

Joan Figueras Tugas

@JoanFiguerasT

Ciberseguretat Industrial

Riscos i amenaces dels sistemes hiperconnectats

ACPJ 
Associació Catalana
de Pèrits Judicials Tecnològics

 Centro de
Ciberseguridad Industrial

Enginyers
Industrials de Catalunya

Convergència IT/OT

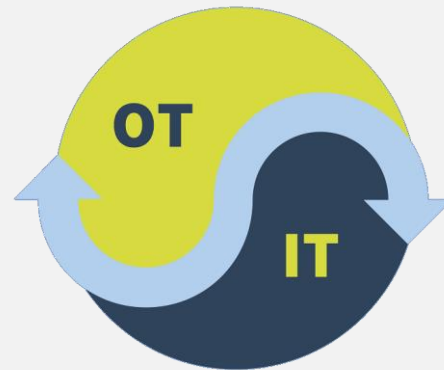


IT (Tecnologies de la Informació)

- Sistemes de hardware, software i comunicacions que donen suport a la gestió d'una companyia i els seus processos de negoci.
 - Es basen en la capacitat de compartir dades i informació

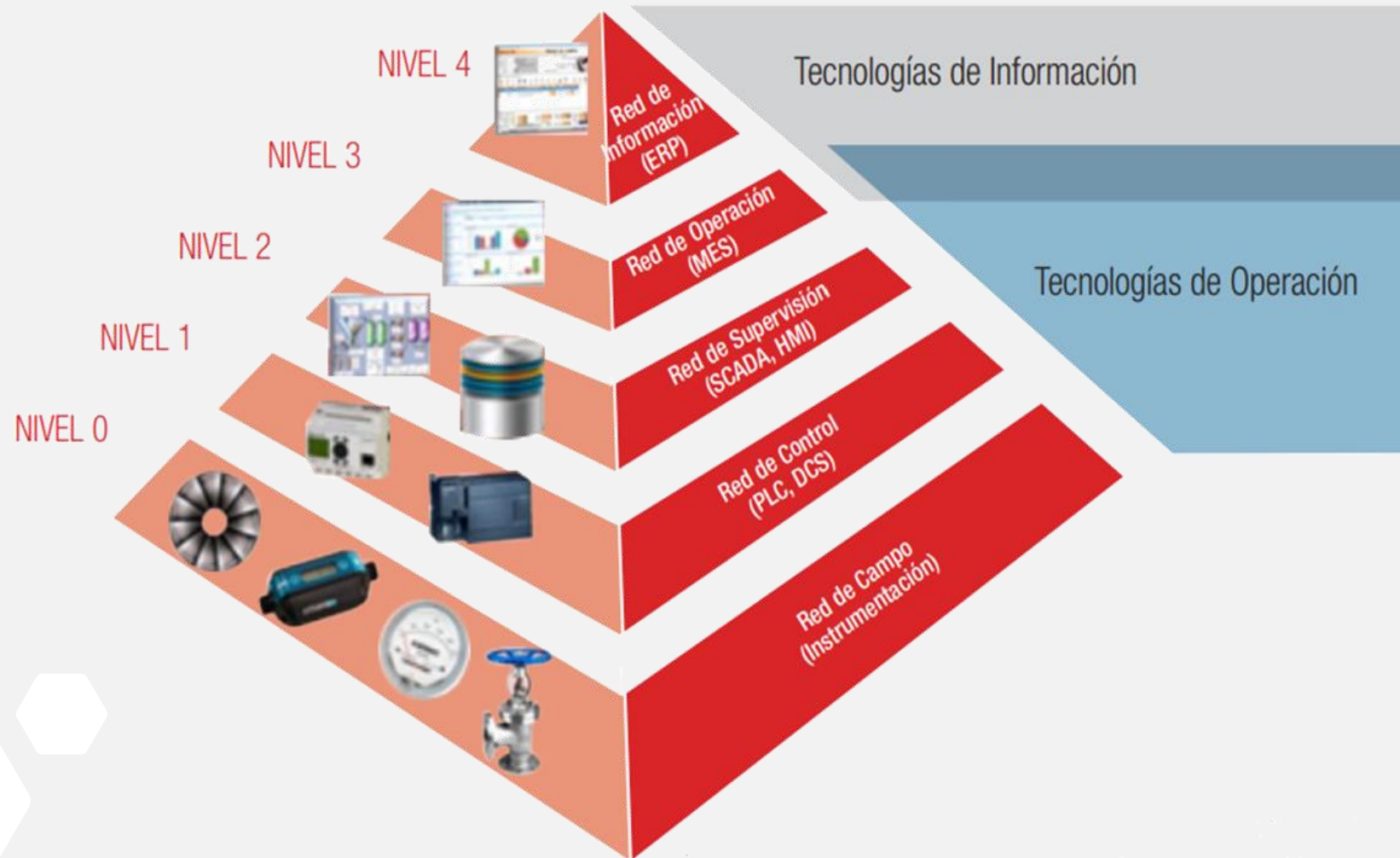
OT (Tecnologies de la Operació)

- Dispositius i automatismes que operen en una planta, així com els dispositius i software que monitoritzen i controlen els processos industrials.
 - Habitualment es tracta de sistemes crítics que requereixen una disponibilitat 24/7.



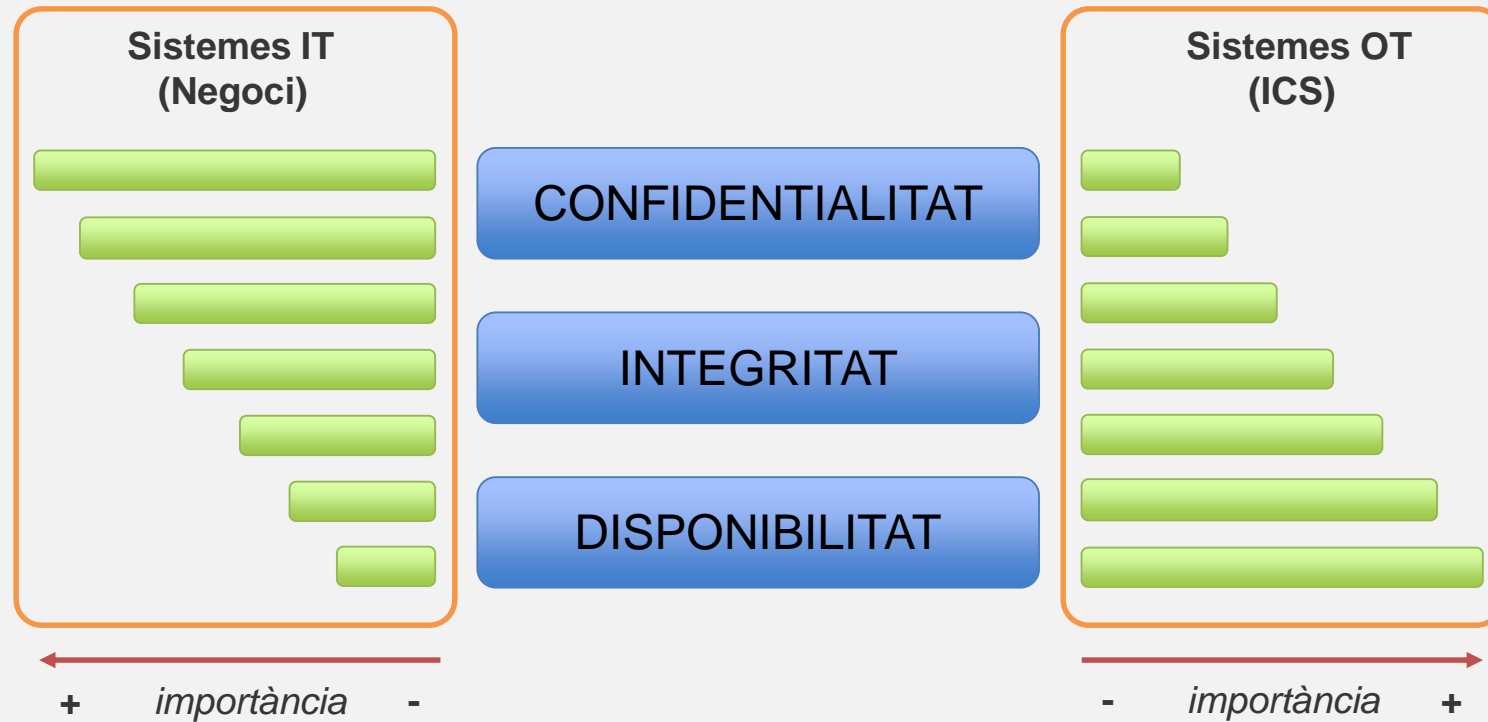
Convergència IT/OT

La piràmide de l'automatització industrial



Convergència IT/OT

Principis de seguretat



Convergència IT/OT

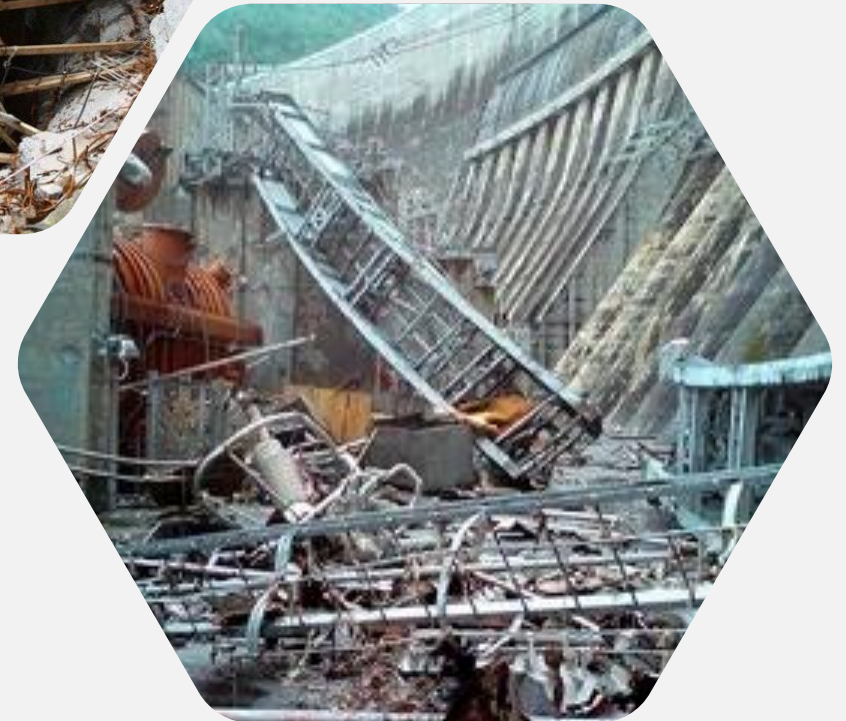
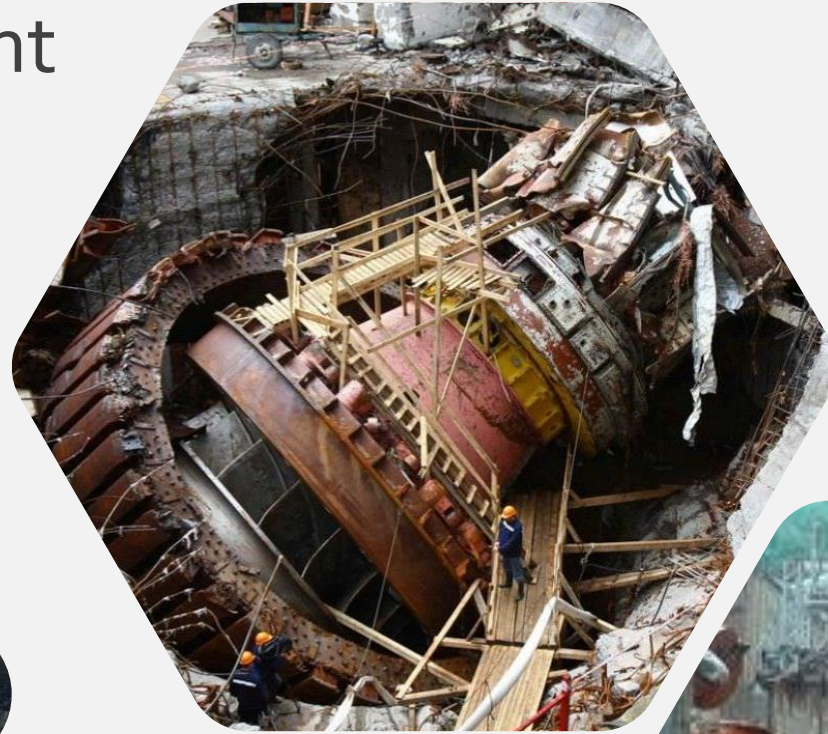
IT

- Àrea d'empresa: configuració de xarxes, equips d'oficina i software de gestió de dades.
- Prioritza la seguretat de la informació.
- Número d'actius similar al d'usuaris, i en entorns controlats.
- Vida útil dels equips informàtics: de 3 a 5 anys.
- Centrat en “*security*” (protecció de la informació)

OT

- Àrea de producció: manteniment de maquinària industrial.
- Prioritza que no s'aturin els processos industrials.
- Molts més dispositius que usuaris, distribuïts en àrees extenses.
- Vida útil dels equipaments industrials: entre 10 i 20 anys, o més.
- Centrat en “*safety*” (protecció del medi ambient, persones i infraestructures)

Conseqüències d'un incident



Central Hidroelèctrica Sayano–Shushenskaya (Rússia)

https://en.wikipedia.org/wiki/2009_Sayano-Shushenskaya_power_station_accident

Debilitats en entorns OT



The screenshot shows the top navigation bar of the InfoSecurity Magazine website with links for MAGAZINE, EVENTS, LEADERS NETWORK, and INSIGHT. Below the navigation is a dark header with the 'info security' logo and social media icons for Facebook, Twitter, Google+, and LinkedIn. The main article header features the date '9 JUN 2017', the category 'NEWS', and the title 'Half of ICS Firms Suffered Security Incident Last Year'. The article text discusses a survey by Kaspersky Lab showing that 50% of global ICS firms suffered security incidents in the past year, despite 83% claiming to be well-prepared. It also notes that 74% expect a cyber-attack and 55% believe third parties can access their networks. The biggest concern is conventional malware (56%), and half of firms struggle to hire security professionals.

infosecurity GROUP

MAGAZINE EVENTS LEADERS NETWORK INSIGHT

info security STRATEGY | INSIGHT | TECHNOLOGY

Sign Up Log In

f t g+ in

INFOSECURITY MAGAZINE HOME » NEWS » HALF OF ICS FIRMS SUFFERED SECURITY INCIDENT LAST YEAR

9 JUN 2017 NEWS

Half of ICS Firms Suffered Security Incident Last Year

Half of global companies that run industrial control systems (ICS) suffered between one and five security incidents in the past year despite the vast majority (83%) claiming to be well prepared to face down attacks, according to Kaspersky Lab.

The AV vendor polled over 350 industrial organizations around the world and found ineffective cybersecurity costs them up to \$497,000 (£383,000) per year.

Despite confidence in their ability to deal with incidents, 74% said they thought a cyber-attack will happen and over half (55%) admitted that third parties can access their industrial control network.

The biggest security concern for most of the organisations surveyed was conventional malware (56%) rather than advanced targeted attacks or ransomware.

Security challenges are compounded by the fact that half of industrial organizations can't hire the right security professionals.

Debilitats en entorns OT

- Xarxes extenses.
- Múltiples protocols.
- Dificultat d'aplicar actualitzacions de seguretat.
- Vida útil dilatada.
- Prioritzen la continuïtat a la seguretat.
- Amenaces emergents.
- Dependència dels proveïdors de sistemes ICS.
- Personal no preparat en ciberseguridad.



Debilitats en entorns OT

- Xa
- M
- D
- S
- V
- P
- A
- D
- S
- P

18°C L/RAIN
TOKYO (7 a.m.)
MARKETS 110.21 ¥/\$ (5 p.m.)

the japan times

NEWS

購読の申し込み SUBSCRIBE

SIGN UP | LOGIN >>

EMAIL UPDATES

TODAY'S STORIES



48,000 PCs at Fukushima plant operator TEPCO still run Windows XP

The Tokyo Electric Power Company (TEPCO) has been under intense scrutiny ever since the 2011 meltdown at the Fukushima Daiichi nuclear energy complex.

Following an investigation by Japan's Board of Audit, TEPCO has been told to upgrade its computer systems. That doesn't sound particularly unusual, except that TEPCO operates more than 48,000 PCs all running Windows XP. Oh, and they're connected to the Internet.



Debilitats en entorns OT

- Xarxes extenses.
- Múltiples protocols.
- Dificultat d'aplicar actualitzacions de seguretat.
- Vida útil dilatada.
- Prioritzen la continuïtat a la seguretat.
- Amenaces emergents.
- Dependència dels proveïdors de sistemes ICS.
- Personal no preparat en ciberseguridad.



Incidents en sistemes ICS

Atac	Any	Descripció	Vector	Consequències
Oleoducte BTC (Bakú-Tbilisi-Ceyhan)	2009	Accés al sistema de control de l'oleoducte per anular les alarmes de les estacions de bombeig	Accés físic al sistema	Aturada temporal de les operacions
Stuxnet	2010	Malware dissenyat per controlar els PLC de les centrifugadores d'urani enriquit de la central nuclear de Natanz (Iran)	Pendrive USB infectat	Aturada total del sistema
Telvent Canada	2012	Vulnerabilitat en el software d'un proveïdor d'eines de control remot de sistemes SCADA (SCADA Admin Tools)	Malware	Robatori d'informació
DragonFly	2014	Ciberespionatge a través de falses actualitzacions de software de proveïdors de sistemes ICS del sector elèctric	Injecció SQL	Sabotatge
Planta siderúrgica alemana	2015	Desconnexió dels HMI i manipulació del sistema de seguretat ICS de uns alts forns	Phishing	Danys físics a les instal·lacions
BlackEnergy (& KillDisk)	2016	Desconnexió de més de 30 subestacions de la xarxa elèctrica de Ucraïna	Phishing	Interrupció del subministrament d'energia
Planta Depuradora KWC	2016	Accés al sistema de control dels nivells de productes químics per al tractament de l'aigua	Web Server Exploit	Contaminació d'aigua potable i interrupció temporal del servei
WannaCry (*)	2017	Ransomware que va afectar a diverses companyies industrials	Exploit	Aturada de la cadena de producció
Triton / Trisis	2017	Malware que aprofita una vulnerabilitat en els sistemes Triconex SIS	Pendrive USB infectat	Aturada de la cadena de producció

Debilitats en entorns OT



BUSINESS
INSIDER

FINANCE

Renault-Nissan is resuming production after a global cyberattack caused stoppages at 5 plants



Laurence Frost and Naomi Tajitsu, Reuters

May 15, 2017, 1:25 PM 1,269



Renault-Nissan said on Monday that output had returned to normal at nearly all its plants, after a global cyber attack caused widespread disruption **including stoppages** at several of the auto alliance's sites.

Renault and its Japanese partner are the only major car manufacturers so far to have reported production problems resulting from Friday's WannaCry ransomware worm attack that spread to more than 150 countries.



Vulnerabilitats en Sistemes ICS

<https://ics-cert.us-cert.gov/advisories>

Official website of the Department of Homeland Security



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM



- [ICSA-18-263-02](#) : Rockwell Automation RSLinx Classic
- [ICSA-18-261-01](#) : WECON PLC Editor
- [ICSA-18-256-01](#) : Honeywell Mobile Computers with Android Operating Systems
- [ICSA-18-254-01](#) : Fuji Electric V-Server
- [ICSA-18-254-02](#) : Fuji Electric V-Server Lite
- [ICSA-18-254-03](#) : Siemens TD Keypad Designer
- [ICSA-18-254-04](#) : Siemens SIMATIC WinCC OA
- [ICSA-18-254-05](#) : Siemens SCALANCE X Switches
- [ICSA-18-249-01](#) : Ice Qube Thermal Management Center
- [ICSA-18-247-01](#) : Opto 22 PAC Control Basic and PAC Control Professional
- [ICSA-18-242-01](#) : Philips e-Alert Unit
- [ICSMA-18-240-01](#) : Qualcomm Life Capsule
- [ICSA-18-240-01](#) : Schneider Electric Modicon M221
- [ICSA-18-240-02](#) : Schneider Electric Modicon M221
- [ICSA-18-240-03](#) : Schneider Electric PowerLogic PM5560
- [ICSA-18-240-04](#) : ABB eSOMS (Update A)



Vulnerabilitats en Sistemes ICS

<https://ics-cert.us-cert.gov/advisories>

Official website of the Department of Homeland Security



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM



- ICSA-18-263-02 : **Rockwell Automation** RSLinx Classic
- ICSA-18-261-01 : WECON PLC Editor
- ICSA-18-256-01 : **Honeywell** Mobile Computers with Android Operating Systems
- ICSA-18-254-01 : Fuji Electric V-Server
- ICSA-18-254-02 : Fuji Electric V-Server Lite
- ICSA-18-254-03 : Siemens TD Keypad Designer
- ICSA-18-254-04 : **Siemens SIMATIC** WinCC OA
- ICSA-18-254-05 : Siemens SCALANCE X Switches
- ICSA-18-249-01 : Ice Qube Thermal Management Center
- ICSA-18-247-01 : Opto 22 PAC Control Basic and PAC Control Professional
- ICSA-18-242-01 : Philips e-Alert Unit
- ICSMA-18-240-01 : Qualcomm Life Capsule
- ICSA-18-240-01 : **Schneider Electric** Modicon M221
- ICSA-18-240-02 : Schneider Electric Modicon M221
- ICSA-18-240-03 : Schneider Electric PowerLogic PM5560
- ICSA-18-240-04 : **ABB** eSOMS (Update A)



Vulnerabilitats en Sistemes ICS

Advisory (ICSA-18-317-06)

Siemens SIMATIC STEP 7 (TIA Portal)

Original release date: November 13, 2018



[More Advisories](#)

1. EXECUTIVE SUMMARY

- **CVSS v3 4.0**
- **ATTENTION:** Low skill level to exploit
- **Vendor:** Siemens
- **Equipment:** SIMATIC STEP 7 (TIA Portal)
- **Vulnerability:** Unprotected Storage of Credentials

2. RISK EVALUATION

Successful exploitation of this vulnerability could allow an attacker to reconstruct passwords.

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

Siemens reports the following SIMATIC STEP 7 product is affected:

- SIMATIC STEP 7 (TIA Portal): All versions prior to 15.1

3.2 VULNERABILITY OVERVIEW

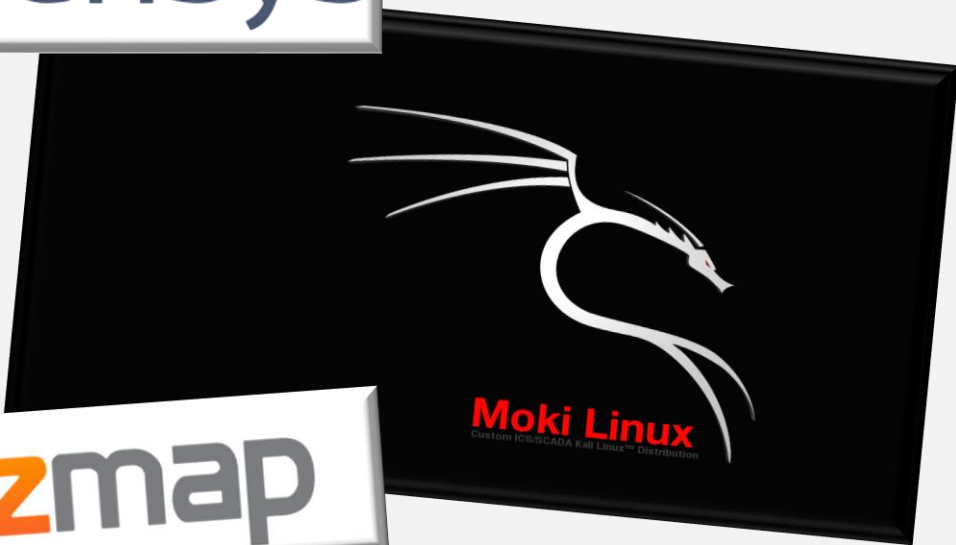
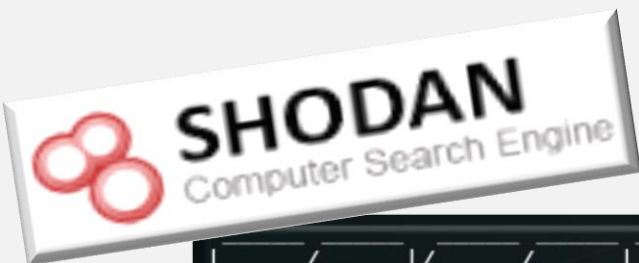
3.2.1 UNPROTECTED STORAGE OF CREDENTIALS CWE-256

Password hashes with insufficient computational effort could allow an attacker to access to a project file and reconstruct passwords. This vulnerability could allow the attacker to obtain certain passwords from the project.

CVE-2018-13811 has been assigned to this vulnerability. A CVSS v3 base score of 4.0 has been calculated; the CVSS vector string is (AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).



Explotació de vulnerabilitats



Explotació de vulnerabilitats

Shodan Developers Book View All...


SHODAN SIMATIC

Explore Downloads Reports Pricing Contact Us

Exploits Maps Share Search Download Results Create Report

TOTAL RESULTS
2,170

TOP COUNTRIES



United States	281
Italy	266
Germany	210
Spain	171
Japan	117

TOP SERVICES

SNMP	1,143
Siemens S7	851
Modbus	156
PPTP	6
NetBIOS	4

TOP ORGANIZATIONS

Emirates Integrated Telecommunications Com...	110
Deutsche Telekom AG	107
University of Maryland	98
NTT	63
Vodafone Italy ask to use the space unassigne...	35

TOP OPERATING SYSTEMS

Linux 3.x	1
-----------	---

TOP PRODUCTS

Conpot	310
Microsoft SQL Server	1
Microsoft ESMTTP	1
Apache httpd	1

115.163
Vodafone Spain
Added on 2018-11-28 00:18:53 GMT
Spain, Miño
Details
Siemens, SIMATIC HMI, XP277, 6AV6 643-0CD01-1AX0, HW: 0, SW: V 1 1 4

108.6
mobile-168-130-108-0.mycingular.net
AT&T Wireless
Added on 2018-11-28 00:18:02 GMT
United States, Atlanta
Details
Siemens, SIMATIC S7, CPU-1200, 6ES7 214-1HG40-0XB0, HW: 5, FW: V.4.2.1, S C-J7MT0030

101.222
p408222-
ipngn200103okayamahigasi.okayama.ocn.ne.jp
NTT
Added on 2018-11-28 00:04:50 GMT
Japan, Okayama
Details
honeypot
Location designation of a module:
Copyright: Original Siemens Equipment
Module type: IM151-8 PN/DP CPU
PLC name: Technodrome
Module: v.0.0
Plant identification: Mouser Factory
OEM ID of a module:
Module name: Siemens, SIMATIC, S7-200
Serial number of module: 88111222

58.18
18.88.43.5.rev.vodafone.pt
Vodafone Portugal - Comunicacoes Pessoais S.A.
Added on 2018-11-28 00:04:13 GMT
Portugal
Details
Siemens, SIMATIC NET, SCALANCE M874-3, 6GKS 874-3AA00-2AA2, HW: Version 3, FW: Version V04.01.00, SVPHD143291

25.13
Turkcell
Added on 2018-11-27 23:46:28 GMT
Turkey
Details
Siemens, SIMATIC S7, CPU-1200, 6ES7 212-1HE40-0XB0, HW: 4, FW: V.4.1.3, S C-FNS29436

2.159.169
pd95c9fa9.dip0.t-ipconnect.de
Deutsche Telekom Business
Added on 2018-11-27 23:42:19 GMT
Germany, Berlin
Details
Siemens, SIMATIC NET, SCALANCE M816-1B, 6GKS 816-1BA00-2AA2, HW: Version 3, FW: Version V04.02.00, SVPE3153157

Protecció, defensa i prevenció



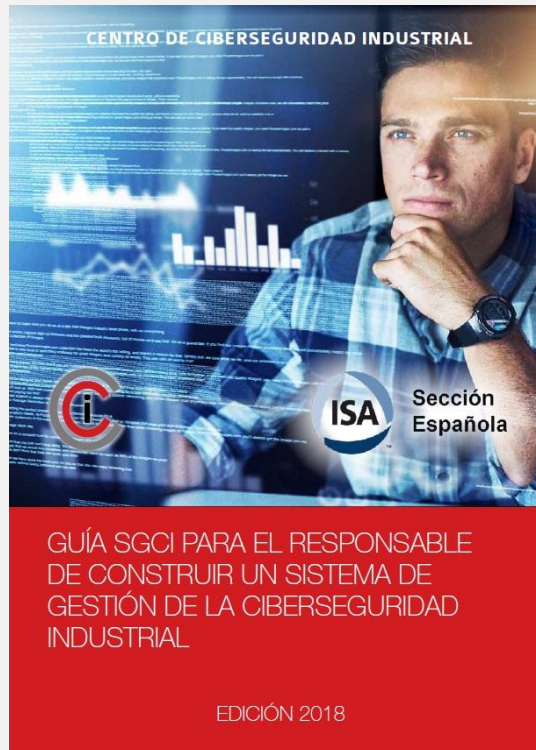
- Mesures de seguretat específiques per a entorns ICS.
- Enfocament de Defensa en profunditat.
- Stàndards / Marcs de referència:
 - IEC 62443
 - NIST SP 800-82
- Recursos:
 - ICS-CERT
 - NERC-CIP
 - INCIBE-CERT

Protecció, defensa i prevenció




- Mesures de seguretat específiques per a entorns ICS.
- Enfocament de Defensa en profunditat.
- Stàndards / Marcs de referència:
 - IEC 62443
 - NIST SP 800-82
- Recursos:
 - ICS-CERT
 - NERC-CIP
 - INCIBE-CERT


Protecció, defensa i prevenció



<https://www.cci-es.org>

Gràcies!

 Joan Figueras Tugas | ACPJT | CCI
Ciberseguretat i Protecció de la Informació

 joan.figueras@es.cci-es.org

 <https://www.linkedin.com/in/joanfiguerastugas/>