



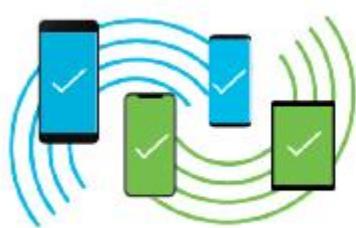
CONATEL C

Cyberseguridad, Redes Industriales y la nueva normalidad

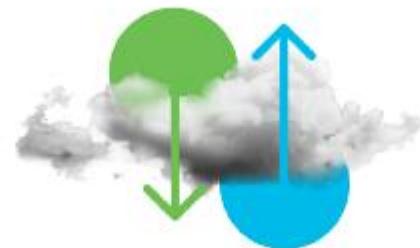
Gerardo Viar - CONATEL – Nov 2020

2020 Cambió Todo ...

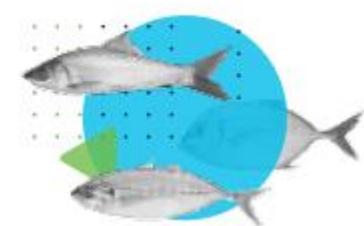
La forma en la que trabajamos está cambiando



Dispositivos Ilimitados



Servicios Cloud



Fuerza de Trabajo Distribuida

Realidad de Riesgos en la Actualidad

Más interconectados que nunca

Mayor superficie de ataque

Operación Continua

Se debe mantener el negocio corriendo

Trabajadores se conectan desde cualquier lado

Pérdida de control



Realidad Multi-cloud

Un mundo “software-defined”

Amenazas sofisticadas y automatizadas

Alta probabilidad de brechas

Panorama de ataques en constante evolución

Advanced Persistent Threats

Supply chain attacks

Unpatched Software

Spyware/Malware

Wiper Attacks

Phishing

Man in the Middle

DDoS

Cryptomining

Ransomware

Data/IP Theft

Malvertising

Drive by Downloads

Rogue Software

Botnets

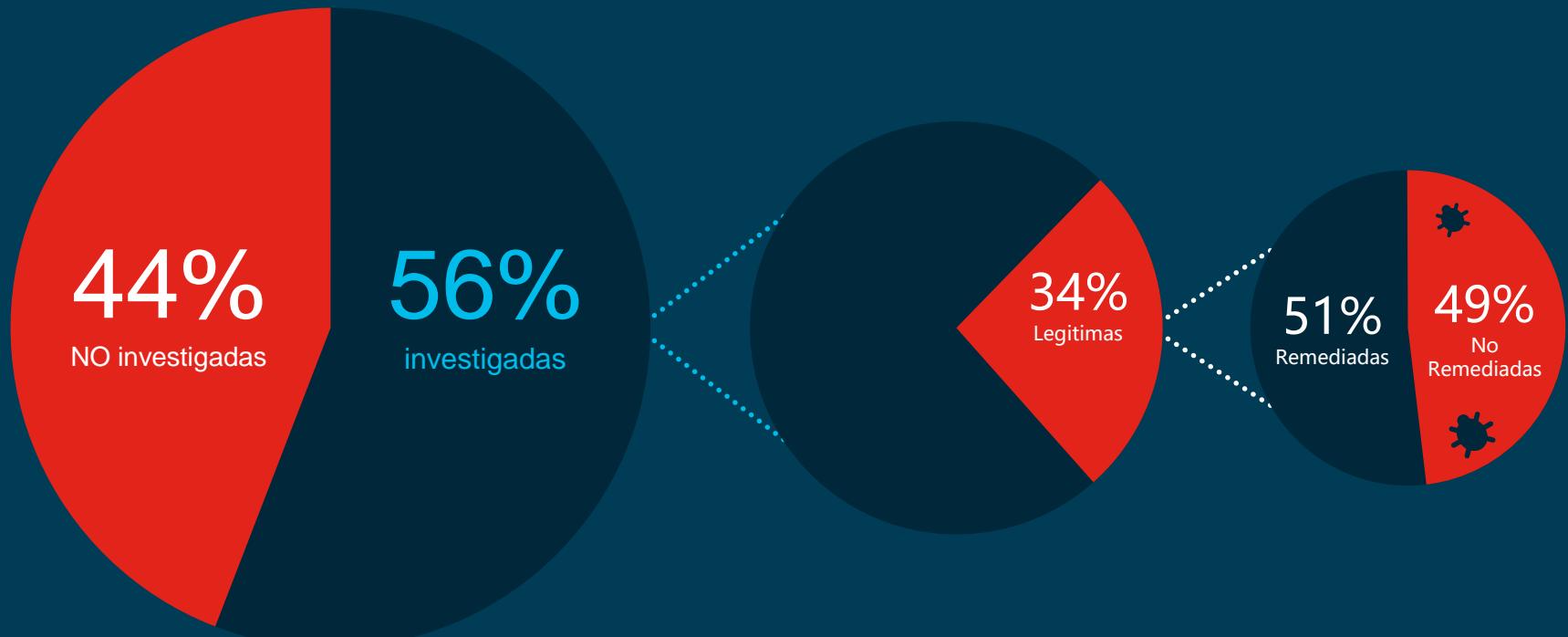
Credential compromise



Imposiblemente Complejo

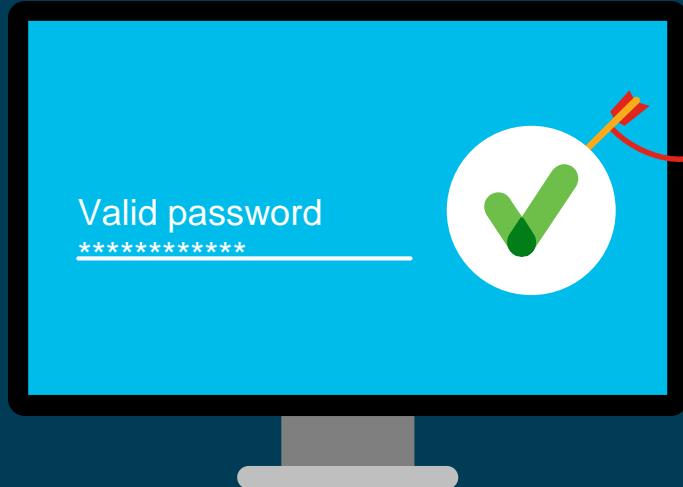


Demasiadas Alertas ...



Fuente: Cisco Annual CyberSecurity Report 2018

Muy poca confianza ...



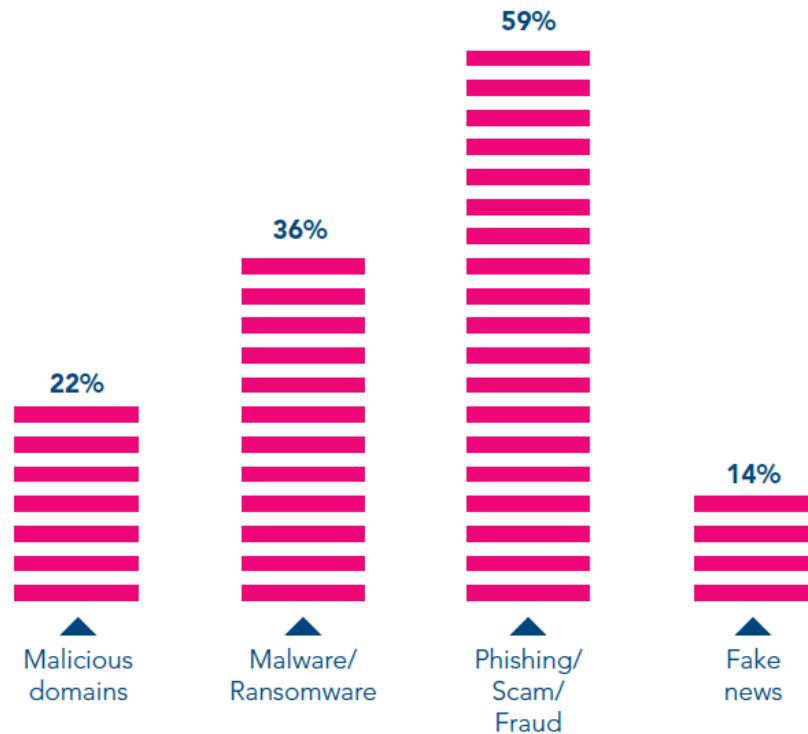
81%

De las brechas se
basan en **passwords**
robadas o débiles

...Cyber Fatiga



COVID-19: Impacto en Cyberseguridad



Hacia una Seguridad más Potenciada



Mejor defensa contra
malware and ransomware



Visibilidad y Control de
Quién entra en la Red



Mejorar la preparación y
respuesta para las Brechas



Mejor seguridad para el
borde de la red



Defender el Data Center
Moderno



Acelerar las Operaciones de
Seguridad

El mercado de Seguridad ...

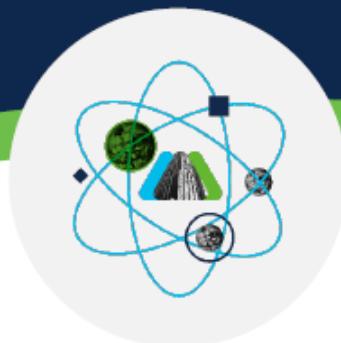


está cambiando

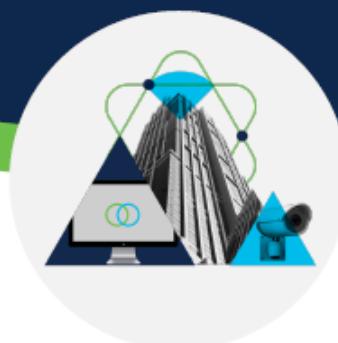
SASE

Zero Trust

XDR



Secure Access Service Edge



Zero Trust



Extended Detection & Response

T

Digitalización de la Industria vs. Superficie de Ataque



Desafíos de Cyberseguridad en OT



Falta Skills

Cómo desarrollar las tareas de Cyberseguridad en OT con el staff de IT y OT existente?



Amenazas Crecientes

53% de las compañías industriales han sufrido cyber-ataques.
Estamos preparados?



Compliance

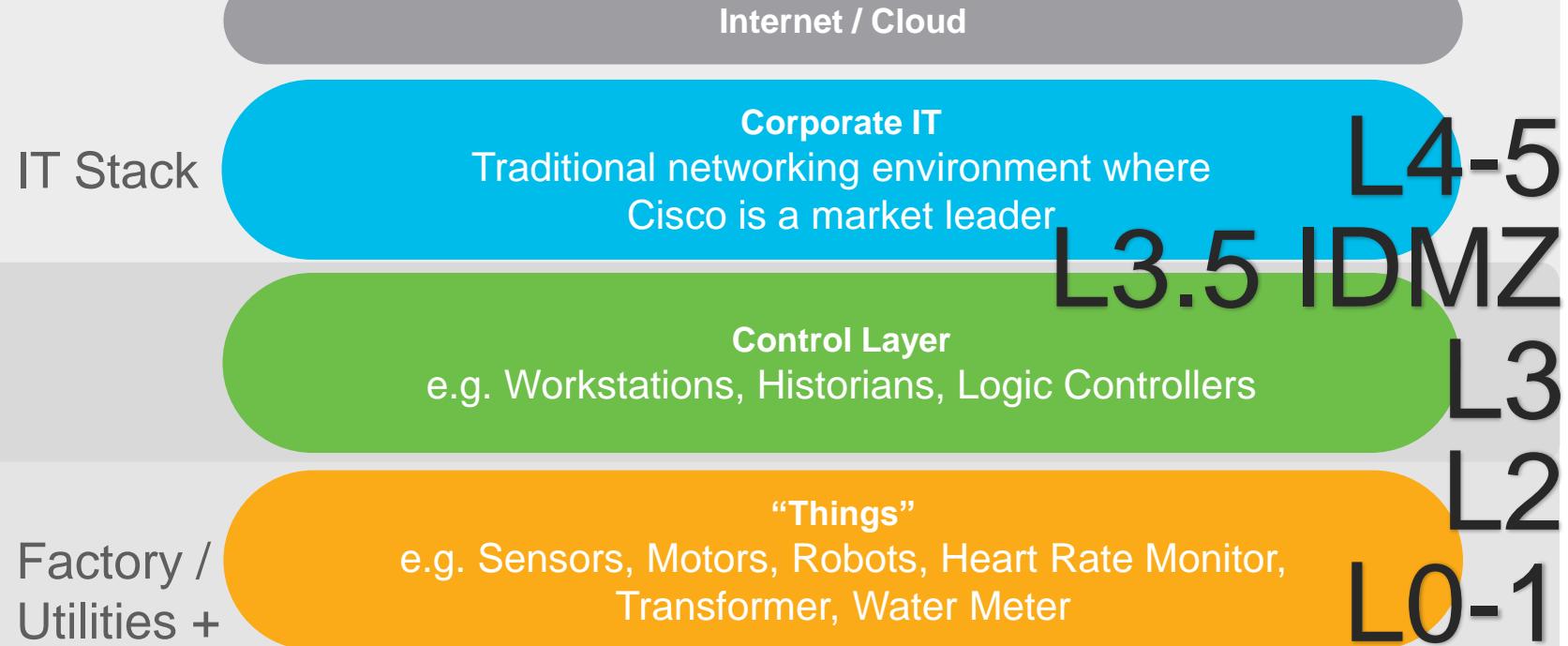
Restricciones regulatorias (NERC CIP, EU-NISIEC 104, IEC 101 over IP, DNP3, IEC 61850 (MMS, Goose), C31.118, DLMS / COSEM, Bacnet, Ethercat, OPC-DA, OPC-UA, OPC-EA...)



Agility

Convergencia segura de OT & IT que permita los beneficios de la digitalización de la Industria

Modelo de Purdue



Falta Visibilidad Dispositivos OT



Mayoría de las organizaciones
no tienen un **Inventario** de
activos preciso

55% tienen poca o ninguna confianza en que
conocen todos los dispositivos que tienen en
la red



Ciegos ante la **Comunicación**
entre elementos

Equipamiento de ICS desplegado durante
años sin una política estricta de seguridad

Pilares Cyber Seguridad en OT



ICS Visibility

Asset Inventory
Communication Patterns
Device Vulnerability



Operational Insights

Identify configuration changes
Record control system events
relevant to the integrity of the system



Threat Detection

Behavioral Anomaly Detection
Signature based IDS
Real-time alerting

Visibilidad

May 29, 2018 3:16:34 PM - Jun 20, 2019 4:16:34 PM (1y 22d 1h) • LIVE

66 Components

Component	Group	First activity	Last activity
Dell 192.168.105.241	Maintenance Station	Apr 6, 2017 10:59:14 PM	Jun 18, 2019 12:23: AM
149.178.42.70	Infrastructure 2	Oct 5, 2017 6:03:16 PM	Jun 18, 2019 12:23: AM
232.108.116.118	-	Apr 6, 2017 10:58:44 PM	Jun 18, 2019 12:23: AM
AMBRE	IT Machines - To Investigate	Apr 6, 2017 10:58:58 PM	Jun 18, 2019 12:23: AM
10.16.116.254	-	Apr 6, 2017 10:58:44 PM	Jun 18, 2019 12:23: AM
SIMATIC 300(1)	-	Apr 6, 2017 11:29:22 PM	Jun 18, 2019 12:23: AM
10.8.0.6	-	Apr 6, 2017 10:58:45 PM	Jun 18, 2019 12:23: AM
OWS1	Emerson Process	Apr 6, 2017 10:58:45 PM	Jun 18, 2019 12:23: AM
239.192.24.4	-	Oct 5, 2017 6:03:14 PM	Jun 18, 2019 12:23: AM
Hirschmann 192.168.1.254	Yokogawa CentumVP	Oct 5, 2017 6:03:14 PM	Jun 18, 2019 12:23:34 AM
Fisher 10.4.0.14	Emerson Process	Apr 6, 2017 10:58:44 PM	Jun 18, 2019 12:23:34 AM
WIOC-1F903A	Emerson Process	Apr 6, 2017 10:58:45 PM	Jun 18, 2019 12:23:34 AM
ff02::1:ffff:3b4b	-	Apr 6, 2017 10:59:14 PM	Jun 18, 2019 12:23:34 AM
IM151-3PN	Manuf IO	Apr 6, 2017 11:29:22 PM	Jun 18, 2019 12:23:34 AM

May 29, 2018 3:37:54 PM - Jun 20, 2019 4:37:54 PM (1y 22d 1h) • LIVE

The diagram illustrates a complex network topology with numerous nodes and connections. Key components include:

- Auto Robot**: Connected to Quality Check, Robot Control, and several sensor nodes.
- Quality Check**: A central node connected to Auto Robot, Robot Control, and other nodes.
- Robot Control**: Connected to Auto Robot and other nodes.
- Power Grid - ECO 104**, **Energy Management**, and **Yokogawa CentumVP**: Large clusters of nodes representing different system domains.
- Emerson Process**, **Infrastructure 2**, and **Manuf IO**: Groups of nodes representing specific industrial environments.
- Dell**, **HP**, and **Siemens**: Specific device models represented by nodes.
- Sensors**: Numerous small nodes scattered throughout the network, often represented by gear icons.

Connections are primarily represented by lines of varying colors, indicating different types of relationships or data flows between the nodes.

Conocimiento Operativo

- Detalle de activos
- Mapas de comunicaciones
- Cambios en PLCs
- Acceso a variables

Component

SIMATIC 300(1)
IP: 192.168.0.1
MAC: 00:0e:8c:84:5b:a6

Add to group Create group

First activity: Apr 6, 2017 11:29:22 PM
Last activity: May 26, 2019 12:21:13 AM

Read Var, PLC

24 Flows

51 Events

5 Vulnerabilities

13 Variables

Credential



Basics Security Activity Automation

Properties Tags

Properties

Vendor-Name:	Siemens AG A&D ET
Model-Name:	CPU 315-2 PN/DP
Fw-Version:	V 2.5.0
Hw-Version:	3
Model-Ref:	6ES7 315-2EH13-0AB0
Serial-Number:	S C-VIR583472007
Name:	SIMATIC 300(1)

Variables accesses 13

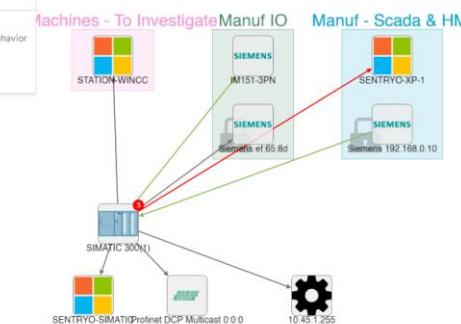
< 1 > 20 / page

Variable	Types	Accessed by	First access	Last access
> M2.0	READ	2 components (2 accesses)	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM
▼ M2.1	READ	2 components (2 accesses)	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM
	READ	Siemens 192.168.0.10	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM
	READ	SENTRYO-XP-1	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM
> M8.0	READ	2 components (2 accesses)	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM
> M8.1	READ	2 components (2 accesses)	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM
> M8.2	READ	2 components (2 accesses)	Apr 6, 2017 11:29:22 PM	May 26, 2019 12:21:23 AM

Minimap

Legend

- Important
- Control system behavior
- IT Behavior
- Network analysis
- Others



Identificación de Vulnerabilidades

Component

SIMATIC 300(1)
IP: 192.168.0.1
MAC: 00:0e:8c:84:5b:a6

Last activity: Apr 6, 2017 11:29:22 PM
Last activity: Jun 20, 2019 12:22:18 AM

Add to group Create group

Basics Security Activity Automation

Vulnerabilities Credentials

Vulnerabilities

- Multiple Siemens Products CVE-2017-12741 Denial of Service Vulnerability**
CVE-2017-12741
Several industrial products are affected by a vulnerability that could allow remote attackers to conduct a Denial-of-Service (DoS) attack.
Solution
Siemens has released updates for several affected products, and recommends that customers update to the new version. Siemens is preparing further updates and recommends specific countermeasures until patches are available.
Published on November 23, 2017
Identified on this component on April 6, 2017
Identified vulnerable because of model-ref (6E57 315-2EH13-0AB0)
Links
[Siemens Security Advisory](#)
- SIMATIC S7-300 and S7-400 CPUs Denial of Service and Information Disclosure Vulnerabilities**
CVE-2016-9158
Successful exploitation of these vulnerabilities could lead to a denial-of-service condition or result in credential disclosure.
Solution
Siemens provides firmware version V3.X.14 for S7-300 CPUs that resolves CVE-2016-9158.
Published on December 16, 2016
Identified on this component on April 6, 2017
Identified vulnerable because of model-ref (6E57 315-2EH13-0AB0)
Links
[www.siemens.com](#)
[ics-cert.us-cert.gov](#)
[www.securityfocus.com](#)
- Multiple Denial of Service Vulnerabilities on Siemens devices using the PROFINET Discovery and Configuration Protocol**

24 Flows 51 Events 5 Vulnerabilities 13 Variables

Explore / All Presets ▾

Jan 1, 2019 12:00:00 AM - Apr 29, 2019 5:04:00 PM (3m 27d 10h 4m) LIVE

234 Vulnerabilities

Top 10 vulns

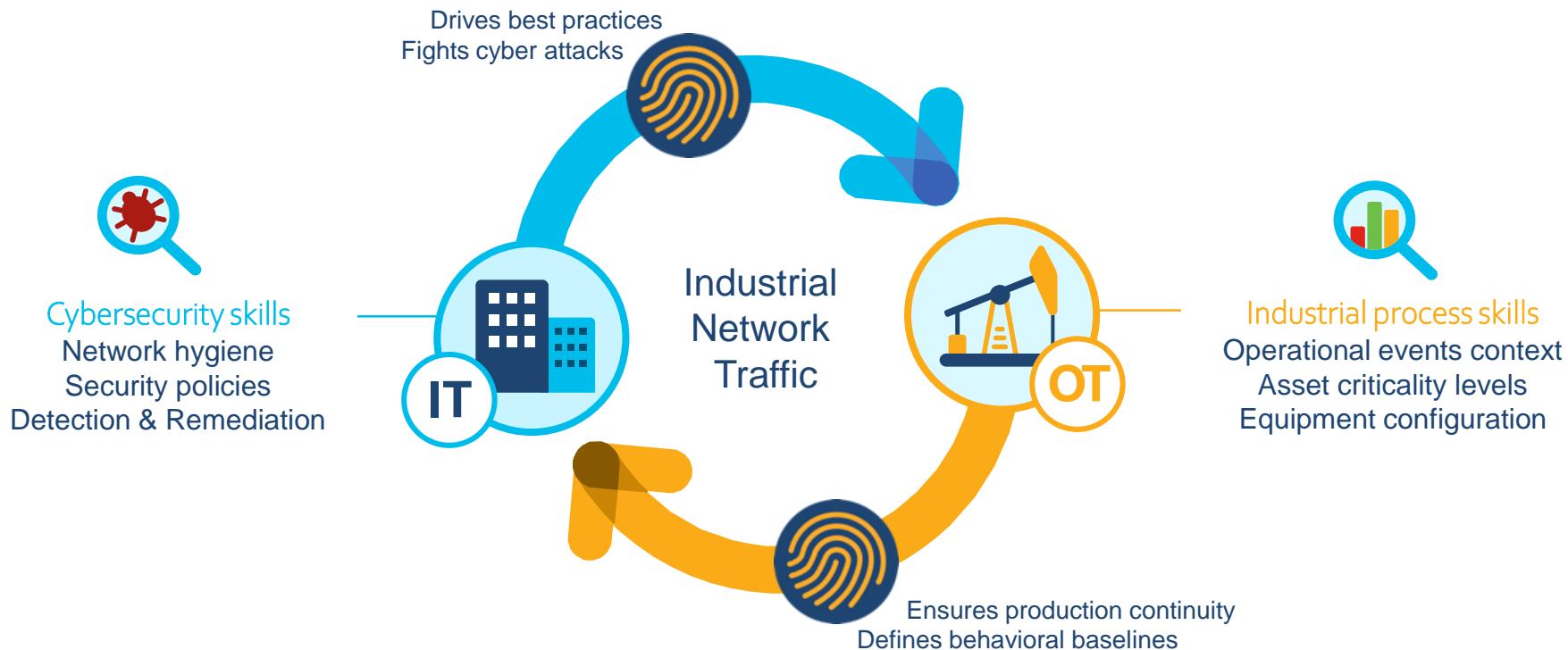
CATEGORY	NUMBER OF VULNS
Multiple Siemens Products	102
Multiple Denial of Service Vulnerabilities on Siemens devices using the PROFINET Discovery and Configuration Protocol	64
Web Vulnerability in S7-1200	58
Vulnerabilities in SIMATIC S7-1200 CPU 3	53
Web Vulnerability in SIMATIC S7-1200	49
Yokogawa CENTUM 'BKLogSvr.exe' Heap Based Buffer Overflow Vulnerability	34
Yokogawa Multiple Products Buffer Overflow Vulnerability	31
Yokogawa CENTUM 'BKESim.exe' Multiple Denial of Service Vulnerability	26
Yokogawa CENTUM and Exaopc Vulnerability	18
Yokogawa CENTUM BKFSim_vhfd.exe Buffer Overflow - Packet Storm	12

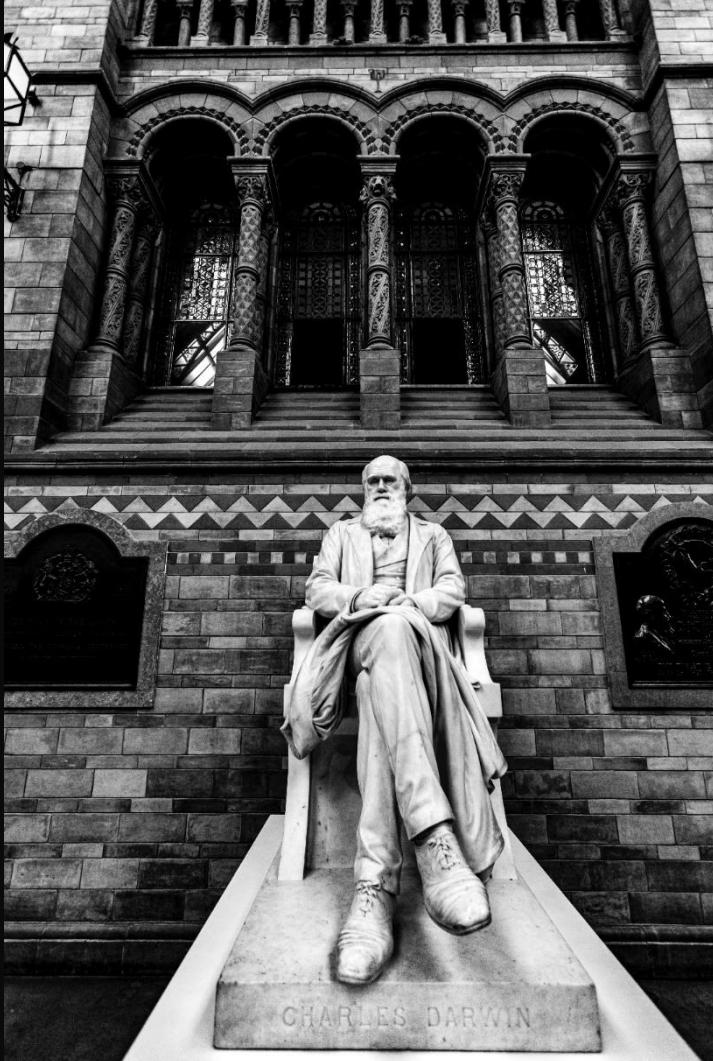
457 Total vulnerable components

Vulnerabilities name CVE Published in CVSS Affected components

Vulnerabilities name	CVE	Published in	CVSS	Affected components
Multiple Siemens Products CVE-2017-12741 Denial of Service Vulnerability	CVE-2017-12741	May, 20 2019	9.8	102 Affected components
Multiple Denial of Service Vulnerabilities on Siemens devices using the PROFINET Discovery and Configuration Protocol	CVE-2014-0781	Sept, 05 2019	9.1	64 Affected components
Web Vulnerability in S7-1200	CVE-2014-3888	Jan, 11 2019	8.8	58 Affected components
Yokogawa CENTUM 'BKLogSvr.exe' Heap Based Buffer Overflow Vulnerability	CVE-2015-5627	Nov, 02 2018	7.9	34 Affected components
Yokogawa CENTUM and Exaopc Vulnerability	CVE-2015-5626	Apr, 03 2018	6.3	18 Affected components
Web Vulnerability in SIMATIC S7-1200	CVE-2015-5628	May, 03 2018	5.6	22 Affected components
Yokogawa CENTUM BKFSim_vhfd.exe Buffer Overflow - Packet Storm	CVE-2014-0783	Feb, 28 2016	4.2	Rockwell 192.168.0.200
Yokogawa Multiple Products Buffer Overflow Vulnerabilities - CVE-2015-5626	CVE-2014-2200 - SSA-253230	Feb, 28 2016	3.5	12 Affected components

Colaboración IT-OT Vital para Seguridad en ICS





1º CONGRESO URUMAN

De la Dificultad a la Oportunidad
Confiabilidad Humana en el Mundo Digital

Gracias



CONATEL C

gviar@conatel.com.uy