



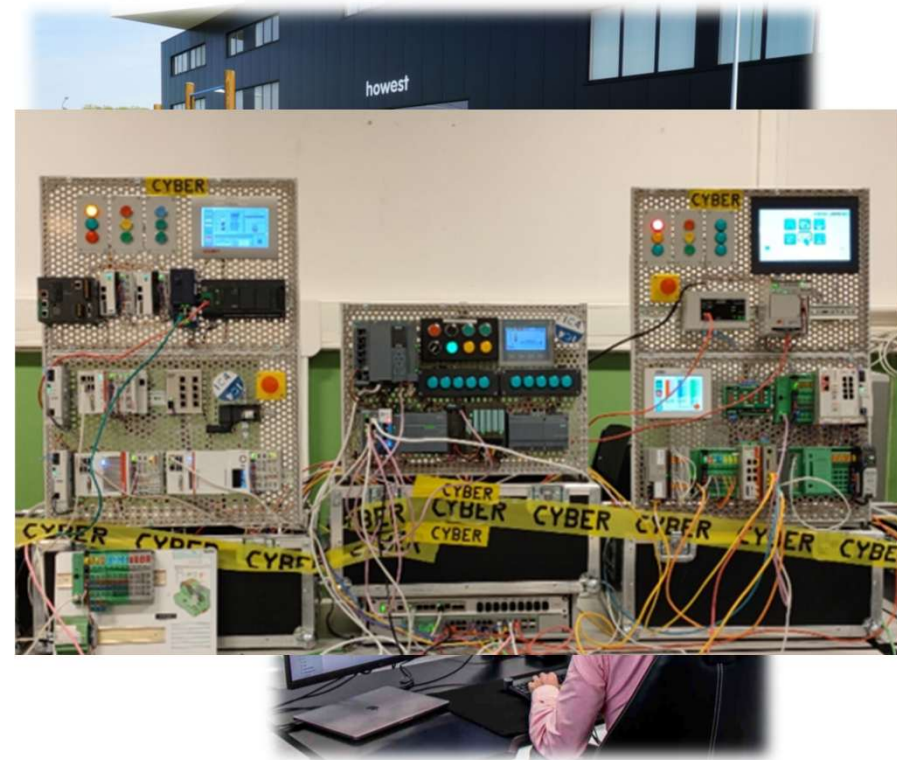
Cyberveiligheid in de industrie

Wie ben ik?



Security Researcher
& Educator
Laurens Singier

Laurens.singier@howest.be 





Wat is OT/ICS

Wat is OT?

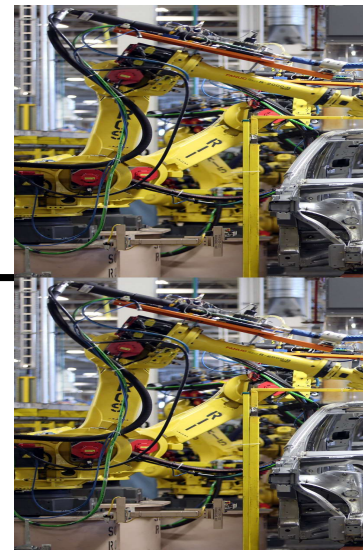
Office



Industrial Control Systems

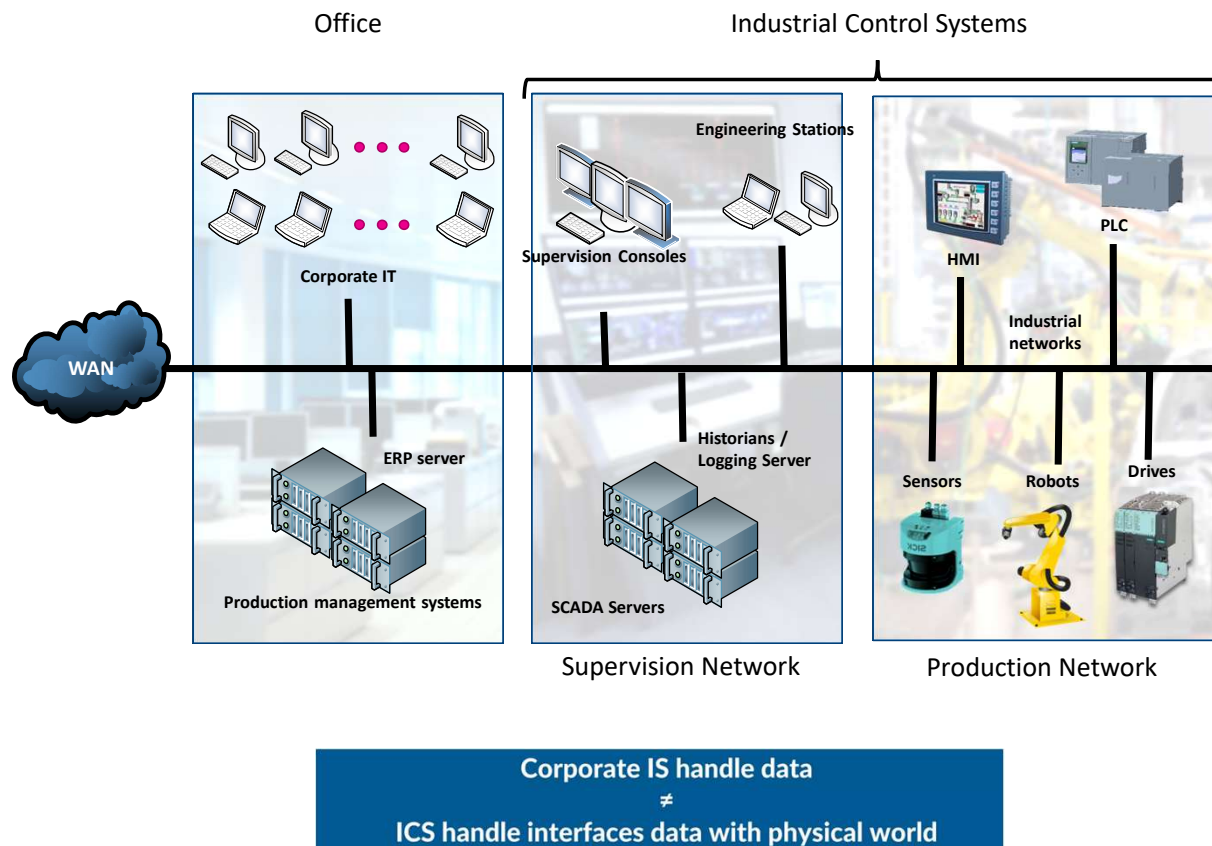


Supervision Network

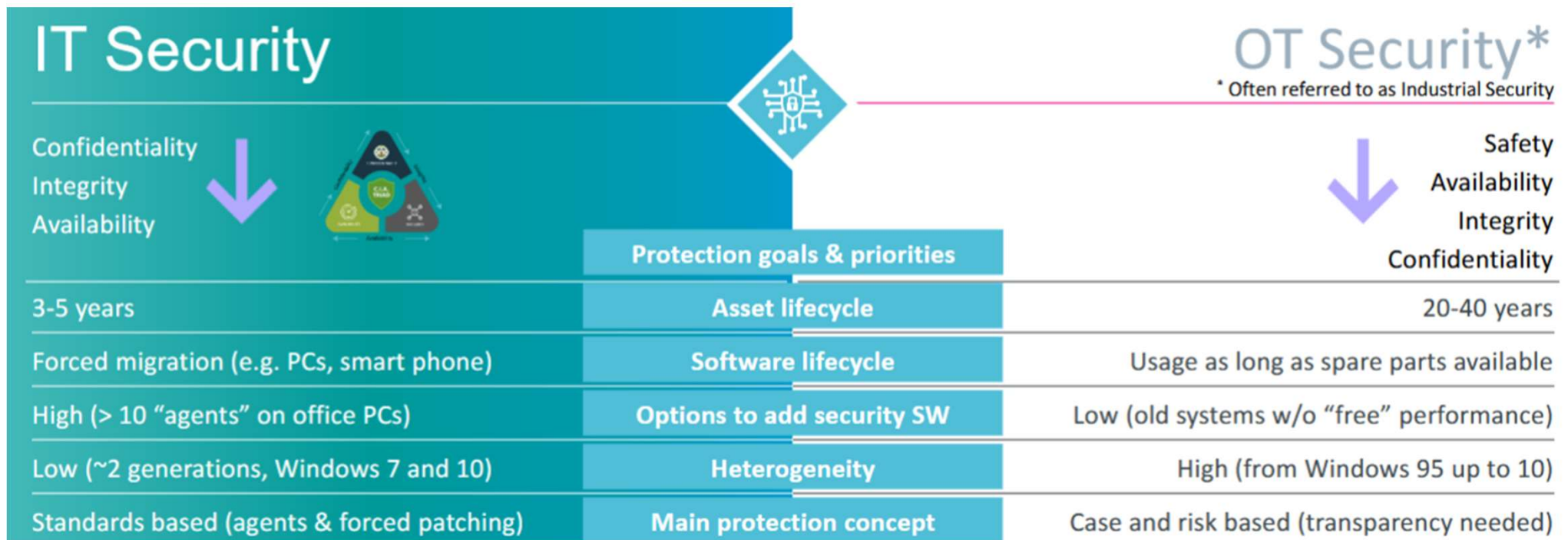


Production Network

Wat is OT?



Andere denkwijze





Hoe geraken hackers binnen?

De grootste gevaren

Top initial access vectors in 2022

Updated 2023-10-24 // @kwm

T1195: Supply Chain Compromise

1.6%

T1133: External Remote Services

4.8%

T1078: Valid Accounts

9.5%

T1189: Drive-by Compromise

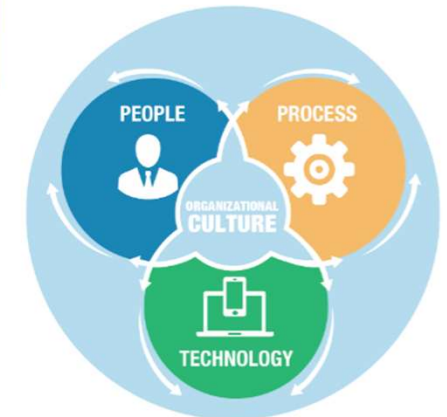
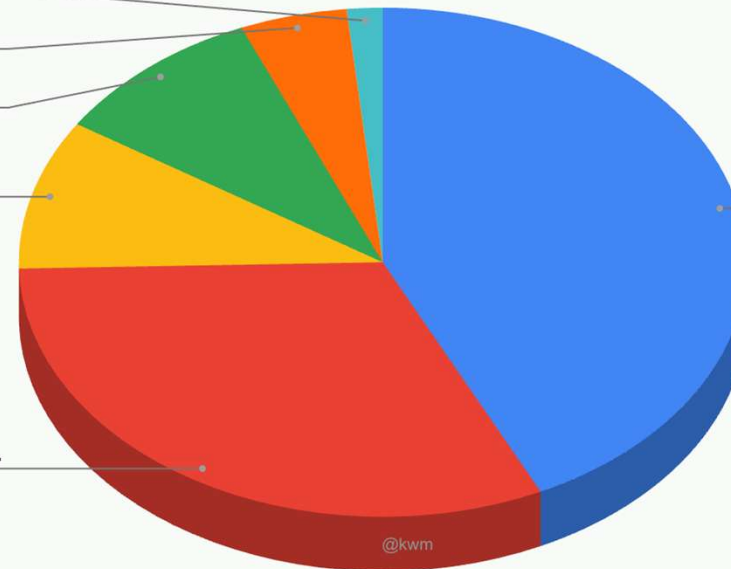
9.5%

T1190: Exploit Public-Facing App...

31.7%

T1566: Phishing

42.9%



Voorbeeld phishing herkennen

Van: bpost <compleet@communications.com>
Verzonden: 12 augustus 2020 11:54:39 CEST
Onderwerp: Informatie over uw pakje



Douanekosten zijn van toepassing op uw pakje

Hallo,
Gelieve de douanebelasting zo spoedig mogelijk te betalen, als er geen betaling plaatsvindt, wordt uw pakje teruggestuurd naar de afzender.

Barcode CB773245529FE

[Klik hier](#)

Van: Federale Overheidsdienst Financiën <info@financien.be>
Onderwerp: Belastingteruggave
Aan: [\[naam\] - Federaal](#)
Antwoord aan: [info@financien.be](#)

Kunt u deze e-mail niet goed lezen, bekijk dan de [webversie](#).



Belastingteruggave

Geachte heer/mevrouw,

Bij controle omtrent uw aangifte hebben wij kunnen zien dat u in aanmerking komt voor een terugbetaling. Dit bedrag maken wij zo snel mogelijk naar u over.
U ontvangt een teruggave van: €1260,85
Verifieer eerst uw gegevens en rekeningnummer om uw teruggave te ontvangen. Uw teruggave kan alleen op uw rekening worden bijgeschreven nadat de verificatie is voltooid.
De aanvraag zal binnen 3 werkdagen worden verwerkt.
www.vlaanderen.be/terugave

Met vriendelijke groet,
Federale Overheidsdienst Financiën

tsme* <service@u-itsme.email>
iden: Vrijdag 23 april 2021 18:36:29
werp: Een bericht over de status van uw account



Update onmiddellijk uw account

We moeten je account verifiëren om je contactgegevens te kunnen bevestigen, of je nu een nieuwe gebruiker bent of al lang klant bent bij ons. Bedankt voor je hulp!

Wij hebben onregelmatigheden in uw account geconstateerd. Uit veiligheidsredenen hebben wij uw account tijdelijk beperkt.

Wij raden aan om uw contactgegevens meteen na ontvangst van dit bericht, te verifiëren om mogelijke schade te voorkomen.

Als u ervoor kiest uw contactgegevens vandaag niet te verifiëren, wordt uw account mogelijk de volgende keer dat u probeert in te loggen geblokkeerd.

Maak u geen zorgen! Op dat moment ontvang je een nieuwe verificatie-e-mail van ons zodat je toegang hebt tot je account.

[contactgegevens verifiëren](#)

Vriendelijke groeten,
Je Itsme team

Dit bericht is verzonden met een e-mailadres waarop geen berichten kunnen worden ontvangen. Antwoord dus niet op deze e-mail.

Toenemende dreiging

VLAIO

Nieuws Duvel Moortgat

Duvel-ha
miljoen

e vraag

Nieuwsblad



Hackers gebruikten ransomware om cyberaanval uit te voeren: grote hinder op Brussels Airport, ook luchthavens Heathrow en Berlijn getroffen

Door een cyberaanval op een partner van Brussels Airport moet de check-in en boarding van passagiers daar zaterdag manueel gebeuren. Dat meldt de luchthaven. Er werden al geannuleerd, vijftien vluchten lopen vertragingen op van een uur of meer.



Technologie & Wetenschap

"Blauw scherm des doods" brengt talloze bedrijven in de problemen: wat is er nu eigenlijk aan de hand?

Computersystemen die plots herstarten, inclusief het fameuze "blauwe scherm des doods": duizenden bedrijven met Windows-pc's wereldwijd ondervinden pannes en problemen. Maar het probleem ligt eigenlijk helemaal niet bij Windows. Waar dan wel? En hoe valt dit op te lossen?

vrt nws

Nieuws Events Ondernemersverhalen Blog Publi
Informatie, begeleiding & advies Subs

Bedrijven in 2024 cyberaanval

Bedrijven (45,8%) slachtoffer van een cyberaanval. Dit zijn de belangrijkste bevindingen uit de 10de schadelijke nieuwe cybersecurity barometer.

De grootste gevaren

Top initial access vectors in 2022

Updated 2023-10-24 // @kwm

T1195: Supply Chain Compromise

1.6%

T1133: External Remote Services

4.8%

T1078: Valid Accounts

9.5%

T1189: Drive-by Compromise

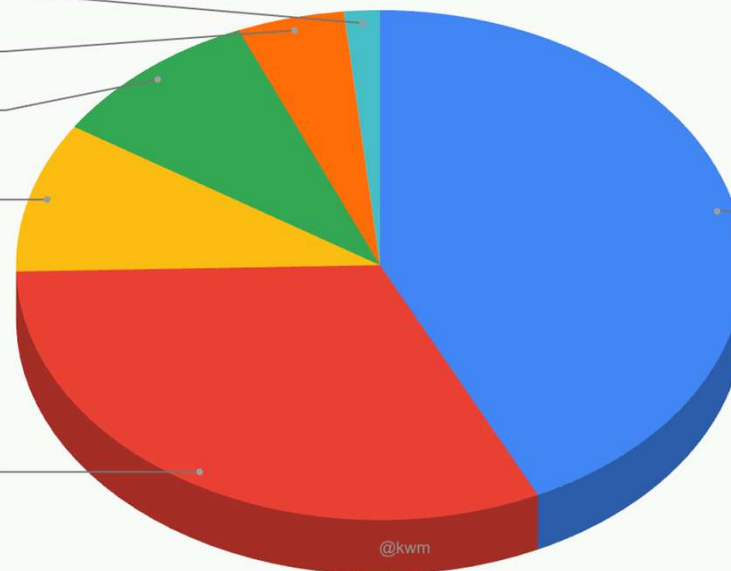
9.5%

T1190: Exploit Public-Facing App...

31.7%

T1566: Phishing

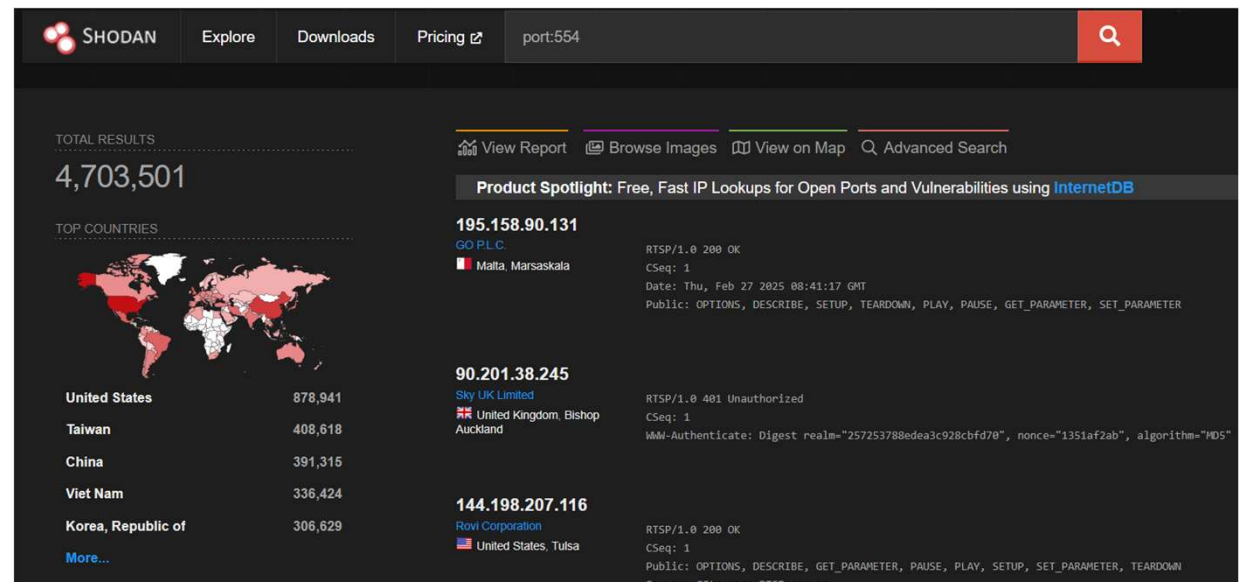
42.9%



Public-facing applications

Shodan is a search engine for devices
Automatically scans and indexes the entire public IP range for multiple TCP ports

- Explore the possibilities:
<https://www.shodan.io/explore>
- Hint: It's free, you can check
your own public IP's!



Shodan

- <https://www.shodan.io/>

The screenshot displays the Shodan search engine interface. The top navigation bar includes links for Shodan, Maps, Images, Monitor, Developer, and More. A search bar at the top contains the text 'screenshot.label:ics'. Below this, a sidebar on the left shows search results for 'port:502'. The sidebar includes a 'Total Results' count of 320,520, a 'Top Countries' list, and a 'Top Organizations' list.

Top Countries

Country	Count
US	269,762
KR	4,792
CA	4,020
FR	2,939
ES	2,353

Top Organizations

Organization	Count
Google LLC	250,456
Brocade Communications	4,100
Korea Telecom	2,751
Equifax, Inc.	2,609
Shopify, Inc.	2,586

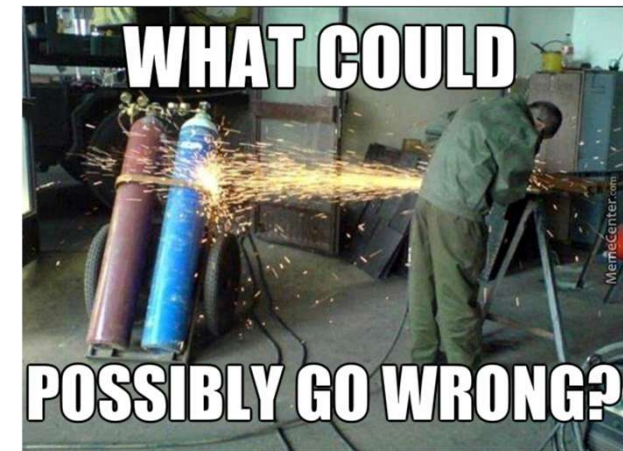
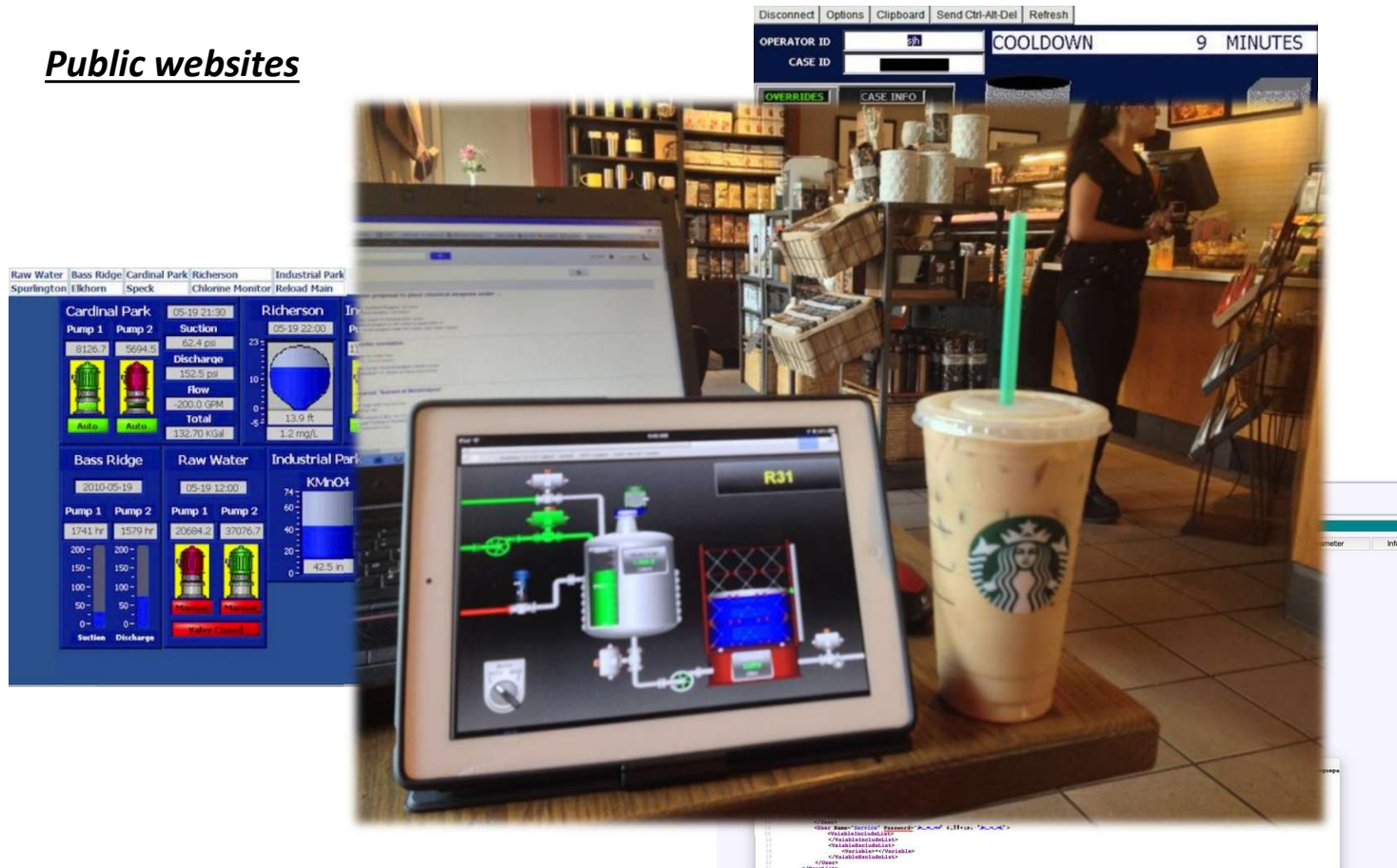
The main search results area shows a map of Belgium with numerous red dots indicating search results. A technical diagram of an aqua centre system is overlaid on the map. The diagram includes components such as a DELIVERY RESERVOIR, FILTER, SUCTION RESERVOIR, and various valves and pumps. The system is labeled 'AQUA CENTRE' and shows a 'SYSTEM STATUS' of 'SYSTEM HEALTHY'. The diagram also includes a 'WASTE' line, a 'FLUSH VALVE', and a 'SCOUR VALVE'. The system is controlled via a 'SYSTEM STATUS' panel with buttons for 'SWITCH SYSTEM OFF', 'START CYCLE', and 'SETTINGS'.

Internet Intelligence

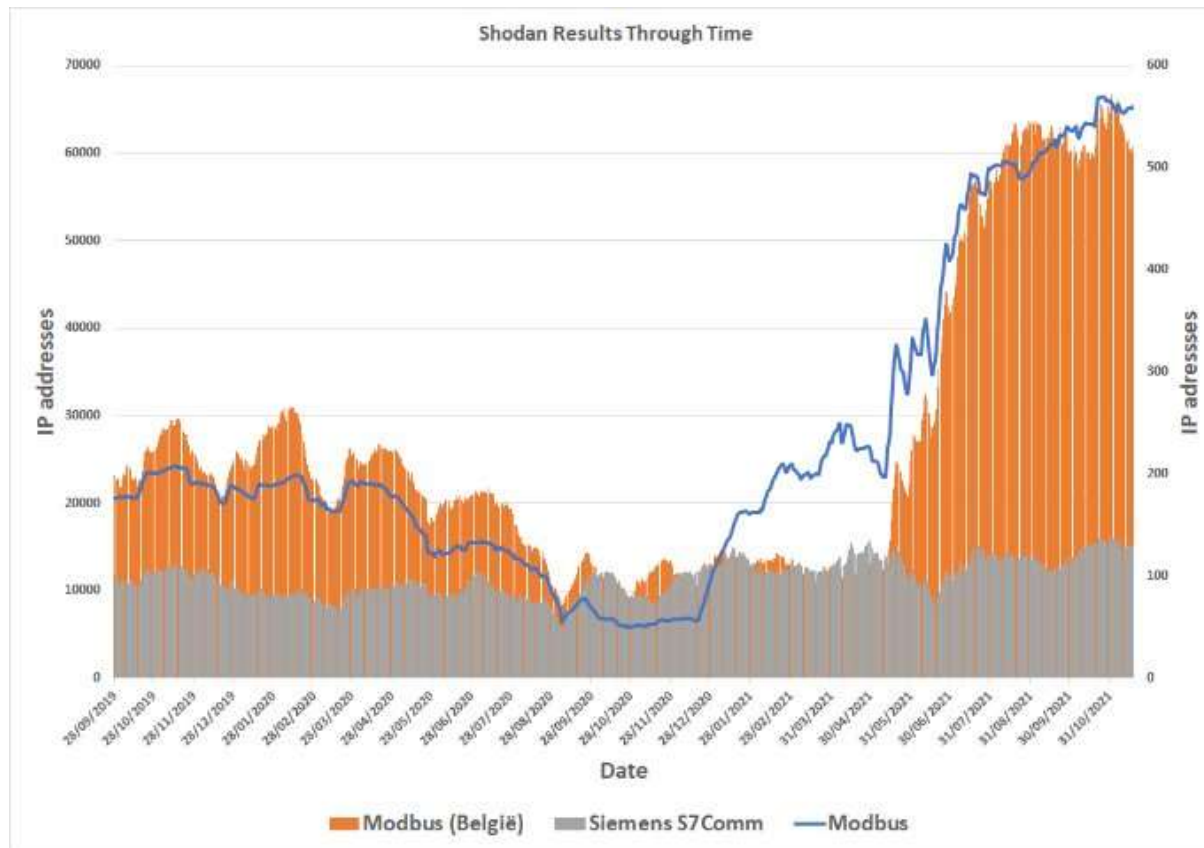
Learn more about who is using various products and how they're changing over time. Shodan gives you a data-driven view of the technology that powers the Internet.

Remote access over internet to ICS

Public websites



Current day?

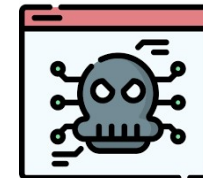


What are cyberthreats

Cyber threats are malicious actions aimed at gaining access to computers and networks to cause damage or steal information.

Their goal:

- Financial losses
- Reputation damage
- Loss of sensitive information



Malware... not something new

CryptoLocker

Your personal files



Your important files encryption produced on this computer. [Here](#) is a performance list of encrypted files.

Encryption was produced using a **unique** public key for this computer. To decrypt files you need to obtain the private key.

The **single copy** of the private key, which will be stored on a secret server on the Internet; After the time specified in the ransom note, the price of recovery will be **increased 2 times**.

In a month, the private key will be automatically destroyed. **nobody and never will be able** to restore files.

To obtain the private key for this computer, which will be sent to you by email, you need to pay **600 USD / 600 EUR / similar amount** in Bitcoin.

Click "Next" to select the method of payment and receive the private key.

Any attempt to remove or damage this software will result in the destruction of the private key by server.

Price will be increased by **2 times**
06 / 03 / 2014 3:43:04
Time left 86:54:22

Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English

What Happened to My Computer?

Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send \$300 worth of bitcoin to this address:

Bitcoin ACCEPTED HERE

[About bitcoin](#)
[How to buy bitcoins?](#)
[Contact Us](#)

Malware for sale

<https://www.nomoreransom.org/nl/index.html>

 **NO MORE RANSOM**

NEED HELP
unlocking your digital
life without paying
your attackers*?

At the moment, not every type of ransomware has a solution. Keep checking this website as new keys and applications are added when available.

 **howest**
we develop people

[Partners](#) [About the Project](#) [English](#) 

[Home](#) [Crypto Sheriff](#) [Ransomware: Q&A](#) [Prevention Advice](#) [Decryption Tools](#) [Report a Crime](#)



Ransomware is malware that locks your computer and mobile devices or encrypts your electronic files. When this happens, you can't get to the data unless you pay a ransom.

However this is not guaranteed and you should never pay!



< New decryptor for **Bianlian** available, please click here. >

Q&A

Wat is de gemiddelde tijdspanne van een inbraak tot ransomware?

90 dagen



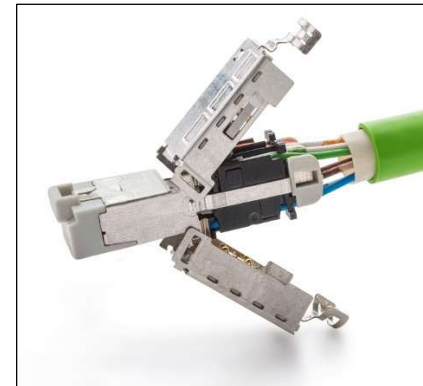
De problemen met OT

Why OT Security now

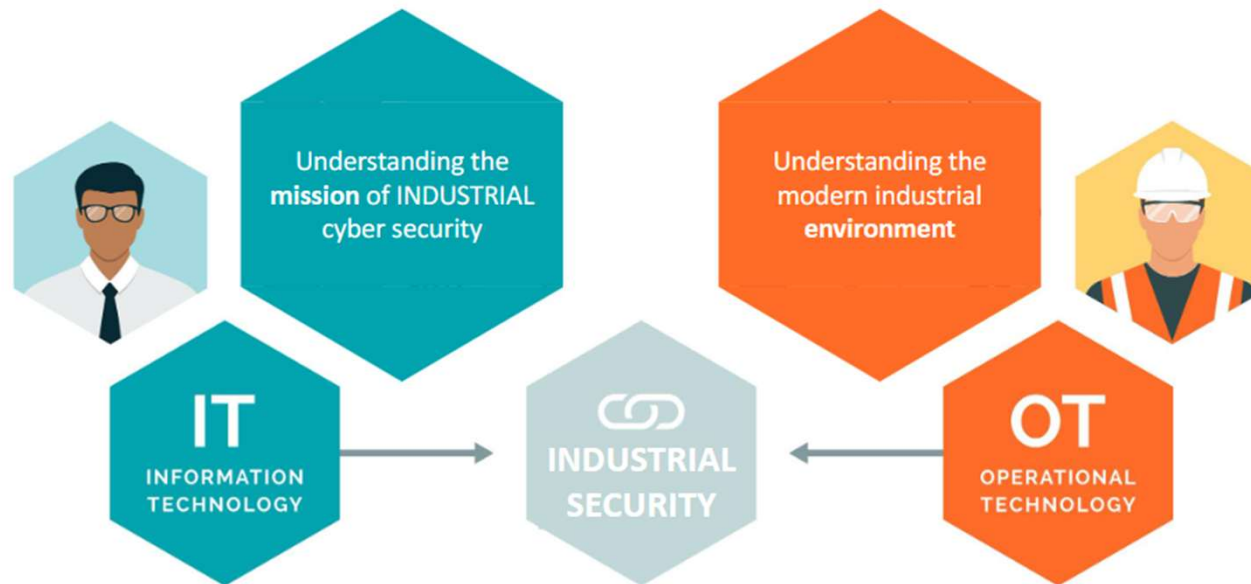
Several migrations have happened over time:

- $\pm$ 15 years ago: all systems still used fieldbus protocols
 - There was a movement to Ethernet based protocols
- $\pm$ 10 years ago: networking became abundant, everything started to become intra connected
 - Engineers / operators / managers connecting to their **production** devices from everywhere in the company
- $\pm$ 5 years ago: the age of IoT, Big Data and Industry 4.0
 - Engineers / operators / managers want to monitor, manage and connect to their **production** devices from at home

*And all this using protocols that were developed +40 years ago
and have zero support for security, authentication, encryption ...*



Ownership



Forced usage of outdated systems

Rockwell Automation Compability	RSLogix 5000	RSLogix 5000	RSLogix 5000	RSLogix 5000	Studio 5000 Logix Designer	Rockwell Automation Compability	RSLogix 5000	RSLogix 5000	RSLogix 5000	RSLogix 5000	Studio 5000 Logix Designer
2019	14.01.00	18.02.00	19.01.01	20.01.01	21.03.02	2019	14.01.00	18.02.00	19.01.01	20.01.01	21.03.02
Windows 7 Enterprise SP1 32-bit	!	✗	✓	✓	!	Linux	!	!	!	!	✗
Windows 7 Enterprise SP1 64-bit	!	✗	✓	✓	!	Windows 2000	!	✗	✗	✗	✗
Windows 7 Home Premium (32-bit)	!	✗	✓	✓	!	Windows NT Workstation 4.0 (NTFS)	!	✓	✓	✗	✗
Windows 7 Home Premium (64-bit)	!	✗	✓	✓	!	Windows 10 Enterprise, 32-bit, Version 1511	!	!	!	!	!
Windows 7 Home Premium SP1 32-bit	!	!	!	!	✓	Windows 10 Enterprise, 32-bit, Version 1607	!	!	!	!	!
Windows 7 Home Premium SP1 64-bit	!	!	!	!	!	Windows 10 Enterprise, 64-bit, Version 1511	!	!	!	!	!
Windows 7 Professional (32-bit)	!	✗	✓	✓	!	Windows 10 Enterprise, 64-bit, Version 1607	!	!	!	!	!
Windows 7 Professional (64-bit)	!	✗	✓	✓	!	Windows 10 Enterprise, 64-bit, Version 1703	!	!	!	!	!
Windows 7 Professional SP1 (32-bit)	!	✗	✓	✓	!	Windows 10 Professional, 32-bit, Version 1511	!	!	!	!	!
Windows 7 Professional SP1 (64-bit)	!	✗	✓	✓	✓	Windows 10 Professional, 32-bit, Version 1607	!	!	!	!	!
Windows 7 Ultimate SP1 32-bit	!	!	!	!	!	Windows 10 Professional, 64-bit, Version 1511	!	!	!	!	!
Windows 7 Ultimate SP1 64-bit	!	!	!	!	!	Windows 10 Professional, 64-bit, Version 1607	!	!	!	!	!
Windows 8 (home) 32-Bit	!	✗	✗	✗	!	Windows 10 Professional, 64-bit, Version 1703	!	!	!	!	!
Windows 8 (home) 64-Bit	!	✗	✗	✗	!	Windows 2003 Standard (32-bit)	!	✓	✓	✓	✗
Windows 8 Enterprise 32-Bit	!	✗	✗	✗	!	Windows 2003 Standard SP1 (32-bit)	!	✓	✓	✓	✗
Windows 8 Enterprise 64-Bit	!	✗	✗	✗	!	Windows 2003 Standard SP2 (32-bit)	!	✓	✓	✓	✗
Windows 8 Professional 32-Bit	!	✗	✗	✗	!	Windows 2003 R2 Standard (32-bit)	!	!	!	!	✗
Windows 8 Professional 64-Bit	!	✗	✗	✗	!	Windows 2003 R2 Standard SP2 (32-bit)	✓	✓	✓	✓	✗
Windows 8.1 Enterprise 32-Bit	!	✗	✗	✗	!	Windows 2003 R2 Standard SP2 (64-bit)	!	!	!	!	✗
Windows 8.1 Enterprise 64-Bit	!	✗	✗	✗	!	Windows Server 2003 Standard R2 SP1 [32-bit]	!	!	!	!	✗
Windows 8.1 Professional 32-Bit	!	✗	✗	✗	!	Windows Server 2008 Standard (32-bit)	!	✓	✓	✓	✗
Windows 8.1 Professional 64-Bit	!	✗	✗	✗	!	Windows Server 2008 Standard SP1 (32-bit)	!	!	!	!	✗
Windows Vista Business (32-bit)	!	✓	✓	✓	!	Windows Server 2008 Standard SP1 [64-bit]	!	!	!	!	✗
Windows XP Pro (32-bit)	!	✗	✗	✗	✗	Windows Server 2008 Standard SP2 (32-bit)	!	!	!	✓	✗
Windows XP Pro SP1 (32-bit)	!	✗	✗	✗	✗	Windows Server 2008 Standard SP2 (64-bit)	!	!	!	✓	✗
Windows XP Pro SP2 (32-bit)	!	✗	✗	✗	✗	Windows Server 2008 R2 Enterprise SP1	!	!	!	!	!
Windows XP Pro SP3 (32-bit)	!	✓	✓	✓	✗	Windows Server 2008 R2 Standard	!	!	!	!	!

Vendor warning



Beckhoff Security Advisory

Advisory 2017-001: ADS is only designed for u

Publication Date 03/13/2017
 Last Update 07/02/2018
 Current Version 1.1
 Relevance Medium
 Related CVE CVE-2017-16726

Summary

ADS is only advised to be used in protected environments, and a
 Attackers can eavesdrop, manipulate and forge arbitrary packets

Appearance

- TwinCAT 2
- TwinCAT 3

Description

Beckhoff TwinCAT supports communication over ADS. ADS, ADS
 protected environments [1]. ADS has not been designed to act
 not include any encryption algorithms because of their negative e

An attacker can forge arbitrary ADS packets when legitimate AD

Solution

Use ADS Protocol only in protected environments.

Siemens Security Advisory by Siemens ProductCERT

SSA-603476: Web Vulnerabilities in SIMATIC CP 343-1/CP 443-1 Modules and SIMATIC S7-300/S7-400 CPUs

Publication Date 2016-11-21
 Last Update 2016-11-21
 Cu
 CV

Mitigation:

Phoenix Contact Software recommends that users implement an adequate defense-in-depth
 networking architecture for control systems where these devices are operating. The use of
 virtual private networks (VPNs) is highly recommended for remote access, as well as the use
 of firewalls for network segmentation or controller isolation when required.

Automation suppliers might use the ProConOS open protocol layer to update their
 automation devices with a new firmware version implementing own authentication
 mechanism.

Acknowledgement:

Phoenix Contact would like to thank Reid Wightman of Digital Bond and ICS-CERT for a
 coordinated release of this vulnerability.

Resources:

Recommended security practices by ICS-CERT:

☞ <http://ics-cert.us-cert.gov/content/recommended-practices>

Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-
 In-Depth Strategies

☞ [https://ics-cert.us-](https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Defense_in_Depth_Oct09.pdf)
[cert.gov/sites/default/files/recommended_practices/Defense_in_Depth_Oct09.pdf](https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Defense_in_Depth_Oct09.pdf)

For more information about the official ICS-CERT advisory please refer to:

☞ <https://ics-cert.us-cert.gov/advisories/ICSA-15-013-03>

Living off the land

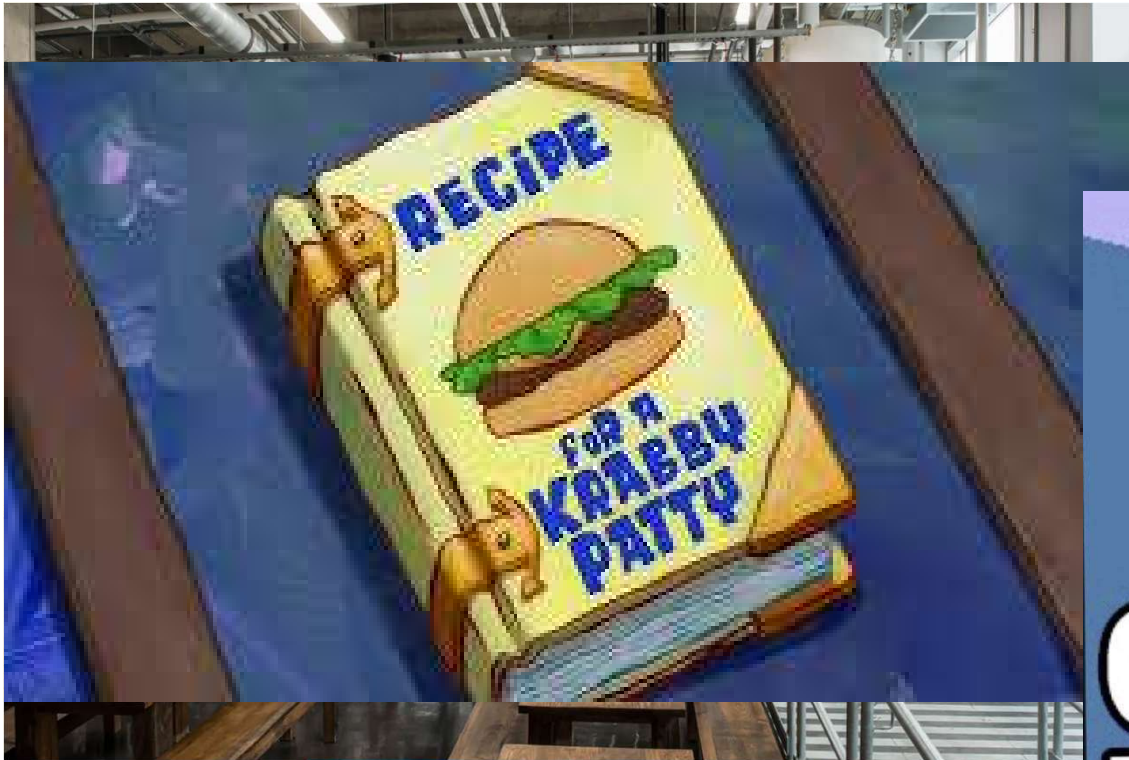
- Use native tools
- Low detectability
- Minimal footprint
 - Powershell scripts
 - WMI abuse
 - Credential dumping
 - Using certutil.exe bitsadmin.exe, wmic.exe to move data and execute commands





Real world cases

Risk awareness: “Public devices”



Risk awareness: “Physical security”



Risk awareness: “Passwords”



Email Address	Password
john.doe@howest.be	X9f!5pH7zV
mary.smith@howest.be	L3r@p8uT1zW
tom.jones@howest.be	T\$7fQn1kLx
sarah.lee@howest.be	J7pH*4uVrM8
mark.ross@howest.be	Kz9Z\$0bKMP
laura.white@howest.be	Y1jR@v6xXw
james.wilson@howest.be	Fz3wLs5#oH
linda.martin@howest.be	U4pB!t7jVg
robert.brown@howest.be	P8dM9!fD2l
lisa.davis@howest.be	R1jY@z7nFQ

Email Address
john.doe@industry-howest.be
mary.smith@industry-howest.be
tom.jones@industry-howest.be
sarah.lee@industry-howest.be
mark.ross@industry-howest.be
laura.white@industry-howest.be
james.wilson@industry-howest.be
linda.martin@industry-howest.be
robert.brown@industry-howest.be
lisa.davis@industry-howest.be

sarah.lee@industry-howest.be

J7pH*4uVrM8



Realistic real word scenario

- Let's say we want to target factory.xyz
- Find their public facing applications with Shodan zoomeye, crt.sh...
- Enumerate those endpoints.
- VPN access into the network
- Enumerate hosts
- Exploit the weak protocols

CVE-2022-40684

POC for CVE-2022-40684 affecting Fortinet FortiOS, FortiProxy, and FortiSwitchManager appliances.

Technical Analysis

A technical root cause analysis of the vulnerability can be found on our blog: <https://www.horizon3.ai/fortios-fortiproxy-and-fortiswitchmanager-authentication-bypass-technical-deep-dive-cve-2022-40684>

Indicators of Compromise

For a detailed analysis, see our blog: <https://www.horizon3.ai/fortios-fortiproxy-and-fortiswitchmanager-authentication-bypass-technical-deep-dive-cve-2022-40684>

Sur

This

CVE-2022-40684

Description

An authentication bypass vulnerability in FortiProxy version 7.2.1 and 7.0.0 through 7.0.6, allowing an unauthenticated attacker to perform operations.



7.2.1 and 7.0.0 through 7.0.6, allowing an unauthenticated attacker to perform operations.

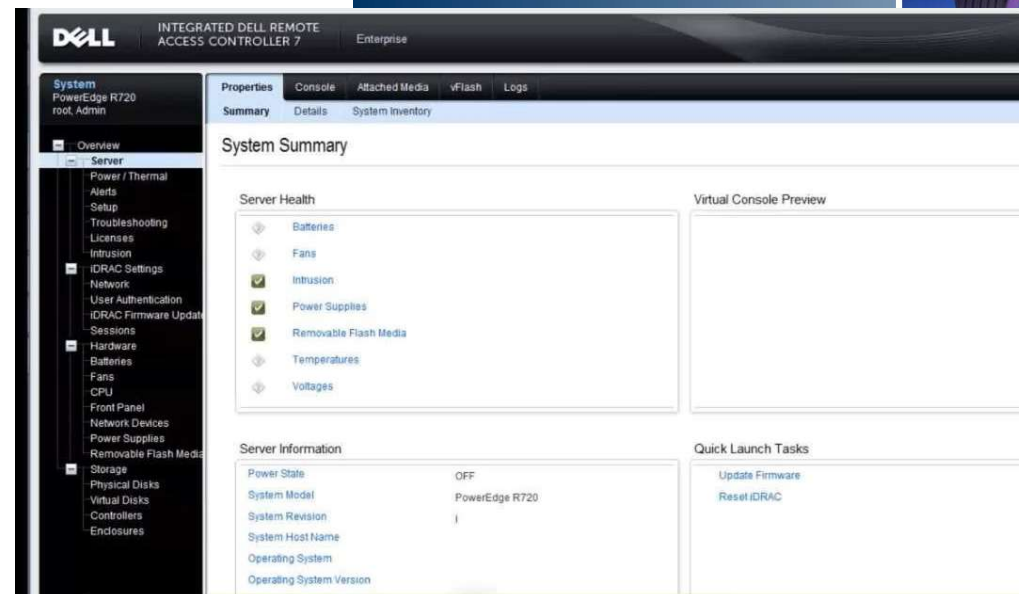
IPMI 2.0 (intelligent platform management interface)

Via IPMI beheer je servers op afstand.

https://www.rapid7.com/db/modules/auxiliary/scanner/ipmi/ipmi_dumphashes/

Als je de naam van een useraccount kent kan je de hash opvragen.

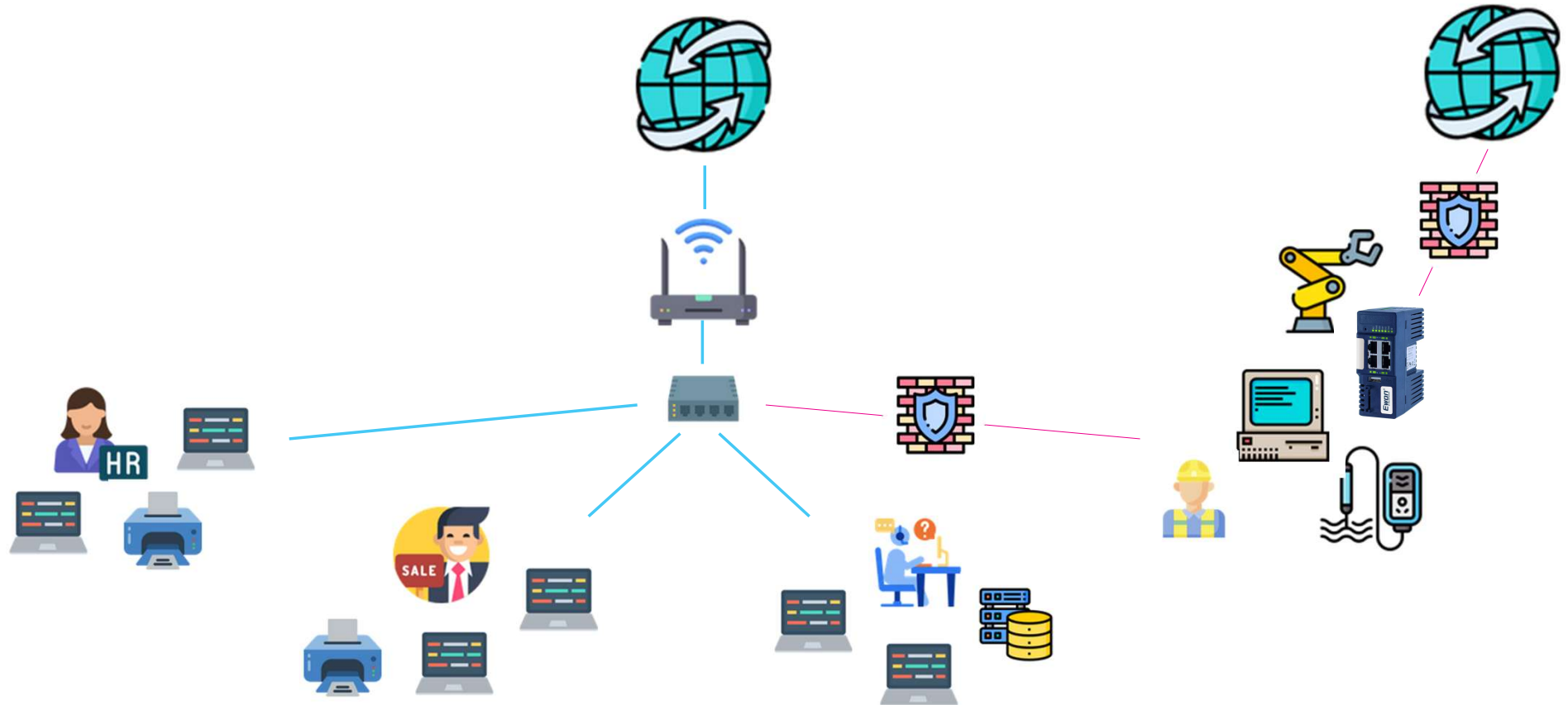
UDP 623





Eerste stappen

Segmentatie



Limit need access

- Separate guest - office WiFi
- Separate or put layers (firewall, data diode,...) between OT & IT
- Don't connect anything to the outside without it being absolutely necessary. (IIoT data, VNC connection to HMI,...)
- Implement accountability, use users/roles to limit access and log who does what in case something goes wrong.



Monitoring solutions

- **Visibility**

- Asset discovery & inventory

- **Detection**

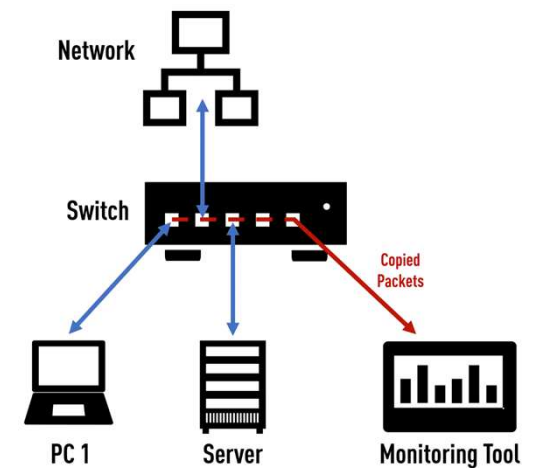
- Pin-point security threats in real time

- **Response**

- Accelerate remediation efforts



Kaspersky®
Industrial
CyberSecurity



Evolution

default password change

segmentation & risk awareness

security architecture & asset management

start incidence response plan

monitoring

