hay muchas pero una Buena y reciente:
  - GUÍA PRÁCTICA PARA CSIRTs,CVolumen 2, 2023 Un modelo de negocio sustentable. PDF publicado por la OEA gratuito.
- CERT (*Computer Emergency Response Team*)
  - It is a group of information security experts responsible for the protection against, detection of and response to an organization's cybersecurity incidents.
  - The two terms are often used synonymously but are technically distinct: CERT is a trademarked term and associated more with partnership on threat intelligence, while a CSIRT has more of an association with a cross-functional business team.

Cibersecurity Laboratory

Actividades

Some of the most common are:

- Vulnerability analysis
- Malware and exploit analysis
- Security product development
- Reverse engineer a security threat
- Custom research

CERT

vs

CSIRT

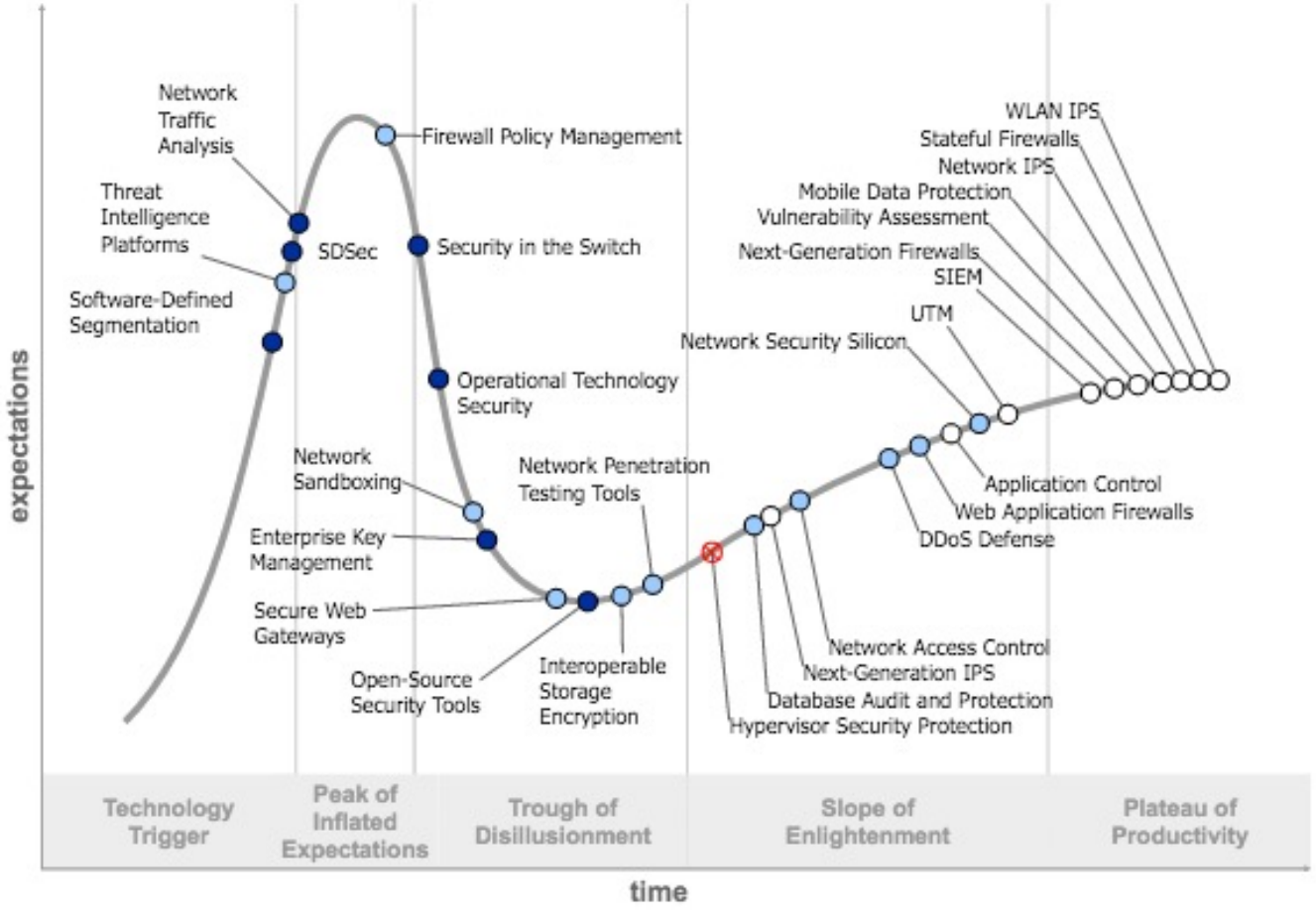
Several topics

Tópicos avanzados

Gartner

Gartner

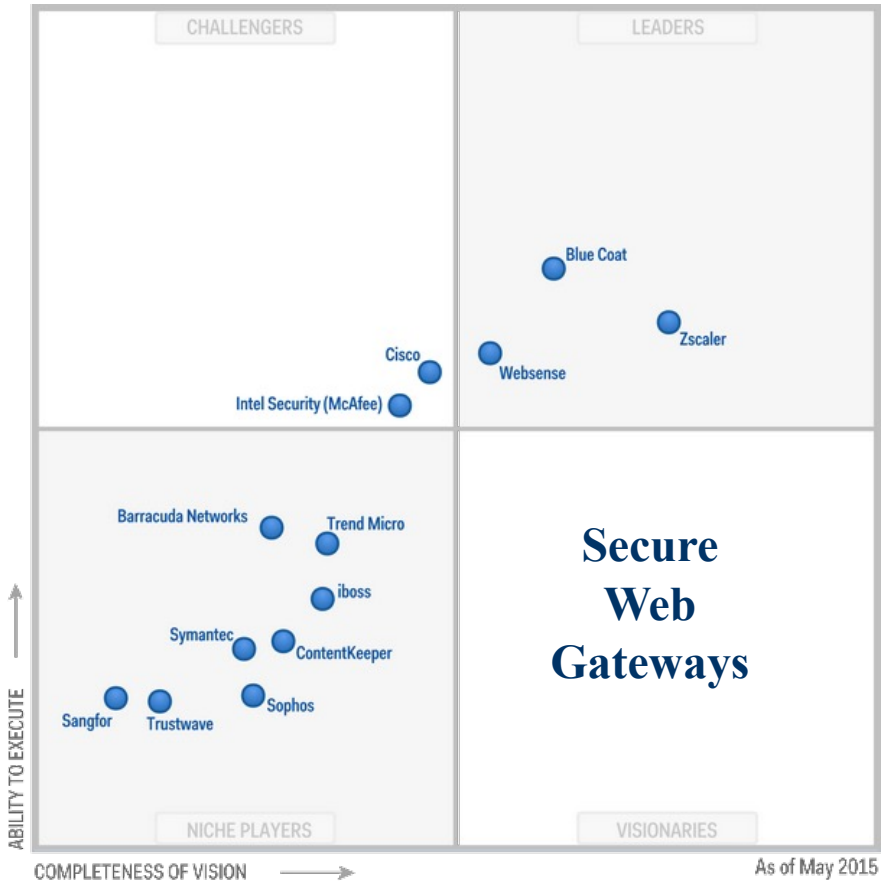
Hype Cycle

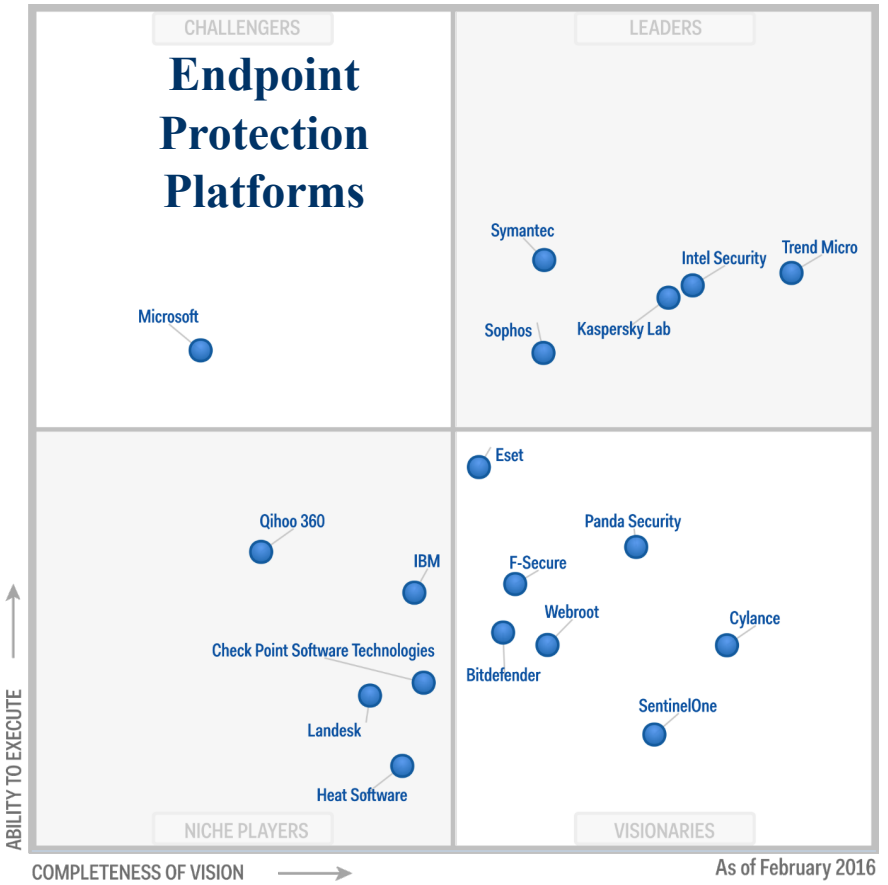


Infrastructure Protection 2015

Gartner

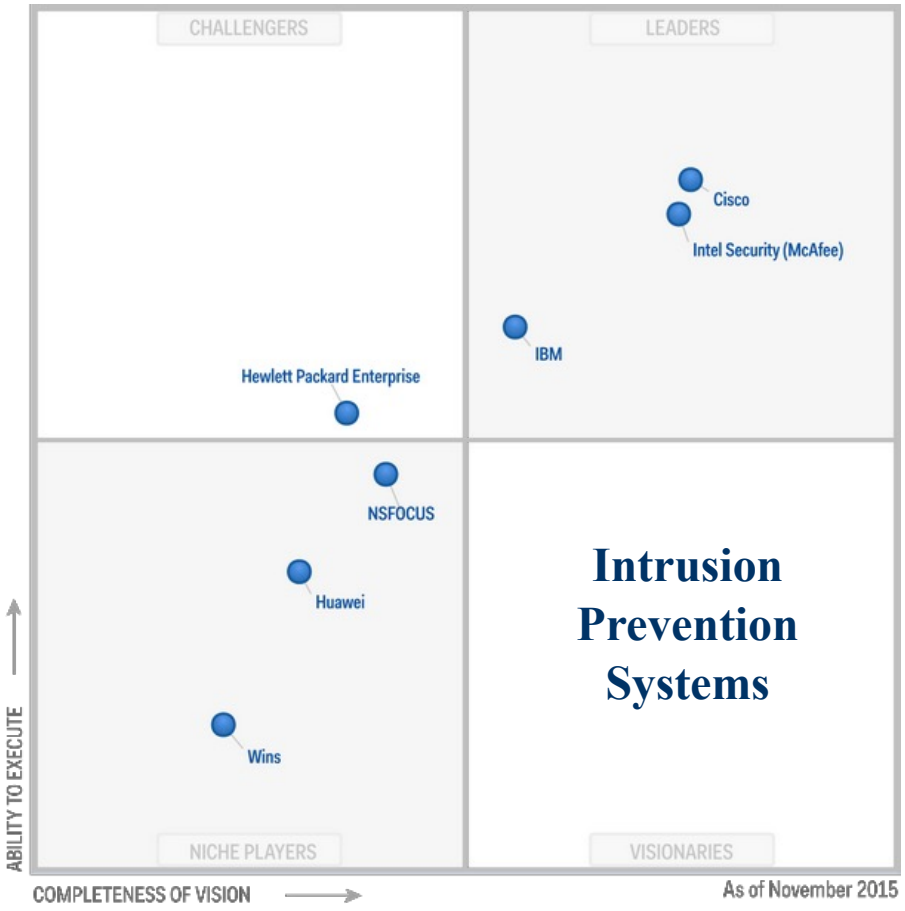
Magic Quadrant

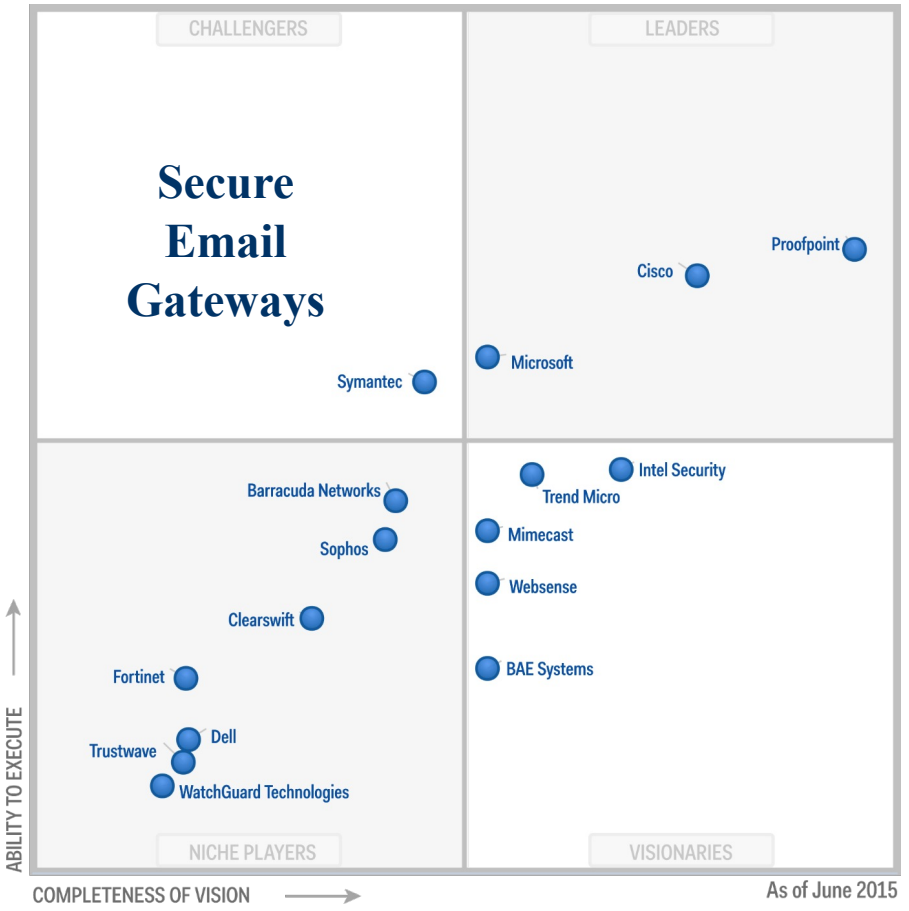




Gartner

Magic Quadrant





Bibliography

Links

- Common Vulnerabilities and Exposures
  - http://cve.mitre.org/
- Exploit
  - https://www.exploit-db.com.
- Microsoft
  - https://technet.microsoft.com/en-us/library/security/dn610807.aspx
- Vars
  - https://samate.nist.gov/SARD/
  - https://security.web.cern.ch/security/home/en/index.shtml
  - http://linuxtesting.org/

Software

Más ejemplos

- PaX
- kGuarda

  https://www.cs.columbia.edu/~vpk/research/kguard/
- http://sectools.org/
- http://insecure.org//

Bibliography

Papers

- eXclusive Page Frame Ownership (XPFO).
- StackGuard
  - https://www.usenix.org/legacy/publications/library/proceedings/sec98/full_papers/cowan/cowan.pdf

Conferences

Sobre malware

- Botconf
  - https://www.botconf.eu/
- Blackhat
- DepeSec
- Malware
  - http://www.malwareconference.org/

The end

Contacto

Raúl Acosta Bermejo

http:www.cic.ipn.mx
http://www.ciseg.cic.ipn.mx/

racostab@ipn.mx
racosta@cic.ipn.mx

57-29-60-00
Ext. 56652