easynet group

enForcer SECURITY

TECNOLOGIE D'IMPRESA Srl

Cybersecurity: un ecosistema fatto di persone

28 gennaio 2020

ore 17.30

Auditorium Casa dell'Economia, Via Tonale 30, Lecco

Agenda

- Industry 4.0
- Quali sono i rischi?
- Come proteggere i nostri impianti?
- Riferimenti
- Q&A

Igor Falcomatà

ifalcomata@enforcer.it

- attività professionale:
  - analisi delle vulnerabilità e penetration testing
  - security consulting
  - formazione
- altro:
  - ISACA Venice
  - sikurezza.org
  - (f|er-|bz-)lug

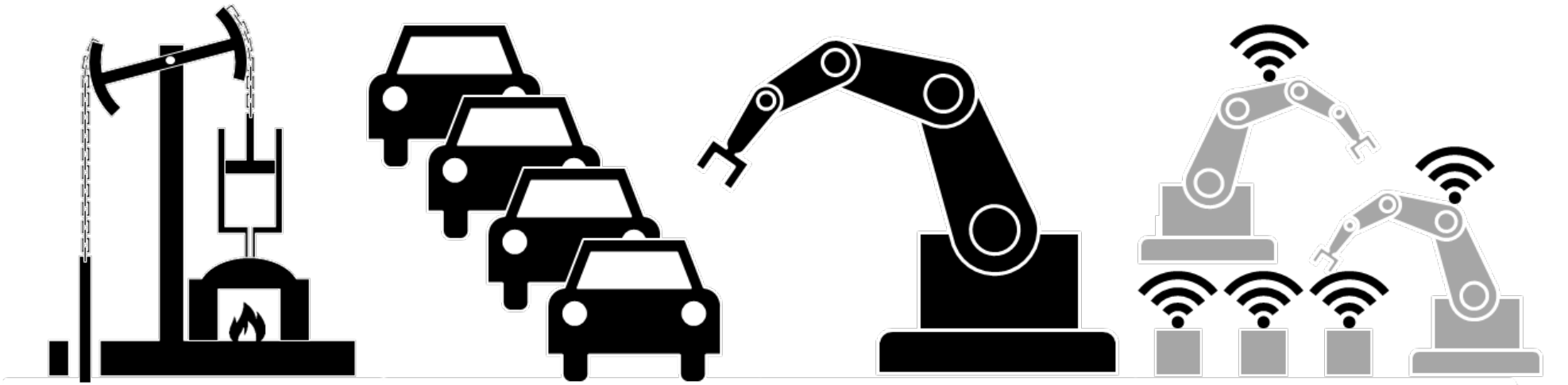
free advertising >

Industry 4.0 Insecurity

Agenda

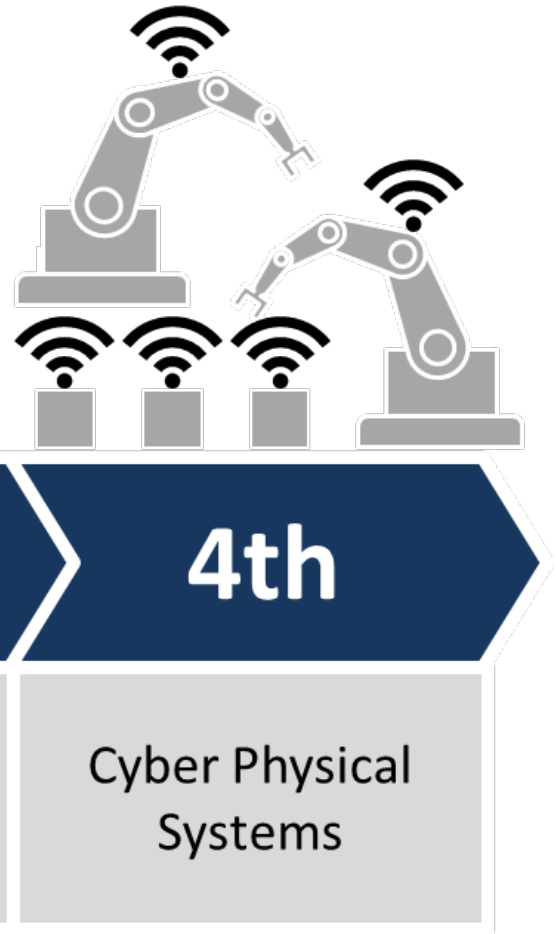
- **Industry 4.0**
- Quali sono i rischi?
- Come proteggere i nostri impianti?
- Riferimenti
- Q&A

Introduzione



1st	2nd	3rd	4th
Mechanization, water power, steam power	Mass production, assembly line, electricity	Computer and automation	Cyber Physical Systems

Industry 4.0

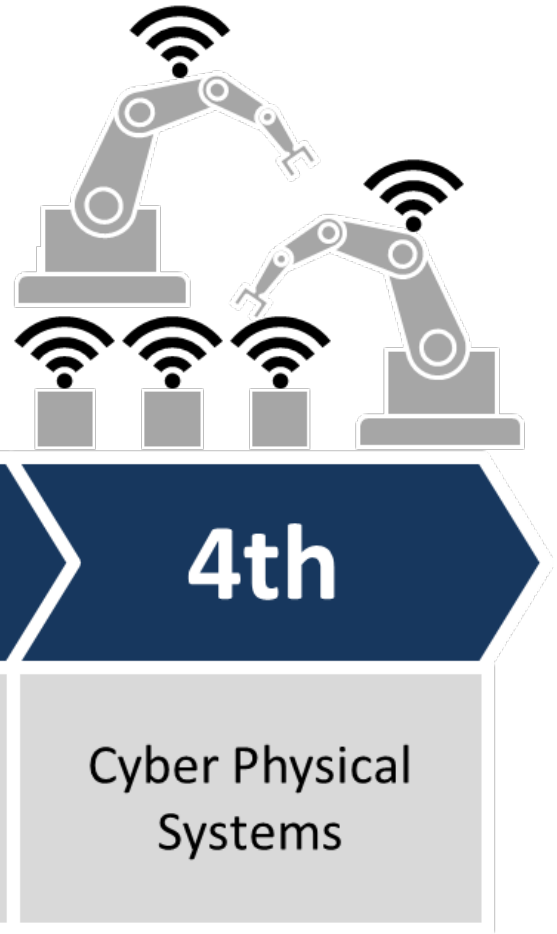


Scambio di dati tra impianti industriali ed altre infrastrutture:

- ➔ **rete locale**
- ➔ **rete geografica / intranet**
- ➔ **Internet**

- **molti vantaggi**
- **molti rischi**

Rete fabbrica



Infrastruttura complessa:

- **tecnologia tradizionali “fabbrica”**
  - **PLC, ICS, SCADA, bus di comunicazione e interfacce “industriali”, sw dedicati, ..**
- **tecnologie tradizionali ICT**
  - **Ethernet, WiFi, TCP/IP, OS “server” e “workstation”, sw general pourpose, virtualizzazione, storage, remote desktop e telecontrollo, ecc.**

Industry 4.0 Insecurity

Agenda

- Industry 4.0
- **Quali sono i rischi?**
- Come proteggere i nostri impianti?
- Riferimenti
- Q&A

Table 1: Threats affecting ICS/SCADA systems

[ENISA]

Image by ENISA, Communication network dependencies for ICS/SCADA Systems, pg. 29

Spesso l'anello più debole (per la sicurezza informatica) sono le componenti dell'ambito "fabbrica":

- **non sono state pensate per essere utilizzate in ambienti potenzialmente "ostili" e "inaffidabili" (p. es. Internet)**
- **il loro design è mirato a garantirne l'affidabilità nel processo produttivo**
- **difficilmente integrano – almeno di default – meccanismi che garantiscano la segretezza delle comunicazioni**
- **configurazioni "di default"**

[ENISA]

Image by ENISA, Communication network dependencies for ICS/SCADA Systems, pg. 29

Scenari di attacco

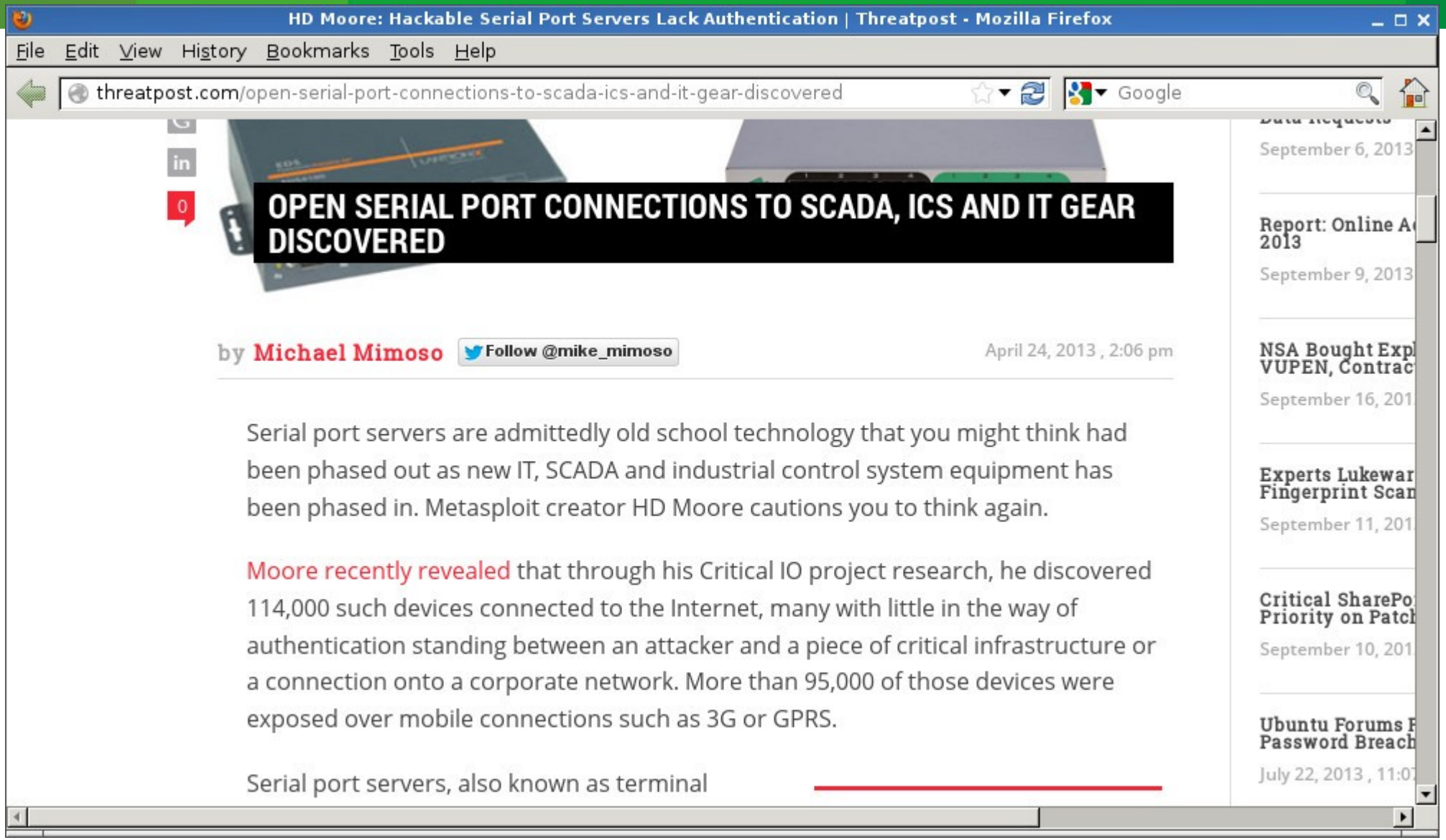
[ENISA]

Table 3: Sample Attack Scenarios

SAMPLE ATTACK SCENARIOS	IMPORTANCE LEVEL
1. Against the administration systems of SCADA	Crucial
2. Against actuators	High / Crucial
3. Against the network link between sensors/actuators and HMI or controller	High
4. Against sensors	Medium / Crucial
5. Against the information transiting the network	Medium / Crucial
6. Compromised ICT components as backdoors	Medium / Crucial
7. Exploit Protocol vulnerabilities	Medium / High
8. Against Control Data Historians, Local HMIs or controllers	Medium

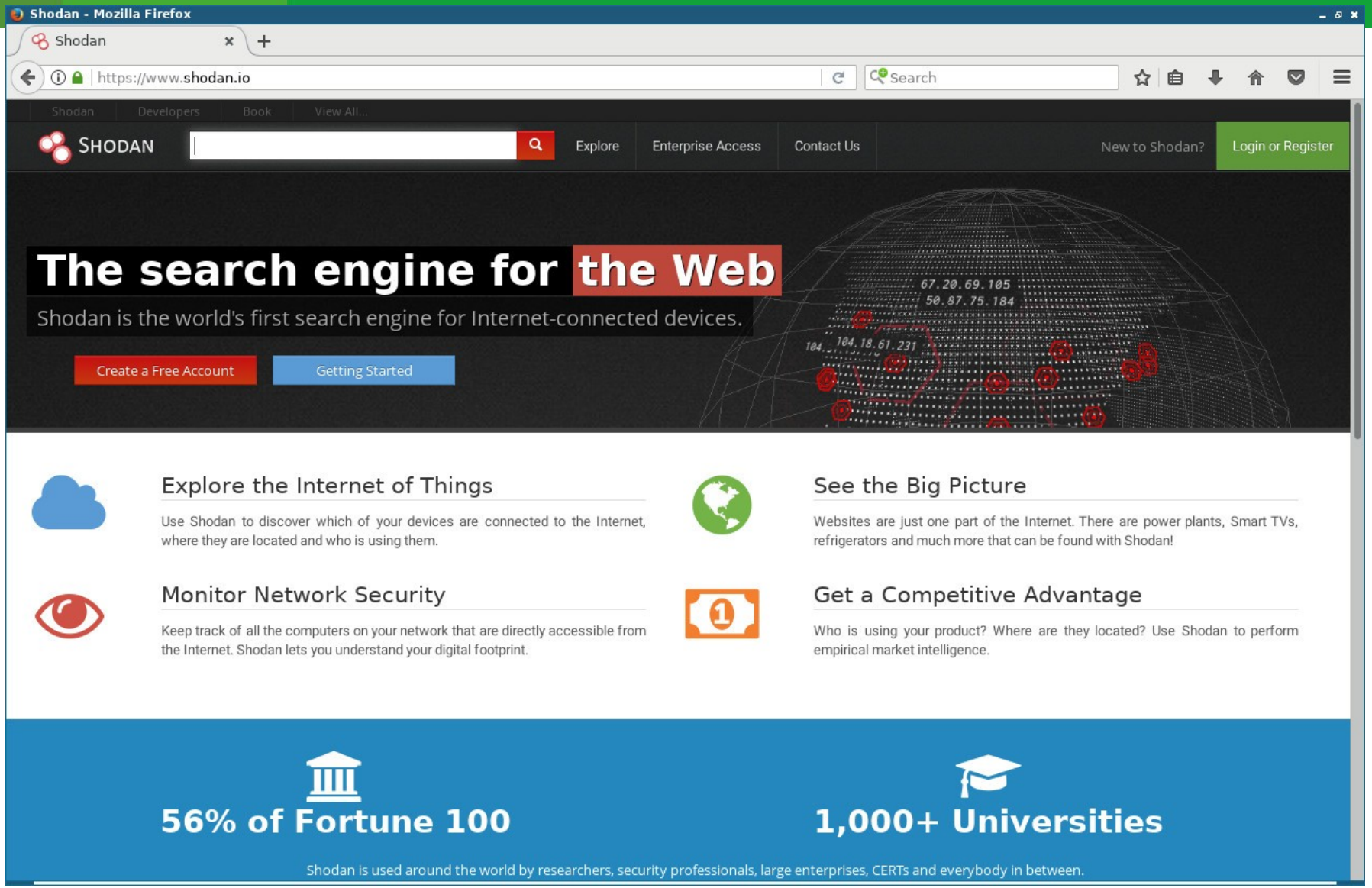
Image by ENISA,
Communication network dependencies for ICS/SCADA Systems, pg. 32

Alcuni esempi..



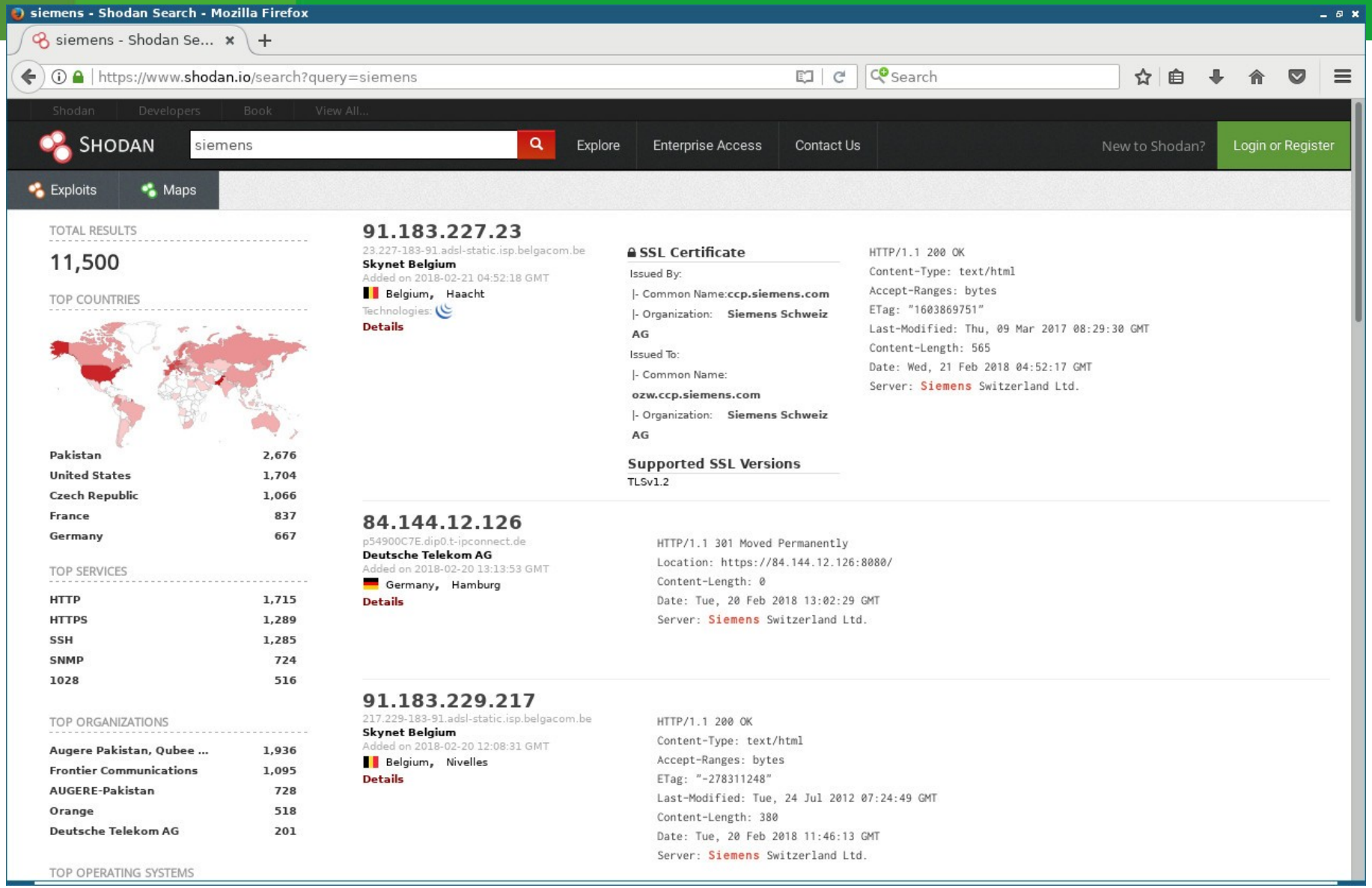
http://threatpost.com/open-serial-port-connections-to-scada-ics-and-it-gear-discovered

Alcuni esempi..



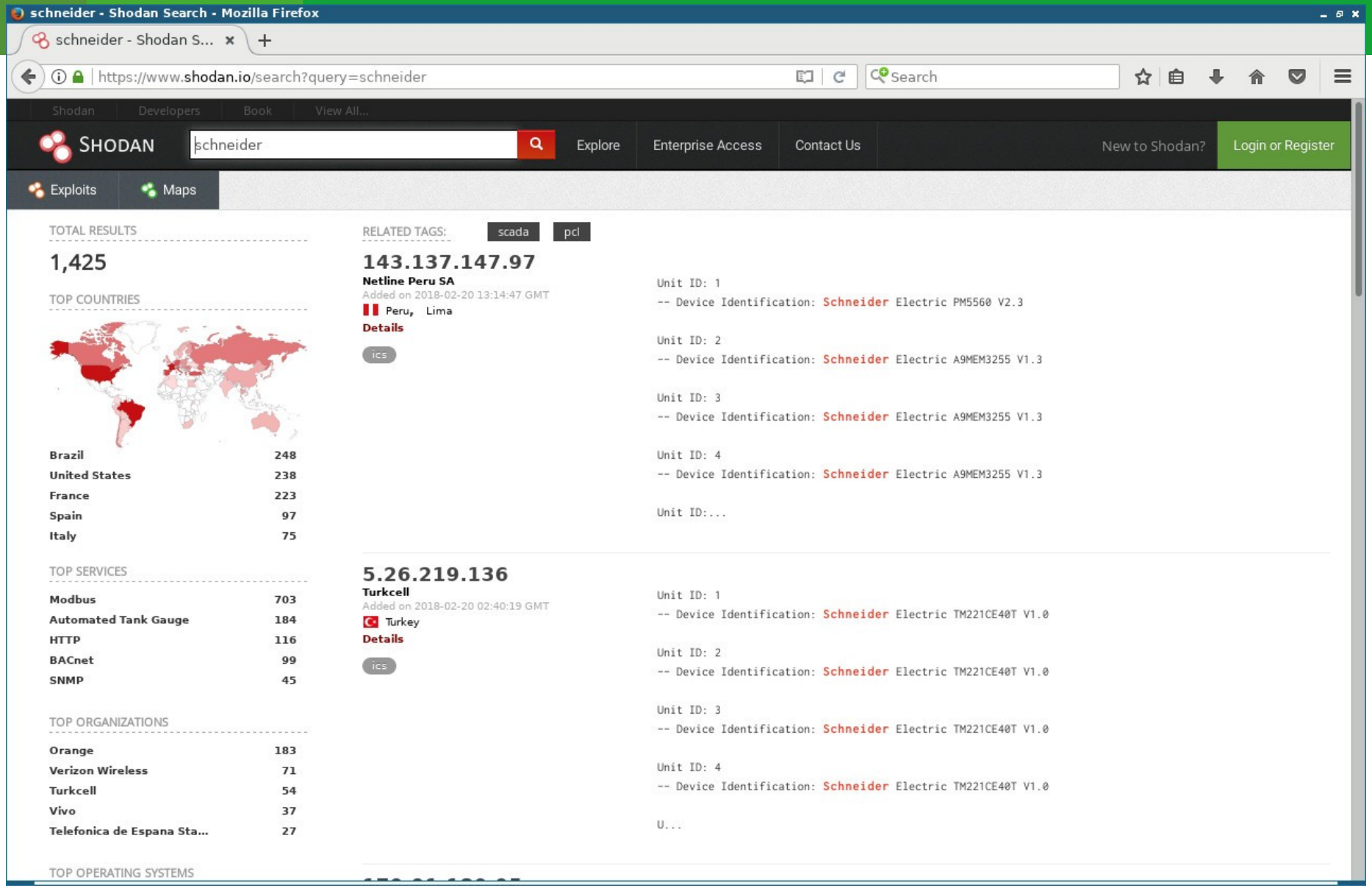
https://www.shodan.io/

Alcuni esempi..



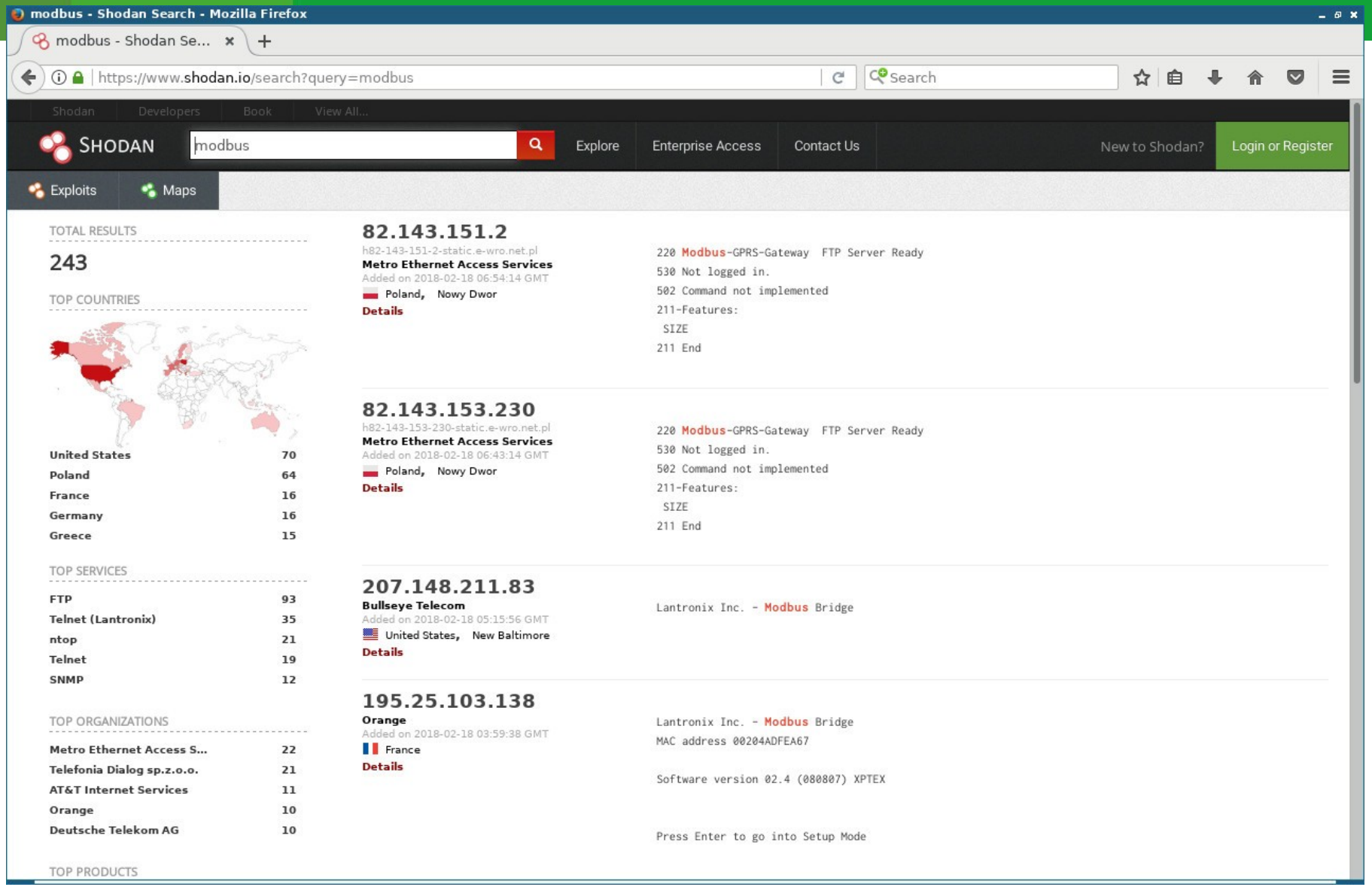
https://www.shodan.io/

Alcuni esempi..



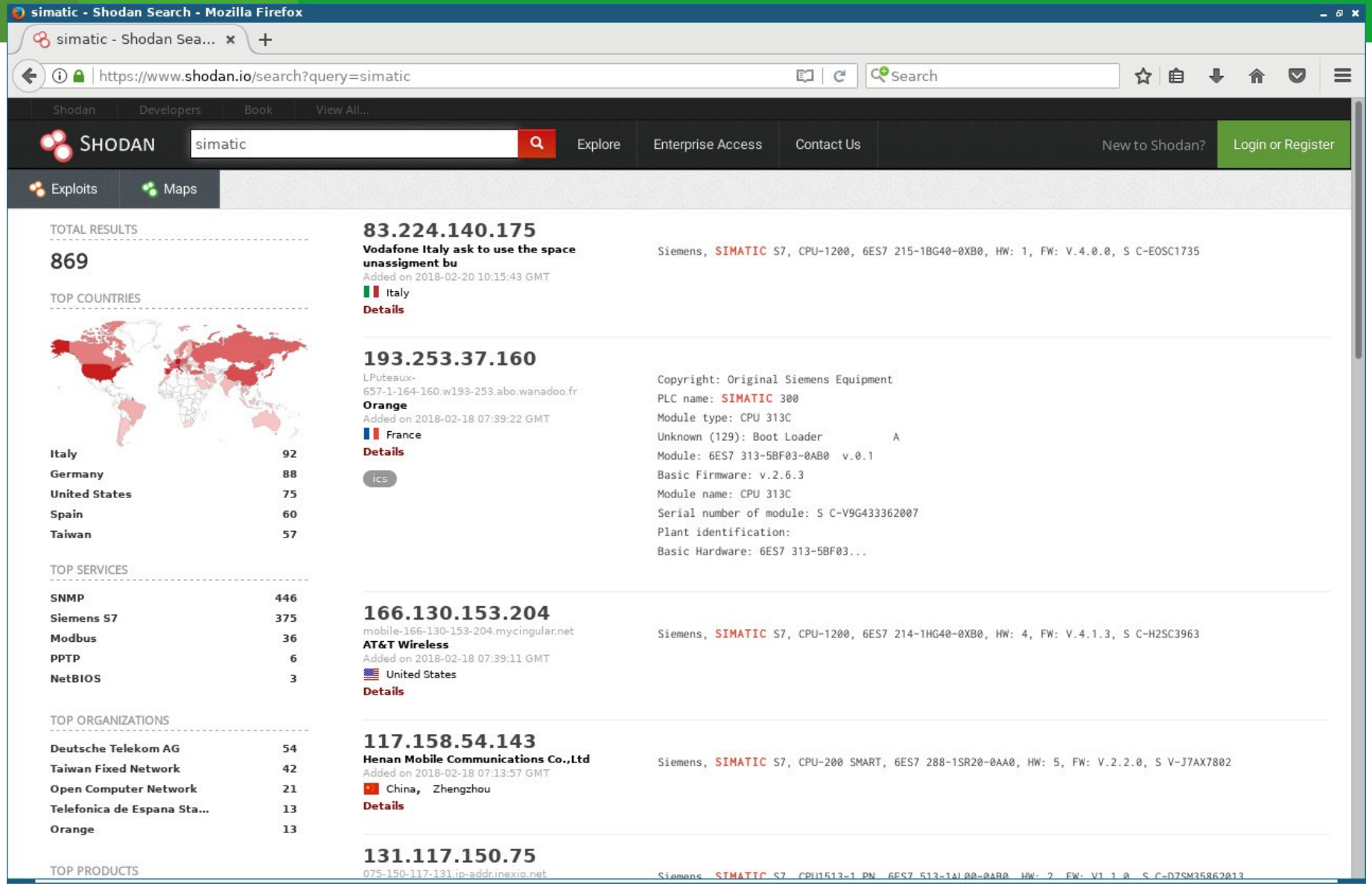
https://www.shodan.io/

Alcuni esempi..



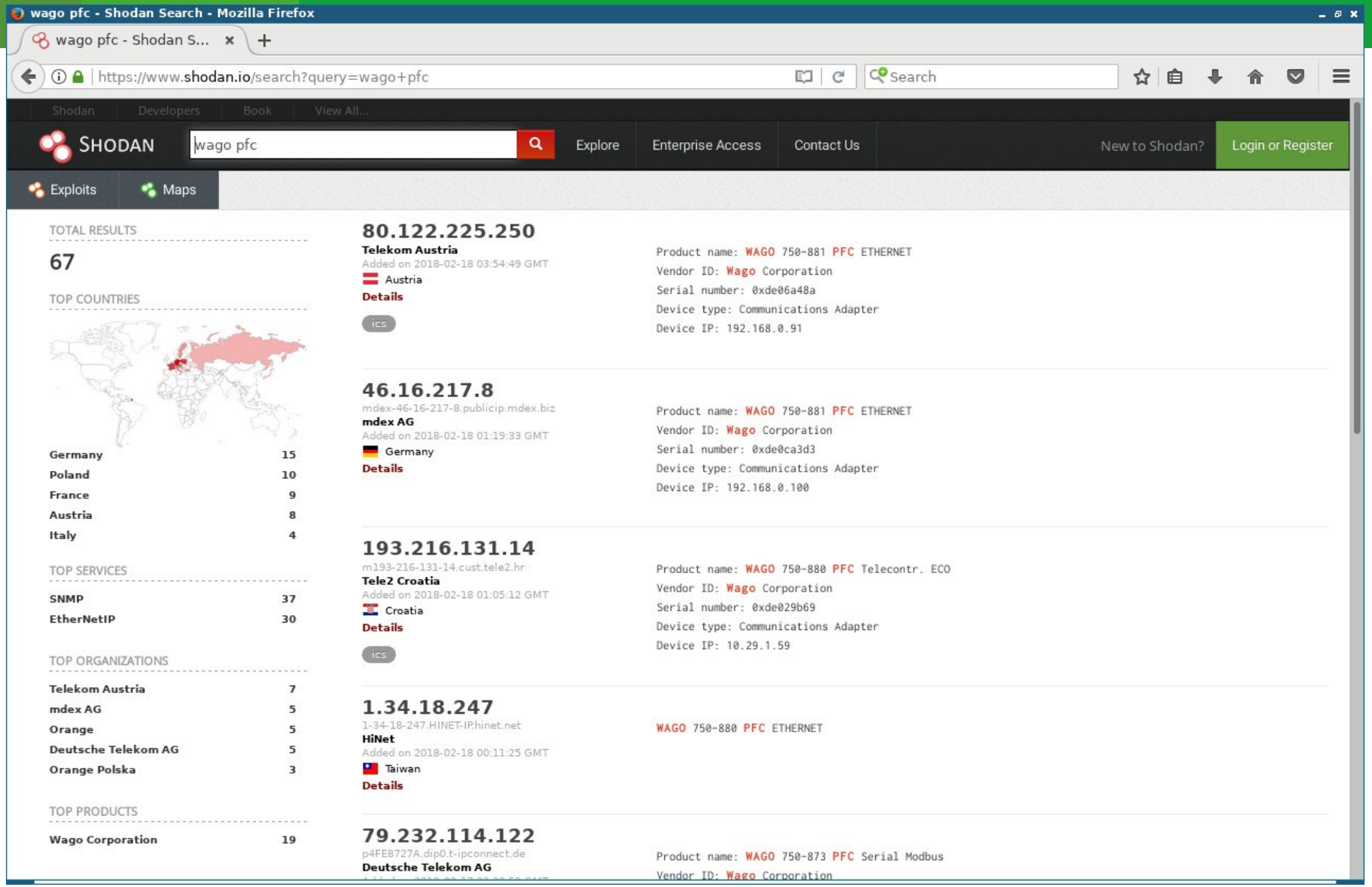
https://www.shodan.io/

Alcuni esempi..



https://www.shodan.io/

Alcuni esempi..



https://www.shodan.io/

“ma saranno dispositivi poco importanti..”

Power Plants and Other Vital Systems Are Totally Exposed on the Internet | WIRED - Mozilla Firefox

Power Plants and Oth...

https://www.wired.com/2013/11/internet-exposed/

Search

WIRED

Power Plants and Other Vital Systems Are Totally Exposed on the Internet

SIGN IN | SUBSCRIBE

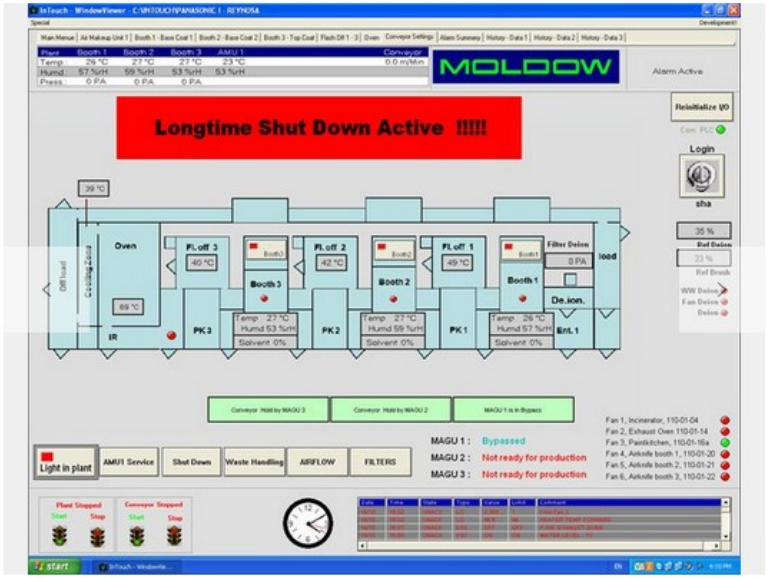
SHARE

SHARE 11

TWEET

COMMENT

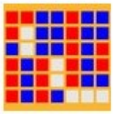
EMAIL



1 / 17 Equipment at a facility in Mexico appears to have been shut down for a while, based on the red banner at the top of the screen, but that wouldn't necessarily prevent intruders from manipulating the settings. It's unclear what the equipment is, but Moldow, based in Denmark, makes industrial filter and ventilation systems as well as industrial fans.

MOST POPULAR

BUSINESS
Facebook Executive Rob Goldman Apologizes After Russia Tweets
NICHOLAS THOMPSON



CULTURE
The Math Behind Pennsylvania's Gerrymandered Map
ISSIE LAPOWSKY

https://www.wired.com/2013/11/internet-exposed/

“ma a me non capiterà, non espongo ..”

Tesla's Cloud Hacked, Used to Mine Cryptocurrency - Mozilla Firefox

Tesla's Cloud Hacke...

https://gizmodo.com/teslas-cloud-hacked-used-to-mine-cryptocurrency-1823155247

Search

PRIVACY AND SECURITY

Tesla's Cloud Hacked, Used to Mine Cryptocurrency

Dell Cameron
Yesterday 11:05am • Filed to: TESLA

23.6K 21 4

Hackers infiltrated Tesla’s cloud environment and stole computer resources to mine for cryptocurrency, according to the security firm RedLock

Share Tweet

https://gizmodo.com/teslas-cloud-hacked-used-to-mine-cryptocurrency-1823155247

easynet group enforcer SECURITY

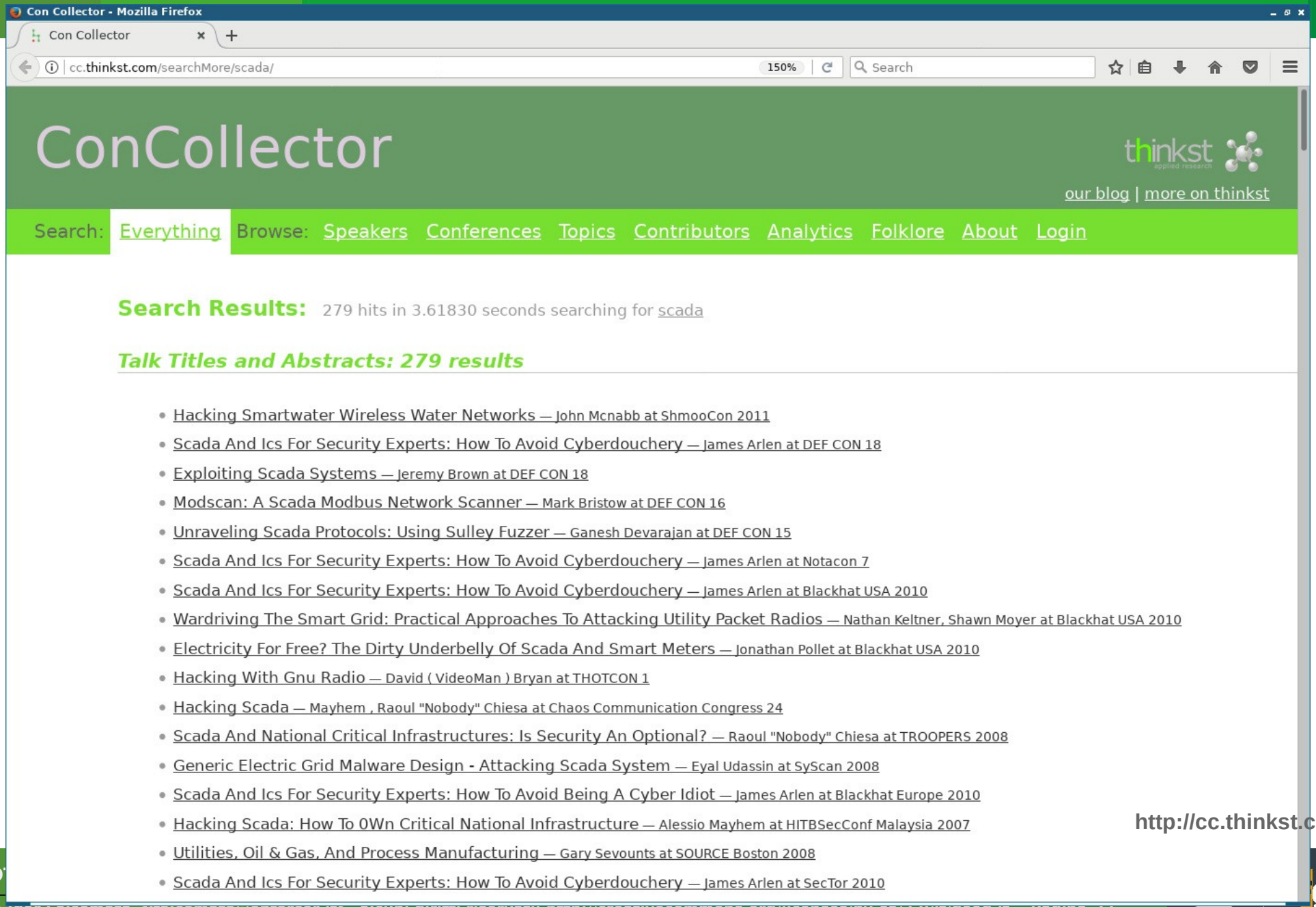
“ma a me non capiterà, non espongo ..”

- e i vostri fornitori?
  - sistemi di telecontrollo (Internet, 3/4G, ..)
  - “VpN”
  - infrastruttura Cloud
  - sicurezza della loro rete?

- e dal perimetro interno (LAN) ?

```
$ nmap -sS -p 22,23,80,443,502,1433,5900,..
```


Agli hacker SCADA piace..



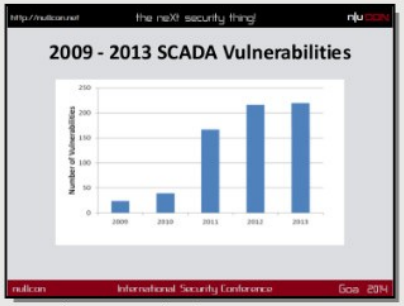
http://cc.thinkst.com/

.. vulnerabilità pubblicate

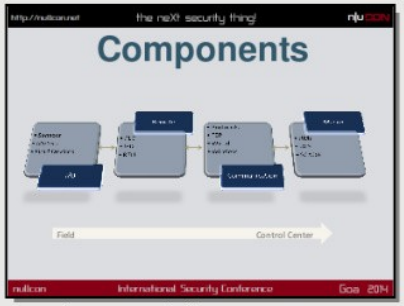
2014-The-year-in-which-we-cannot-ignore-SCADA-by-Amol-Sarwate
page 1

2014-The-year-in-which-we-cannot-ignore-SCADA-by-Amol-Sarwate
page 2


2014-The-year-in-which-we-cannot-ignore-SCADA-by-Amol-Sarwate
page 3



2014-The-year-in-which-we-cannot-ignore-SCADA-by-Amol-Sarwate
page 4



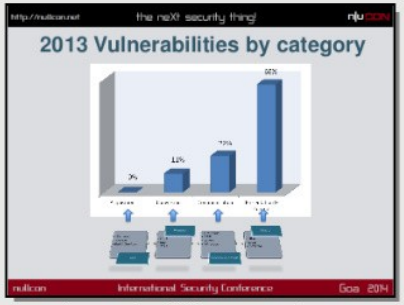
2014-The-year-in-which-we-cannot-ignore-SCADA-by-Amol-Sarwate
page 5

2014-The-year-in-which-we-cannot-ignore-SCADA-by-Amol-Sarwate
page 6

2014-The-year-in-which-we-cannot-ignore-SCADA-by-Amol-Sarwate
page 7

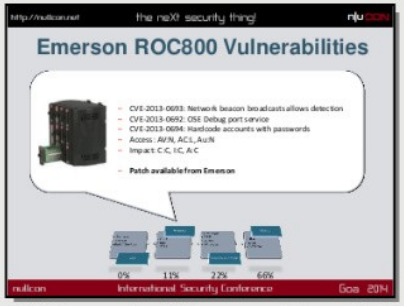
2014-The-year-in-which-we-cannot-ignore-SCADA-by-Amol-Sarwate
page 8

2014-The-year-in-which-we-cannot-ignore-SCADA-by-Amol-Sarwate
page 9

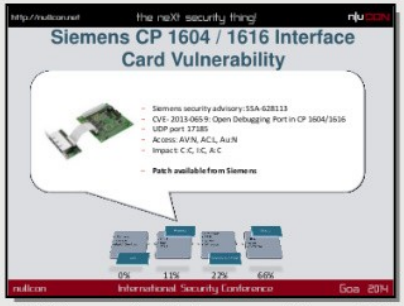


2014-The-year-in-which-we-cannot-ignore-SCADA-by-Amol-Sarwate
page 10

2014-The-year-in-which-we-cannot-ignore-SCADA-by-Amol-Sarwate
page 11

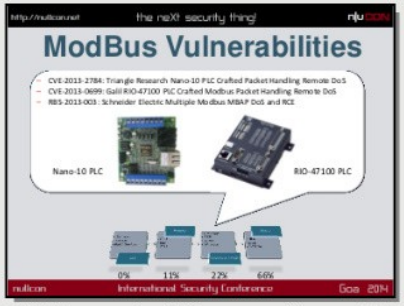


2014-The-year-in-which-we-cannot-ignore-SCADA-by-Amol-Sarwate
page 12



2014-The-year-in-which-we-cannot-ignore-SCADA-by-Amol-Sarwate
page 13

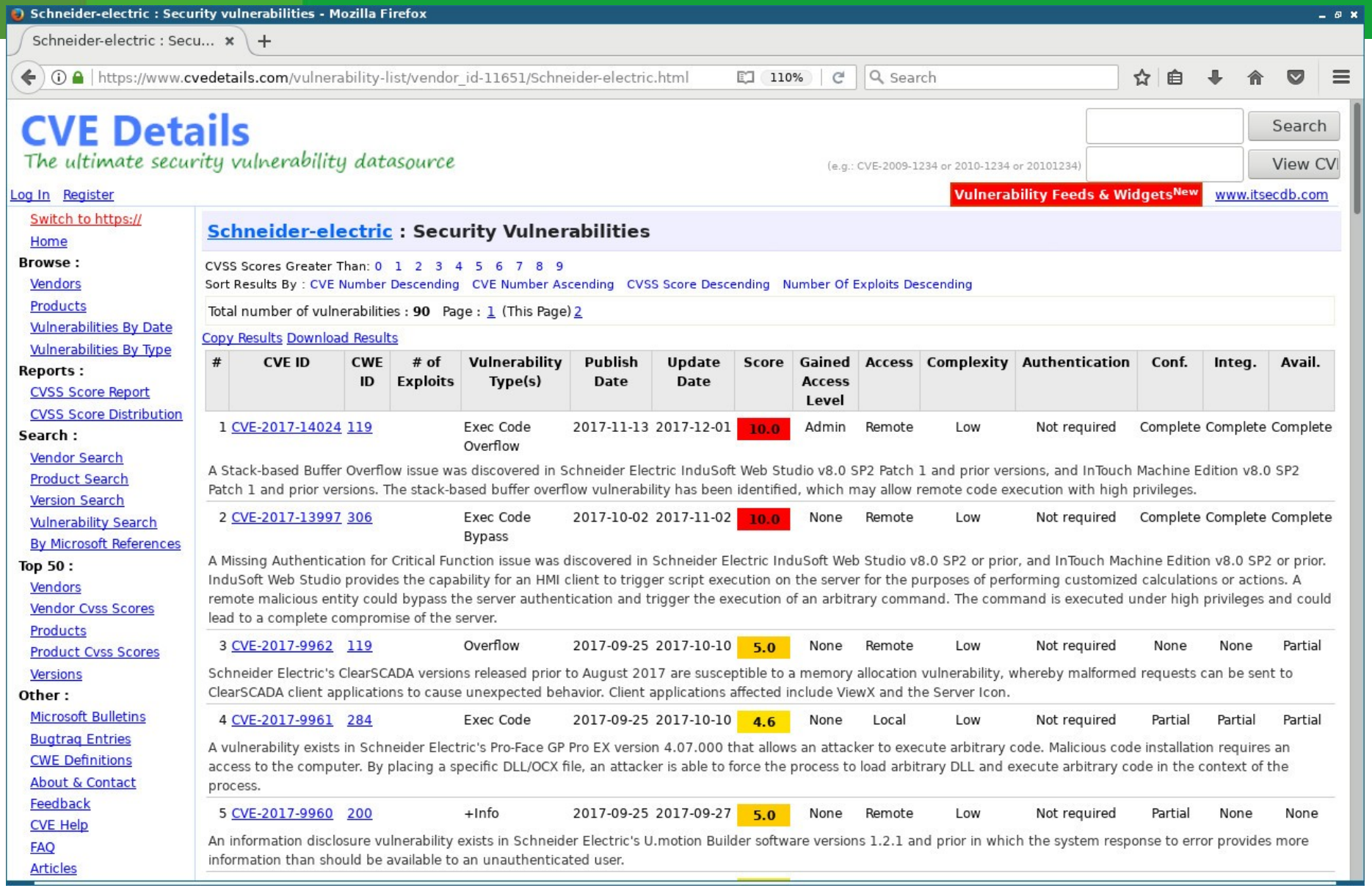
2014-The-year-in-which-we-cannot-ignore-SCADA-by-Amol-Sarwate
page 14



2014-The-year-in-which-we-cannot-ignore-SCADA-by-Amol-Sarwate
page 15

https://nullcon.net/website/archives/pdf/2014-The-year-in-which-we-cannot-ignore-SCADA-by-Amol-Sarwate.pdf

.. continuamente ..



Agenda

- Industry 4.0
- Quali sono i rischi?
- **Come proteggere i nostri impianti?**
- Riferimenti
- Q&A

Best practices

[ENISA]

Include security as a main consideration during the design phase of ICS/SCADA systems.

Traditionally, only safety is included as one of the main considerations during the design of the ICS/SCADA systems, infrastructures or assets (alongside efficiency, real-time constraints, etc.), but security was usually omitted. The objective is to ensure that security is included as one of these main considerations not only during the design phase but also during the update of the systems.

Communication network dependencies for ICS/SCADA Systems, pg. 8

Best practices

[ENISA]

Identify and establish roles of people operating in ICS/SCADA systems.

The management of the access privileges of users in ICS/SCADA systems is a critical process. The objective is to improve this process to ensure that the privilege assignation is adequately controlled and unauthorised access to systems, either intentional or accidental, is reduced to a minimum.

Communication network dependencies for ICS/SCADA Systems, pg. 8

Best practices

[ENISA]

Define network communication technologies and architecture with interoperability in mind.

As ICS/SCADA systems are becoming more interconnected with other systems, not only from the same organisation but also with external ones, interconnectivity and compatibility become critical factors.
The objective is to focus on promoting the use of common protocols and technologies that are compatible across different devices from multiple manufacturers, avoiding locked proprietary protocols and technologies.

Communication network dependencies for ICS/SCADA Systems, pg. 8

Best practices

[ENISA]

Establish brainstorming and communication channels for the different participants in the lifecycle of the devices to exchange needs and solutions.

Another point of concern is that there is usually a lack of communication between the different actors involved across the lifecycle of the ICS/SCADA
assets and devices. The need to improve between all these parties involved is a factor that would definitely improve the security of the systems, as needs and solutions would be shared across all.

Communication network dependencies for ICS/SCADA Systems, pg. 8

Best practices

[ENISA]

Include the periodic ICS/SCADA device update process as part of the main operations of the systems.

The process of updating the software and firmware of ICS/SCADA devices is a relatively new process, and a very delicate one. Traditionally, this was not needed as there was no interconnection and the threats were limited to physical tampering. Nowadays, the update process needs to be added as part of the lifecycle of the devices, including periodical update processes, to ensure that they are protected against the threats they are exposed to.

Communication network dependencies for ICS/SCADA Systems, pg. 8

Best practices

[ENISA]

Establish periodic ICS/SCADA security training and awareness campaign within the organisation.

The concept of cyber-security is relatively new in ICS/SCADA environments, as it was not needed traditionally. Therefore, there is a need to ensure that the staff is aware of the threats that they are exposed to on a daily basis, both in their operations and in the systems they operate with.

Communication network dependencies for ICS/SCADA Systems, pg. 8

Best practices

[ENISA]

Promote increased collaboration amongst policy decision makers, manufacturers and operators at an EU Level.

Nowadays, critical infrastructures have become linked with the cyberspace, taking advantage of the functionality and benefits it offers. However, this brings about the need to make critical systems and infrastructures safer and more reliable, in order to protect them from the new threats that have arisen from this new interconnectivity level. This also needs to be addressed by policy makers, manufacturers and operators in order to ensure that they are aligned with this objective.

Communication network dependencies for ICS/SCADA Systems, pg. 8

Best practices

[ENISA]

Define guidelines for the establishment of reliable and appropriate cybersecurity insurance requirements.

The critical infrastructures of the organisations are now more exposed than ever to threats and attackers worldwide due the use of network communications and the Internet. This leads to the appearance of insurance solutions to protect the assets in case of an incident. For this purpose, it is recommended to establish guidelines on proper insurance coverage to help both organisations and companies in providing and making use of these services.

Communication network dependencies for ICS/SCADA Systems, pg. 8

Figure 2: ISA95 levels applied to a SCADA architecture.

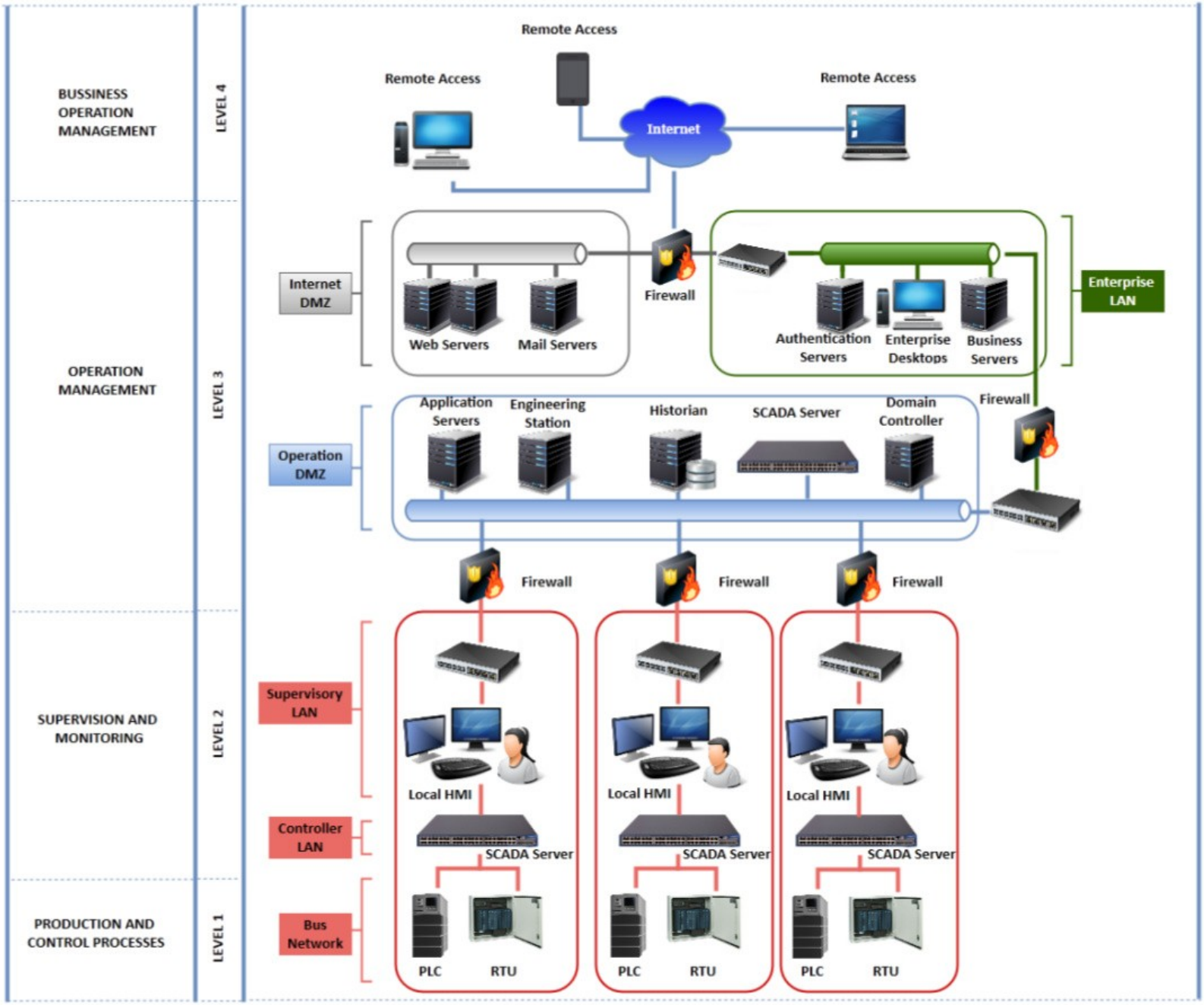


Image by ENISA, Communication network dependencies for ICS/SCADA Systems, pg. 17

Figure 2: ISA95 levels applied to a SCADA architecture.

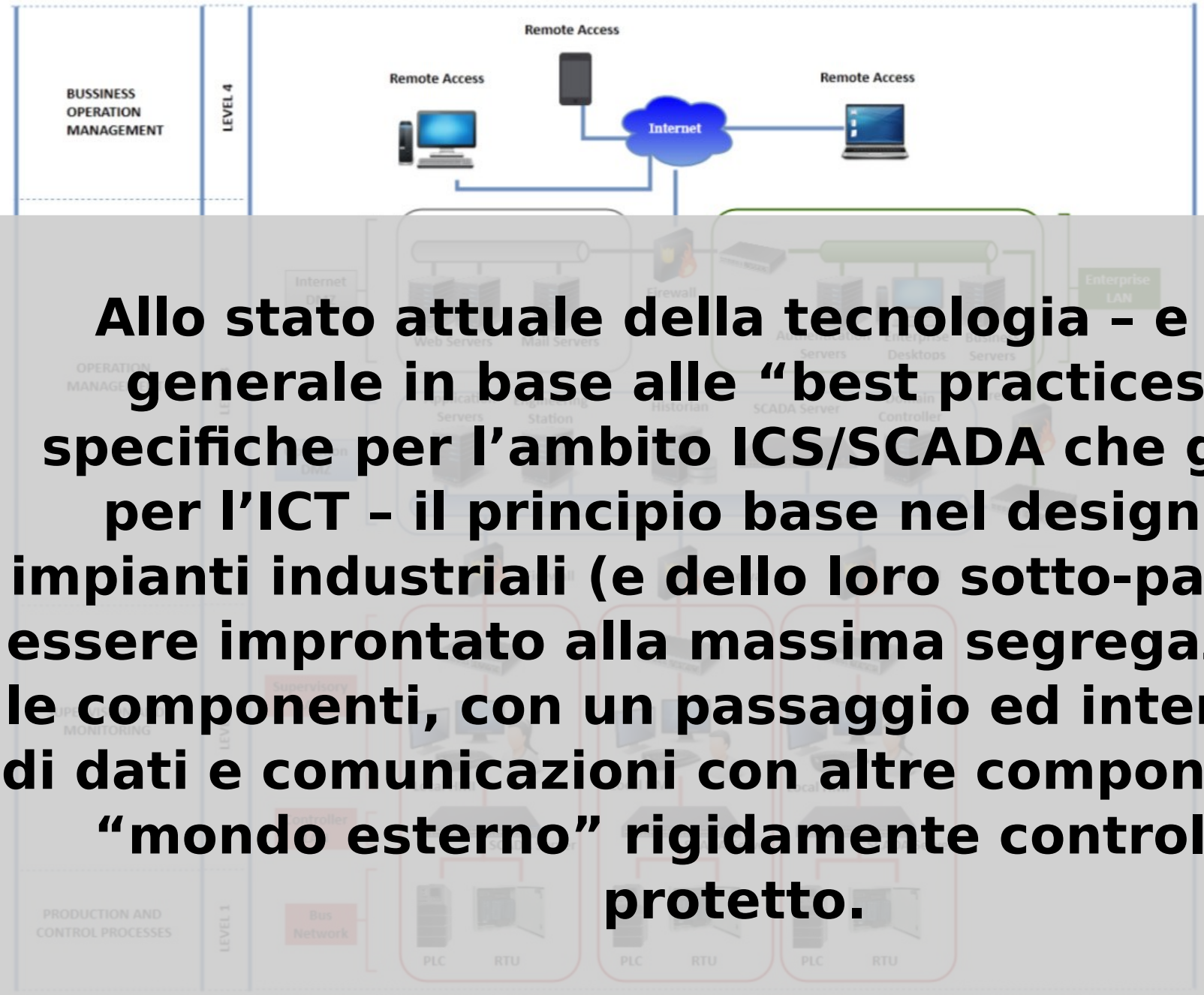


Image by ENISA, Communication network dependencies for ICS/SCADA Systems, pg. 17

Allo stato attuale della tecnologia – e più in generale in base alle "best practices" sia specifiche per l'ambito ICS/SCADA che generali per l'ICT – il principio base nel design degli impianti industriali (e dello loro sotto-parti) deve essere improntato alla massima segregazione tra le componenti, con un passaggio ed interscambio di dati e comunicazioni con altre componenti ed il "mondo esterno" rigidamente controllato e protetto.

Progettazione

- Security “by design” (linee guida..)
- Collaborazione con lo staff ICT
- Sicurezza fisica e logica
- Collaborazione con fornitori terzi (clausole contrattuali..)
- Audit e revisione..
- .. da una terza parte autorevole e indipendente

Messa in opera

- **Documentazione dettagliata asset**
- **Aggiornamenti (firmware, OS, applicazioni)**
- **Utenze (“di default” o “deboli”)**
- ***Hardening***
- **(Remote) management**
- **Monitoraggio e log management**

Particolare attenzione a..

- **Affidabilità (networking/apparati HA, ..)**
- **Ciclo di vita apparati**
- **Contratti di supporto hw/sw**
- **Copie di sicurezza config/dati**
- **Comunicazioni *wireless***
- ***(No) Internet***

Gestione della sicurezza

- **Business Impact Analysis**
- **Analisi del rischio (informatico)**
- **Analisi delle vulnerabilità**
- **Simulazione di attacco**
- **Analisi e risposta agli incidenti**

VA e PT

- **VA != PT**
- **Competenze specialistiche**
- **particolare “delicatezza” per ICS/SCADA**
- **Effettuato da una “terza parte”**

“Molti apparati industriali, soprattutto quelli più vecchi, potrebbero bloccarsi o funzionare in maniera inaspettata se sottoposti senza cautele alle tecniche di analisi delle vulnerabilità o simulazione di attacco utilizzate in ambito ICT.”

Industry 4.0 Insecurity

Agenda

- Industry 4.0
- Quali sono i rischi?
- Come proteggere i nostri impianti?
- **Riferimenti**
- **Q&A**

Riferimenti

Communication network dependencies for ICS/SCADA Systems (ENISA)
https://www.enisa.europa.eu/publications/ics-scada-dependencies

Guide to Industrial Control Systems (ICS) Security (NIST, SP-800-82 r2)
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Securing Industrial Control Systems-2017 (SANS Institute)
https://www.sans.org/reading-room/whitepapers/analyst/securing-industrial-control-systems-2017-37860

ISO/IEC 27001:2013
https://www.iso.org/standard/54534.html

CIS Critical Security Controls
https://www.sans.org/critical-security-controls

OWASP (Open Web Application Security Consortium)
https://www.owasp.org/

Domande ?