Ivera Kenniscafe

27 September 2023

Who are we…

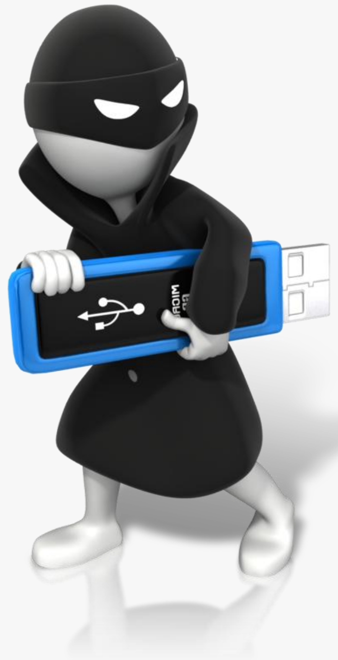
Willy
Leuvering

ISA-62443 SME
ISA-95 SME
ISA-88 SME

RvA Technical
Assessor

ISA-62443 SME
EN 50518

CCNA
Siemens Scalance
Ethical Hacker



Joshua
Smits

Cybersecurity Myths in OT

*“Why **we** do not need cybersecurity…”*

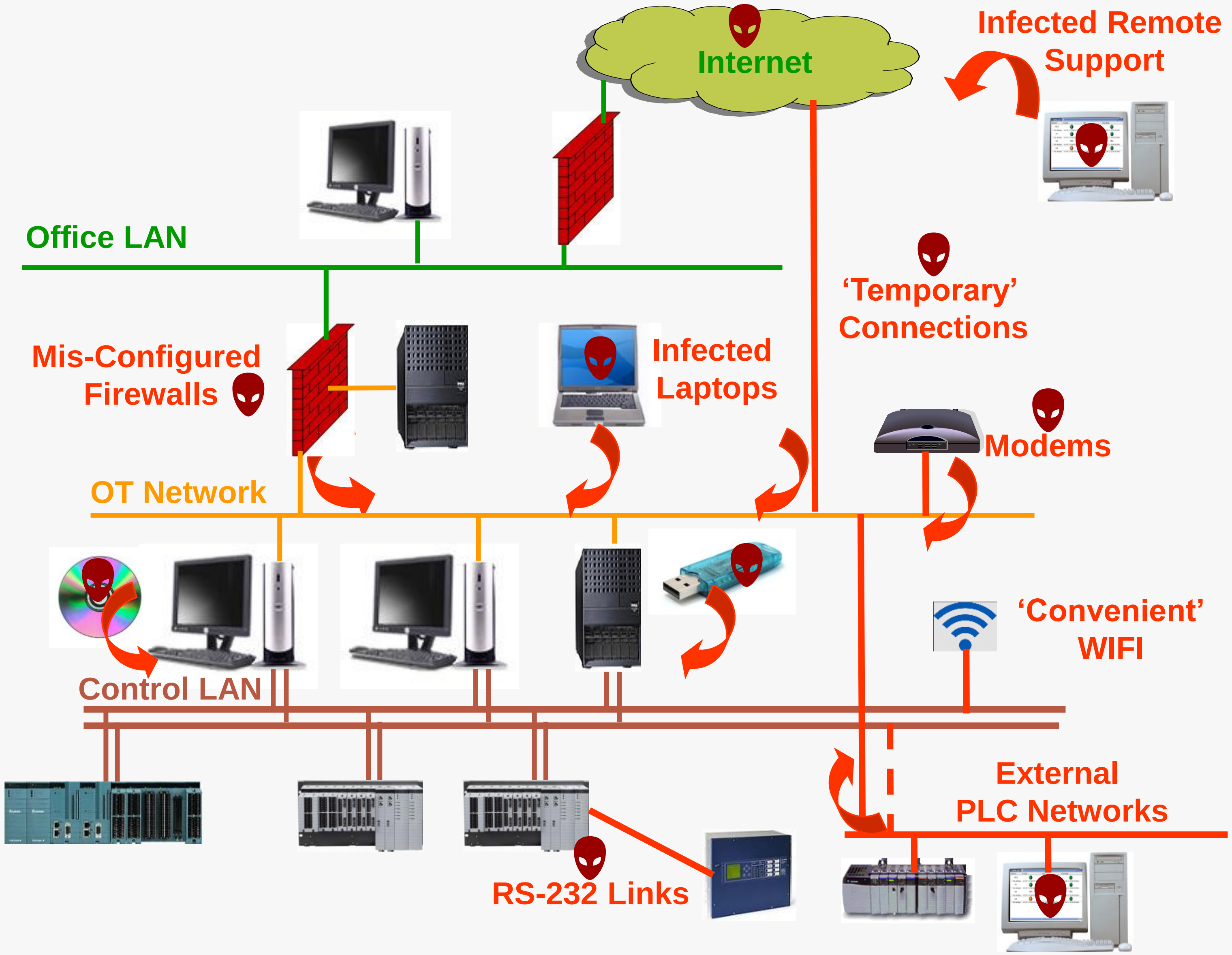
Common Cyber Myths

- We don’t connect to the Internet
- Hackers don’t understand control systems
- Cyber security only costs money

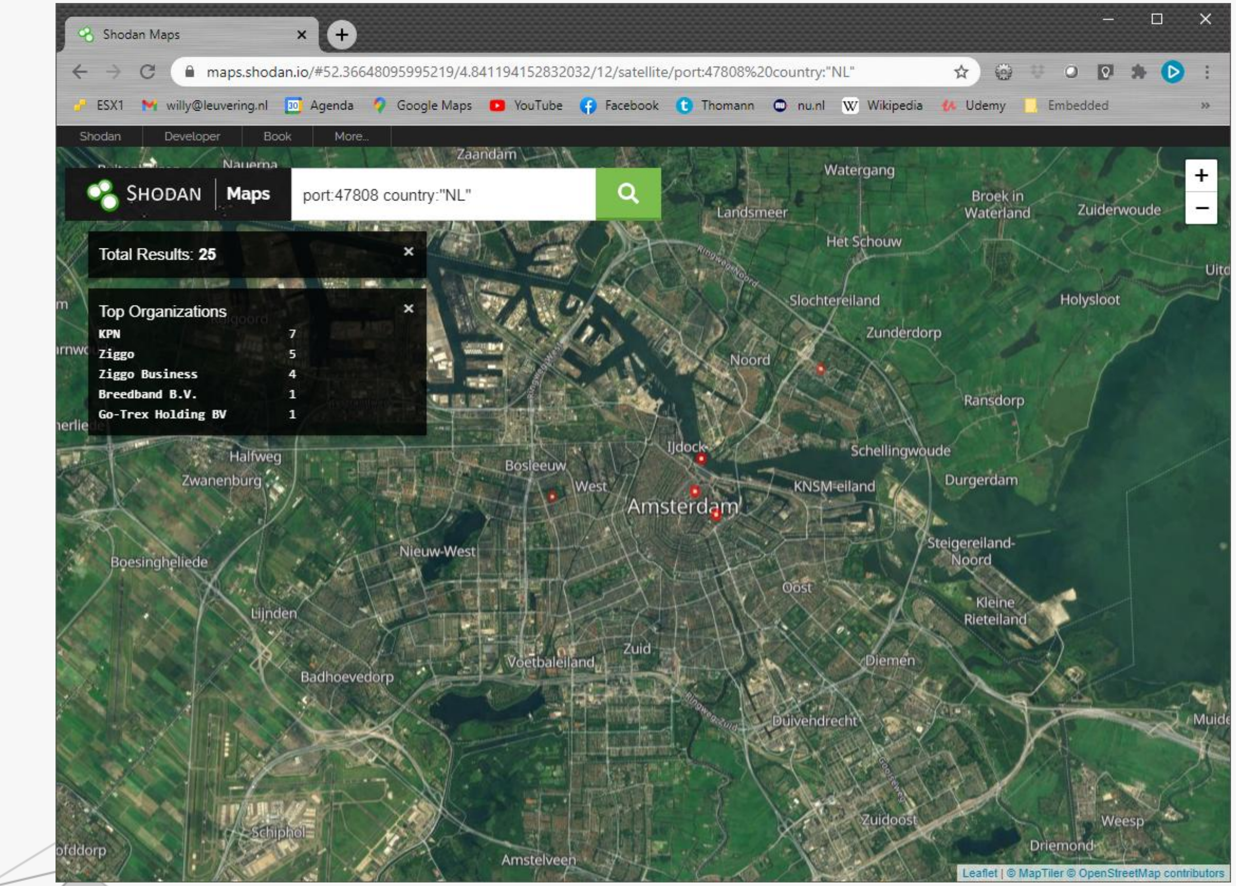
We don’t connect to the internet

“Our systems are behind an expensive firewall…”

“Our systems are air-gapped…”


Internet
Infected Remote Support
Office LAN
'Temporary' Connections
Mis-Configured Firewalls
Infected Laptops
Modems
OT Network
'Convenient' WIFI
Control LAN
External PLC Networks
RS-232 Links

https://shodan.io



Shodan Maps

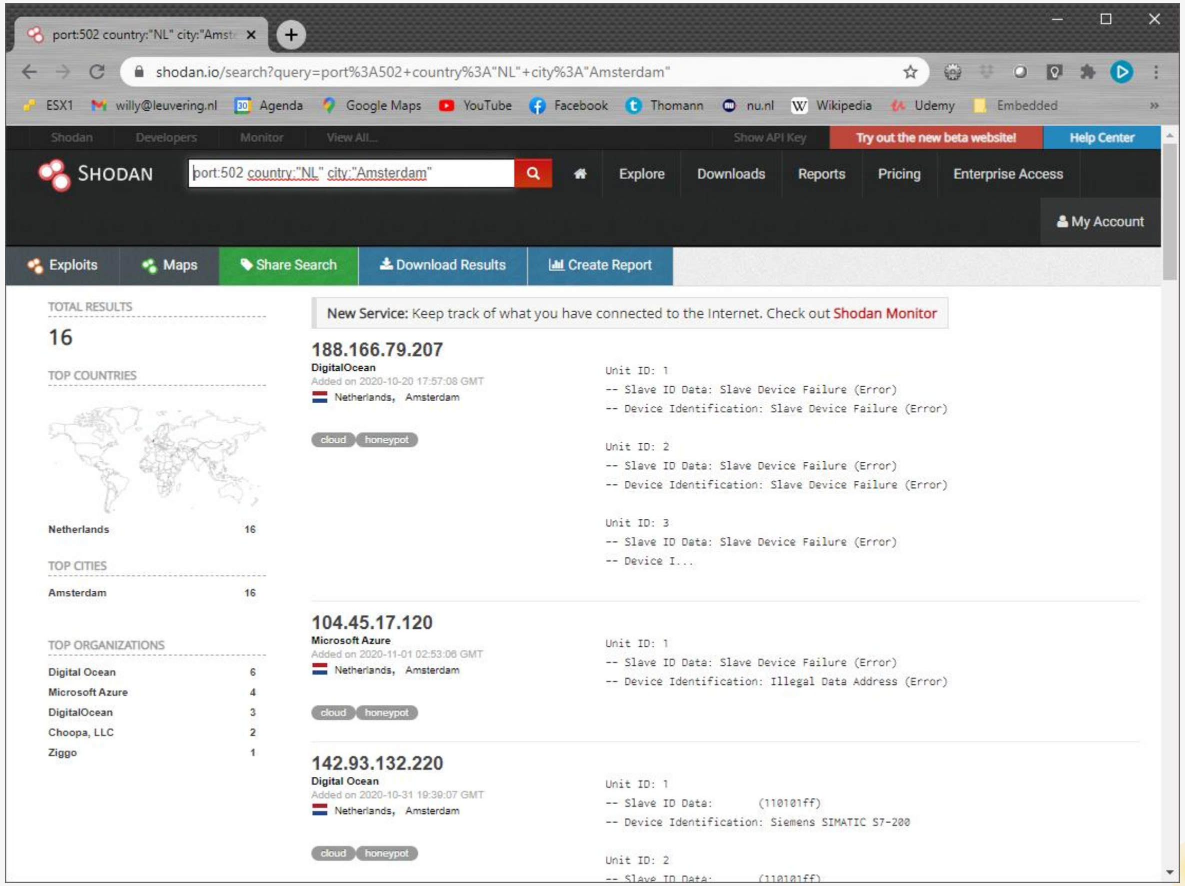
maps.shodan.io/#52.36648095995219/4.841194152832032/12/satellite/port:47808%20country:"NL"

port:47808 country:"NL"

Total Results: 25

Top Organizations

KPN	7
Ziggo	5
Ziggo Business	4
Breedband B.V.	1
Go-Trex Holding BV	1



port:502 country:"NL" city:"Amst

shodan.io/search?query=port%3A502+country%3A"NL"+city%3A"Amsterdam"

port:502 country:"NL" city:"Amsterdam"

TOTAL RESULTS

16

TOP COUNTRIES

Netherlands	16

TOP CITIES

Amsterdam	16

TOP ORGANIZATIONS

Digital Ocean	6
Microsoft Azure	4
DigitalOcean	3
Choopa, LLC	2
Ziggo	1

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

188.166.79.207
DigitalOcean
Added on 2020-10-20 17:57:08 GMT
Netherlands, Amsterdam
cloud honeypot

```
Unit ID: 1
-- Slave ID Data: Slave Device Failure (Error)
-- Device Identification: Slave Device Failure (Error)

Unit ID: 2
-- Slave ID Data: Slave Device Failure (Error)
-- Device Identification: Slave Device Failure (Error)

Unit ID: 3
-- Slave ID Data: Slave Device Failure (Error)
-- Device I...
```

104.45.17.120
Microsoft Azure
Added on 2020-11-01 02:53:06 GMT
Netherlands, Amsterdam
cloud honeypot

```
Unit ID: 1
-- Slave ID Data: Slave Device Failure (Error)
-- Device Identification: Illegal Data Address (Error)
```

142.93.132.220
Digital Ocean
Added on 2020-10-31 19:39:07 GMT
Netherlands, Amsterdam
cloud honeypot

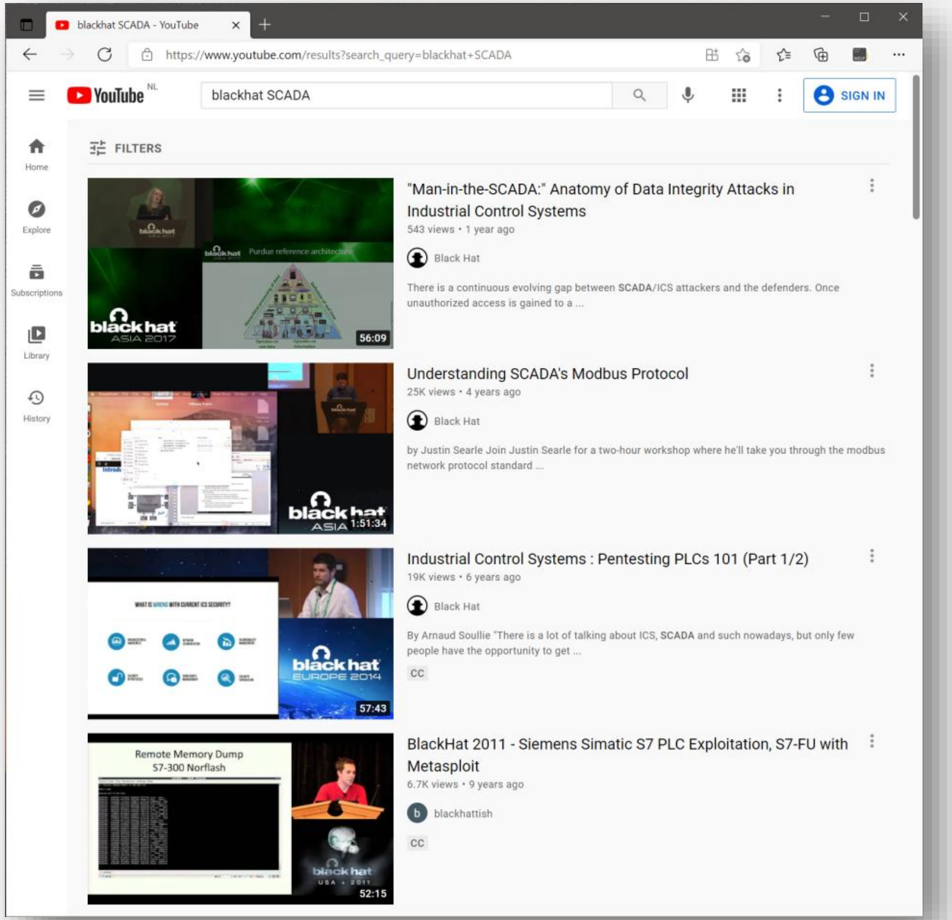
```
Unit ID: 1
-- Slave ID Data:       (110101ff)
-- Device Identification: Siemens SIMATIC S7-200

Unit ID: 2
-- Slave ID Data:       (110101ff)
```

Hackers Don’t Understand OT Systems

“It is complicated and very specialized…”

University of YouTube

- OT is using more COTS technology
- Cyber crime is a business model
  - OT uses legacy hard- and software
  - OT thinks they do not need cyber security
  - Loss of Production is expensive
- Stealing Intellectual Property (IP)
- Terrorist Attacks on Critical National Infrastructure



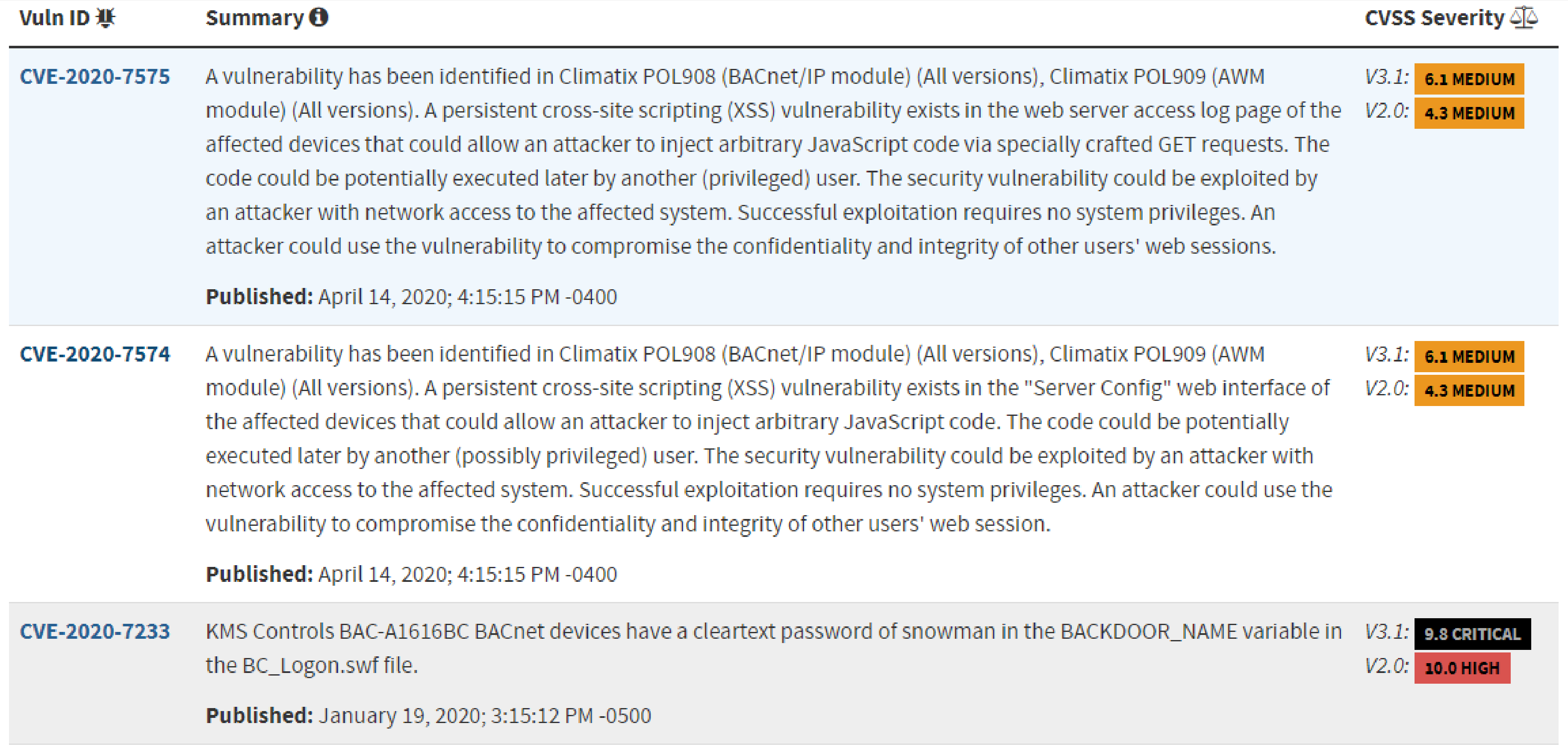
"Man-in-the-SCADA:" Anatomy of Data Integrity Attacks in Industrial Control Systems
543 views • 1 year ago
Black Hat
There is a continuous evolving gap between SCADA/ICS attackers and the defenders. Once unauthorized access is gained to a ...

Understanding SCADA's Modbus Protocol
25K views • 4 years ago
Black Hat
by Justin Searle Join Justin Searle for a two-hour workshop where he'll take you through the modbus network protocol standard ...

Industrial Control Systems : Pentesting PLCs 101 (Part 1/2)
19K views • 6 years ago
Black Hat
By Arnaud Soullie "There is a lot of talking about ICS, SCADA and such nowadays, but only few people have the opportunity to get ...

BlackHat 2011 - Siemens Simatic S7 PLC Exploitation, S7-FU with Metasploit
6.7K views • 9 years ago
blackhattish

We publish vulnerabilities

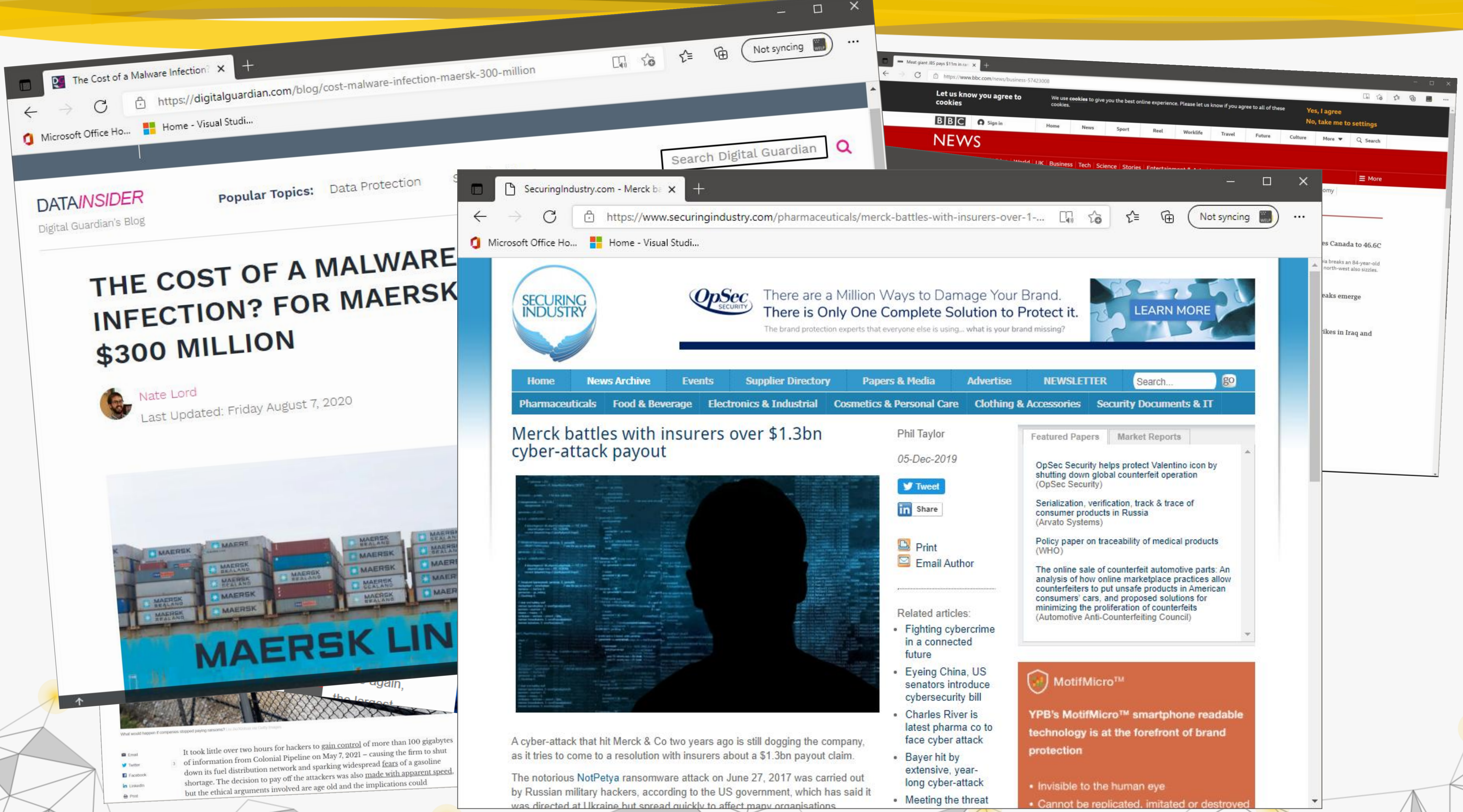


Vuln ID	Summary	CVSS Severity
CVE-2020-7575	A vulnerability has been identified in Climatix POL908 (BACnet/IP module) (All versions), Climatix POL909 (AWM module) (All versions). A persistent cross-site scripting (XSS) vulnerability exists in the web server access log page of the affected devices that could allow an attacker to inject arbitrary JavaScript code via specially crafted GET requests. The code could be potentially executed later by another (privileged) user. The security vulnerability could be exploited by an attacker with network access to the affected system. Successful exploitation requires no system privileges. An attacker could use the vulnerability to compromise the confidentiality and integrity of other users' web sessions. **Published:** April 14, 2020; 4:15:15 PM -0400	*V3.1:* 6.1 MEDIUM *V2.0:* 4.3 MEDIUM
CVE-2020-7574	A vulnerability has been identified in Climatix POL908 (BACnet/IP module) (All versions), Climatix POL909 (AWM module) (All versions). A persistent cross-site scripting (XSS) vulnerability exists in the "Server Config" web interface of the affected devices that could allow an attacker to inject arbitrary JavaScript code. The code could be potentially executed later by another (possibly privileged) user. The security vulnerability could be exploited by an attacker with network access to the affected system. Successful exploitation requires no system privileges. An attacker could use the vulnerability to compromise the confidentiality and integrity of other users' web session. **Published:** April 14, 2020; 4:15:15 PM -0400	*V3.1:* 6.1 MEDIUM *V2.0:* 4.3 MEDIUM
CVE-2020-7233	KMS Controls BAC-A1616BC BACnet devices have a cleartext password of snowman in the BACKDOOR_NAME variable in the BC_Logon.swf file. **Published:** January 19, 2020; 3:15:12 PM -0500	*V3.1:* 9.8 CRITICAL *V2.0:* 10.0 HIGH

Source: https://nvd.nist.gov/

Cyber Security only costs money

“There is no Return-On-Investment …”



THE COST OF A MALWARE INFECTION? FOR MAERSK $300 MILLION

Nate Lord

Last Updated: Friday August 7, 2020

What would happen if companies stopped paying ransoms? Liu Jie/Xinhua via Getty Images

It took little over two hours for hackers to gain control of more than 100 gigabytes of information from Colonial Pipeline on May 7, 2021 – causing the firm to shut down its fuel distribution network and sparking widespread fears of a gasoline shortage. The decision to pay off the attackers was also made with apparent speed, but the ethical arguments involved are age old and the implications could

Let us know you agree to cookies

We use cookies to give you the best online experience. Please let us know if you agree to all of these cookies.

Yes, I agree

No, take me to settings

es Canada to 46.6C

ia breaks an 84-year-old north-west also sizzles.

eaks emerge

ikes in Iraq and

OpSec SECURITY There are a Million Ways to Damage Your Brand. There is Only One Complete Solution to Protect it. The brand protection experts that everyone else is using... what is your brand missing?

Merck battles with insurers over $1.3bn cyber-attack payout

Phil Taylor

05-Dec-2019

A cyber-attack that hit Merck & Co two years ago is still dogging the company, as it tries to come to a resolution with insurers about a $1.3bn payout claim.

The notorious NotPetya ransomware attack on June 27, 2017 was carried out by Russian military hackers, according to the US government, which has said it was directed at Ukraine but spread quickly to affect many organisations

Related articles:

- Fighting cybercrime in a connected future
- Eyeing China, US senators introduce cybersecurity bill
- Charles River is latest pharma co to face cyber attack
- Bayer hit by extensive, year-long cyber-attack
- Meeting the threat

OpSec Security helps protect Valentino icon by shutting down global counterfeit operation (OpSec Security)

Serialization, verification, track & trace of consumer products in Russia (Arvato Systems)

Policy paper on traceability of medical products (WHO)

The online sale of counterfeit automotive parts: An analysis of how online marketplace practices allow counterfeiters to put unsafe products in American consumers' cars, and proposed solutions for minimizing the proliferation of counterfeits (Automotive Anti-Counterfeiting Council)

MotifMicro™

YPB's MotifMicro™ smartphone readable technology is at the forefront of brand protection

- Invisible to the human eye
- Cannot be replicated, imitated or destroyed

Defense in Depth

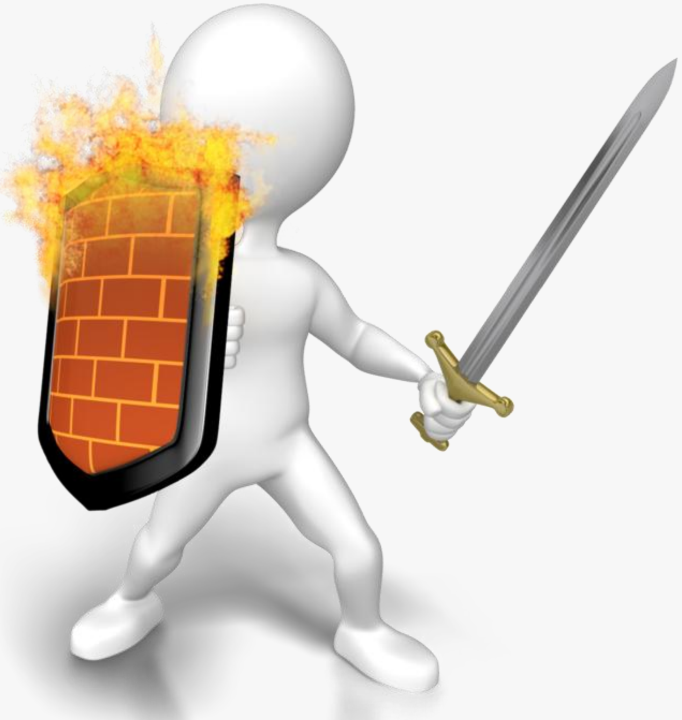
Segments – Firewalls – IDS – VPN

Defense in Depth

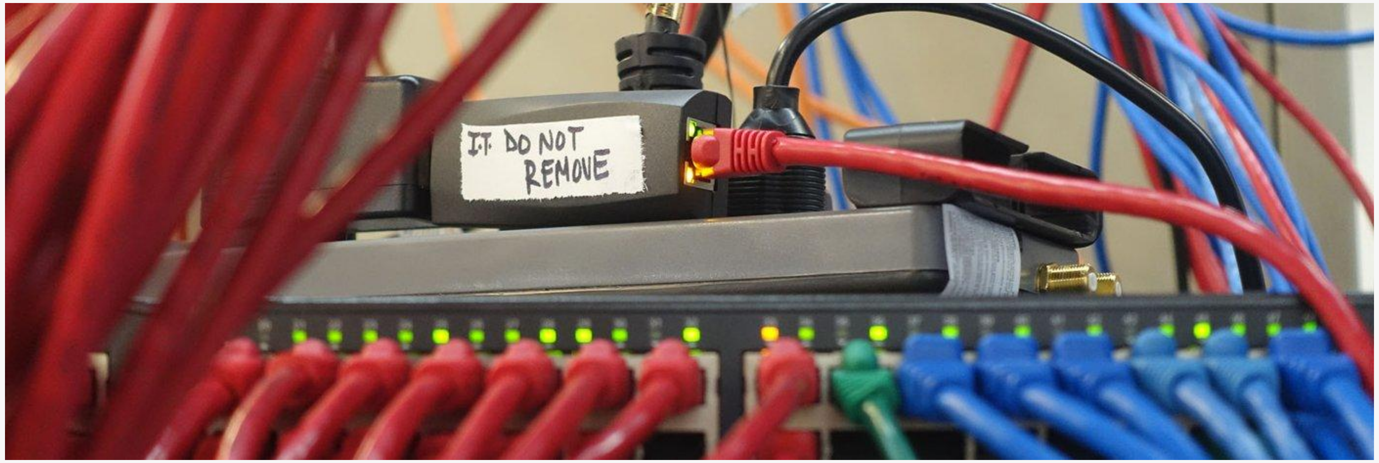
Deter-Deny-Detect-Delay-Defeat

Cyberwar: Protect using the 5 D’s from the military

Physical – Procedural - Network



Physical Security



Network Implants

Disgruntled Employees

Policies and Procedures

- Awareness
- Use of strong Passwords
- Least Privilege
- Separation / Segregation of Duties
- Temporary Devices
  - USB
  - Laptops

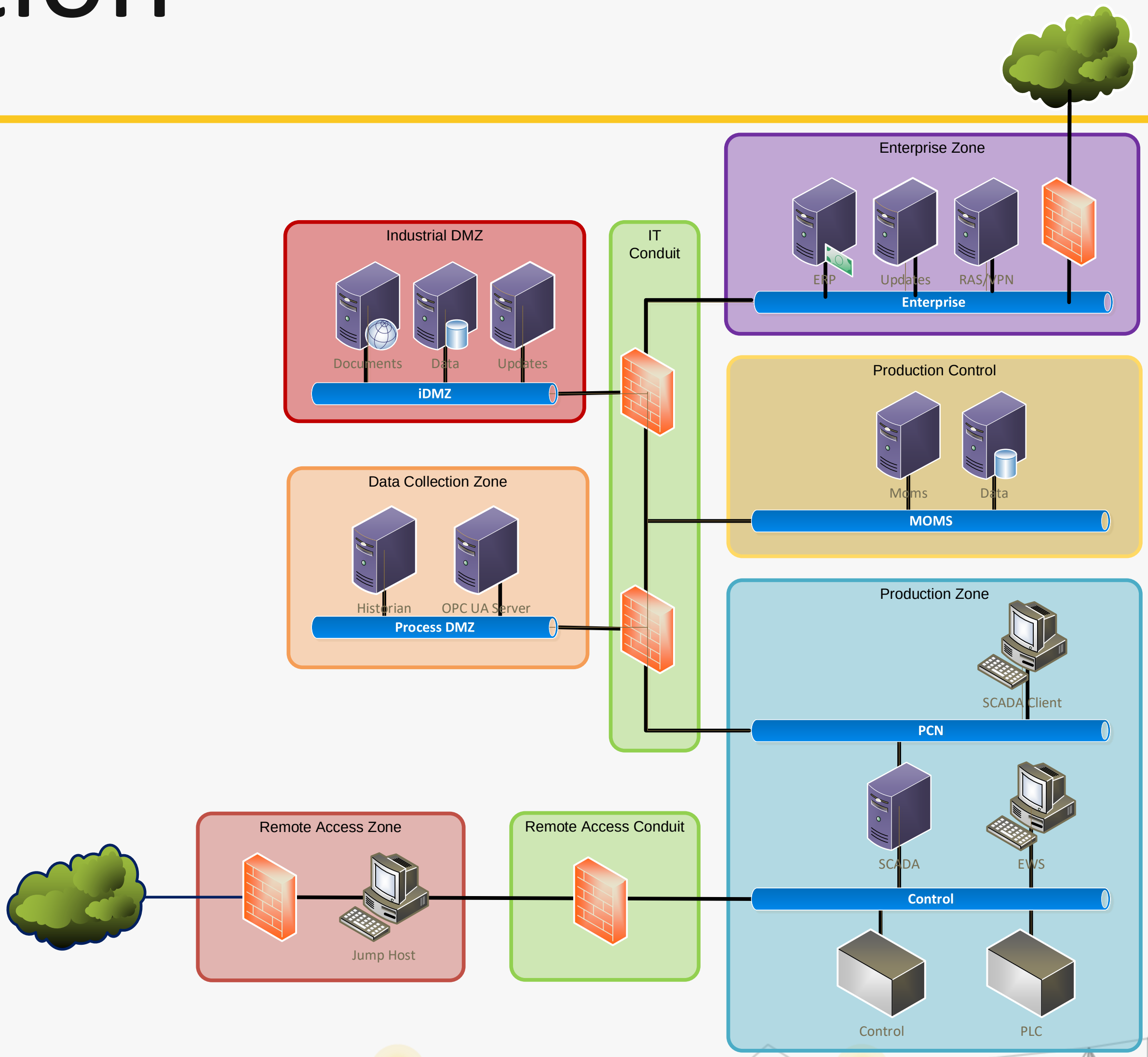
Network Security

- Network Segmentation
- Firewalls
- VPN
- Malware Prevention
- IDS – SIEM

Network Segmentation

- Zones and Conduits
  - Separate Business vs Control
  - Separate Safety
  - Separate Wireless
  - Separate Temporary Connected Devices
  - Separate Untrusted Networks

- Multiple Segments per Zone
- Multiple Functionality per Zone



Firewall

- Restricted Data Flow
- Rules
  - MAC / IP Address / Range
  - Port Number(s)
  - Direction (In – Out)
- Stateful Inspection
  - Sequence of the packets
- Protocol Inspection
  - Deep Packet Inspection (DPI)
  - Proxy Server

Virtual Private Network

- Using public telecom network
  - The Internet
  - POTS

- Secure – Private Connection

- Site to Site

- Remote Access Services (RAS)

Malware – Antivirus

- Bad-listing
  - Known bad programs (signatures).
  - Known bad behavior.
  - Long list, keeps growing.

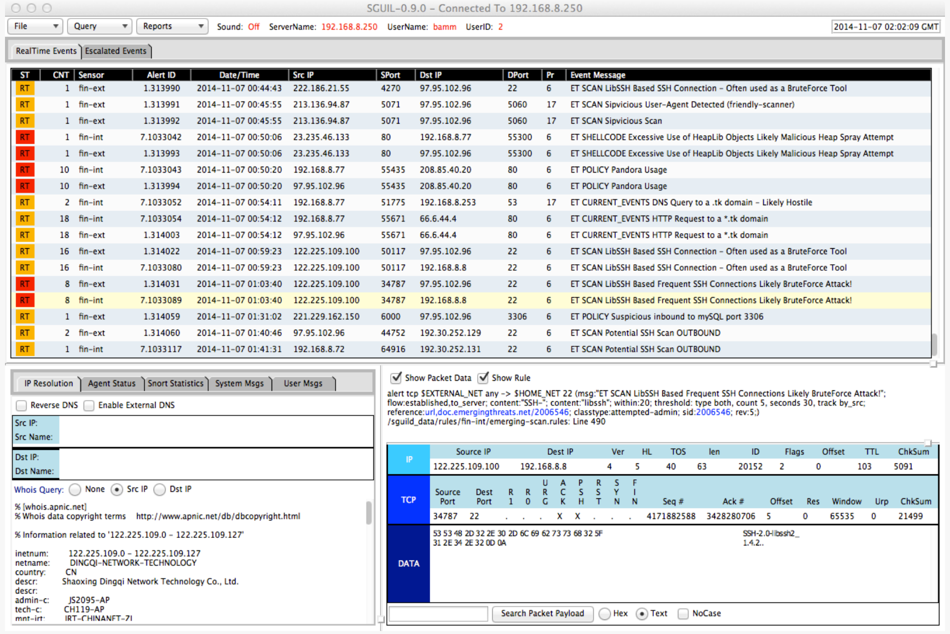
- Good-listing
  - Only good programs are allowed to start.
  - Zero-day protection.
  - Harder to install updates and new programs.

- Endpoint Protection / Endpoint Detection and Response (EDR)

IDS - SIEM

- Intrusion Detection Systems
  - “If a firewall is the lock on the door, the IDS is the burglar alarm”
  - Signature, Behavior, Anomaly

- Security Information Event Management
  - Events and logfiles from:
    - IDS
    - Firewall
    - Operating Systems
    - Network Devices
    - etc



ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	fin-ext	1.313990	2014-11-07 00:44:43	222.186.21.55	4270	97.95.102.96	22	6	ET SCAN LibSSH Based SSH Connection – Often used as a BruteForce Tool
RT	1	fin-ext	1.313991	2014-11-07 00:45:55	213.136.94.87	5071	97.95.102.96	5060	17	ET SCAN Sipvicious User-Agent Detected (friendly-scanner)
RT	1	fin-ext	1.313992	2014-11-07 00:45:55	213.136.94.87	5071	97.95.102.96	5060	17	ET SCAN Sipvicious Scan
RT	1	fin-int	7.1033042	2014-11-07 00:50:06	23.235.46.133	80	192.168.8.77	55300	6	ET SHELLCODE Excessive Use of HeapLib Objects Likely Malicious Heap Spray Attempt
RT	1	fin-ext	1.313993	2014-11-07 00:50:06	23.235.46.133	80	97.95.102.96	55300	6	ET SHELLCODE Excessive Use of HeapLib Objects Likely Malicious Heap Spray Attempt
RT	10	fin-int	7.1033043	2014-11-07 00:50:20	192.168.8.77	55435	208.85.40.20	80	6	ET POLICY Pandora Usage
RT	10	fin-ext	1.313994	2014-11-07 00:50:20	97.95.102.96	55435	208.85.40.20	80	6	ET POLICY Pandora Usage
RT	2	fin-int	7.1033052	2014-11-07 00:54:11	192.168.8.77	51775	192.168.8.253	53	17	ET CURRENT_EVENTS DNS Query to a .tk domain – Likely Hostile
RT	18	fin-int	7.1033054	2014-11-07 00:54:12	192.168.8.77	55671	66.6.44.4	80	6	ET CURRENT_EVENTS HTTP Request to a *.tk domain
RT	18	fin-ext	1.314003	2014-11-07 00:54:12	97.95.102.96	55671	66.6.44.4	80	6	ET CURRENT_EVENTS HTTP Request to a *.tk domain
RT	16	fin-ext	1.314022	2014-11-07 00:59:23	122.225.109.100	50117	97.95.102.96	22	6	ET SCAN LibSSH Based SSH Connection – Often used as a BruteForce Tool
RT	16	fin-int	7.1033080	2014-11-07 00:59:23	122.225.109.100	50117	192.168.8.8	22	6	ET SCAN LibSSH Based SSH Connection – Often used as a BruteForce Tool
RT	8	fin-ext	1.314031	2014-11-07 01:03:40	122.225.109.100	34787	97.95.102.96	22	6	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack!
RT	8	fin-int	7.1033089	2014-11-07 01:03:40	122.225.109.100	34787	192.168.8.8	22	6	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack!
RT	1	fin-ext	1.314059	2014-11-07 01:31:02	221.229.162.150	6000	97.95.102.96	3306	6	ET POLICY Suspicious inbound to mySQL port 3306
RT	2	fin-ext	1.314060	2014-11-07 01:40:46	97.95.102.96	44752	192.30.252.129	22	6	ET SCAN Potential SSH Scan OUTBOUND
RT	1	fin-int	7.1033117	2014-11-07 01:41:31	192.168.8.72	64916	192.30.252.131	22	6	ET SCAN Potential SSH Scan OUTBOUND

□ Reverse DNS □ Enable External DNS

Src IP:
Src Name:

Dst IP:
Dst Name:

Whois Query: ○ None ● Src IP ○ Dst IP

```
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to '122.225.109.0 - 122.225.109.127'

inetnum:        122.225.109.0 - 122.225.109.127
netname:        DINGQI-NETWORK-TECHNOLOGY
country:        CN
descr:          Shaoxing Dingqi Network Technology Co., Ltd.
descr:
admin-c:        JS2095-AP
tech-c:         CH119-AP
mnt-irt:        IRT-CHINANET-ZJ
```

☑ Show Packet Data ☑ Show Rule

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 22 (msg:"ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack!";
flow:established,to_server; content:"SSH-"; content:"libssh"; within:20; threshold: type both, count 5, seconds 30, track by_src;
reference:url,doc.emergingthreats.net/2006546; classtype:attempted-admin; sid:2006546; rev:5;)
/sguild_data/rules/fin-int/emerging-scan.rules: Line 490
```

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
	122.225.109.100	192.168.8.8	4	5	40	63	20152	2	0	103	5091

TCP	Source Port	Dest Port	R 1	R 0	URG	ACK	PSH	RST	SYN	FIN	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
	34787	22	.	.	.	X	X	.	.	.	4171882588	3428280706	5	0	65535	0	21499

DATA

```
53 53 48 2D 32 2E 30 2D 6C 69 62 73 73 68 32 5F     SSH-2.0-libssh2_
31 2E 34 2E 32 0D 0A                                1.4.2..
```

Search Packet Payload ○ Hex ● Text □ NoCase

Network Information Security Directive 2
NIS2

European Regulations

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

L 333/80 EN Official Journal of the European Union 27.12.2022

DIRECTIVES

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 December 2022

on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

7.6.2019 EN Official Journal of the European Union L 151/15

REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 17 April 2019

on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

(Text with EEA relevance)

ND THE COUNCIL OF THE EUROPEAN UNION,

the Functioning of the European Union, and in particular Article 114 thereof,

m the European Commission,

lative act to the national parliaments,

European Economic and Social Committee ([1]),

ommittee of the Regions ([2]),

legislative procedure ([3]),

Highlights

- ENISA: European Union Agency for Cyber Security

- Create an overall higher level of cybersecurity in the EU
- Report incidents to Cyber Security Incident Response Teams (CSIRT)
- Cyber Risk-Management
- Fines up to € 10.000.000

- In the Netherlands
  - NIB2: Netwerk en Informatie Beveiligingsrichtlijn
  - WBNI: Wet Beveiliging Netwerk en Informatiesystemen
  - RDI: Rijksinspectie Digitale Infrastructuur (https://rdi.nl)
  - NCCA: National Cybersecurity Certification Authority (https://dutchncca.nl)

Sectors of High Criticality

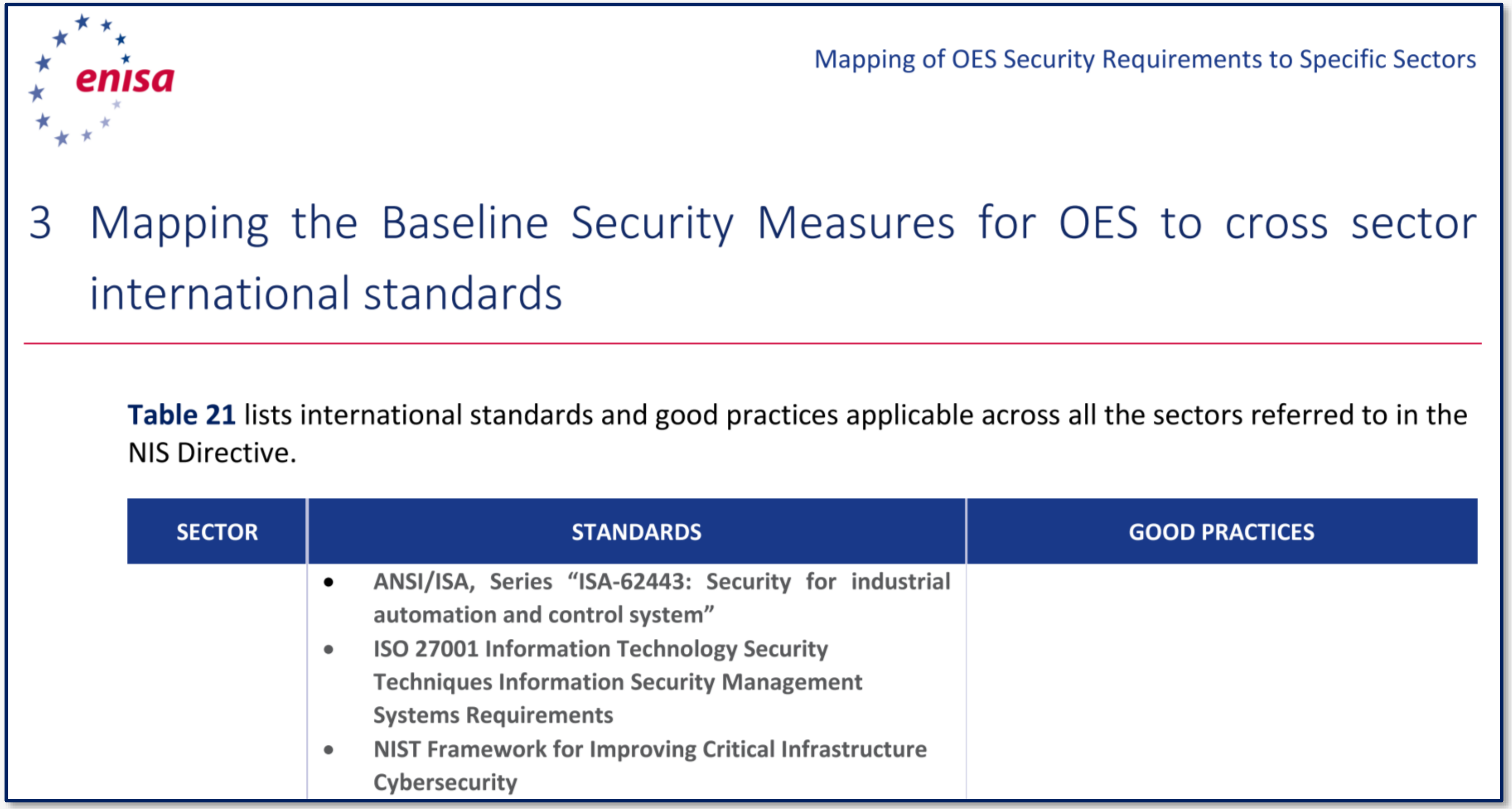
- Energy
  - Electricity
  - District Heating and Cooling
  - Oil, Gas, Hydrogen
- Transport
  - Air, Rail, Water, Road
- Health
- Drinking Water
- Waste Water

- Digital Infrastructure
- ICT Service Management (B2B)
- Public Administration
- Banking
- Financial Market
- Space

Other Critical Sectors

- Postal and Courier Servcies
- Waste Management
- Manfacture and Distribution of Chemicals
- Production, processing and distribution of Food
- Digital Providers
  - Online Marketplaces
  - Search Engines
  - Social Networking
- Manufacturing
  - Medical Devices
  - Computer, Electronic and Optical
  - Electrical Equipment
  - Machinery
  - Motor Vehicles, (Semi) Trailers
  - Other Transport Equipment
- Research

Mapping Baseline Security Measures



Mapping of OES Security Requirements to Specific Sectors

3 Mapping the Baseline Security Measures for OES to cross sector international standards

Table 21 lists international standards and good practices applicable across all the sectors referred to in the NIS Directive.

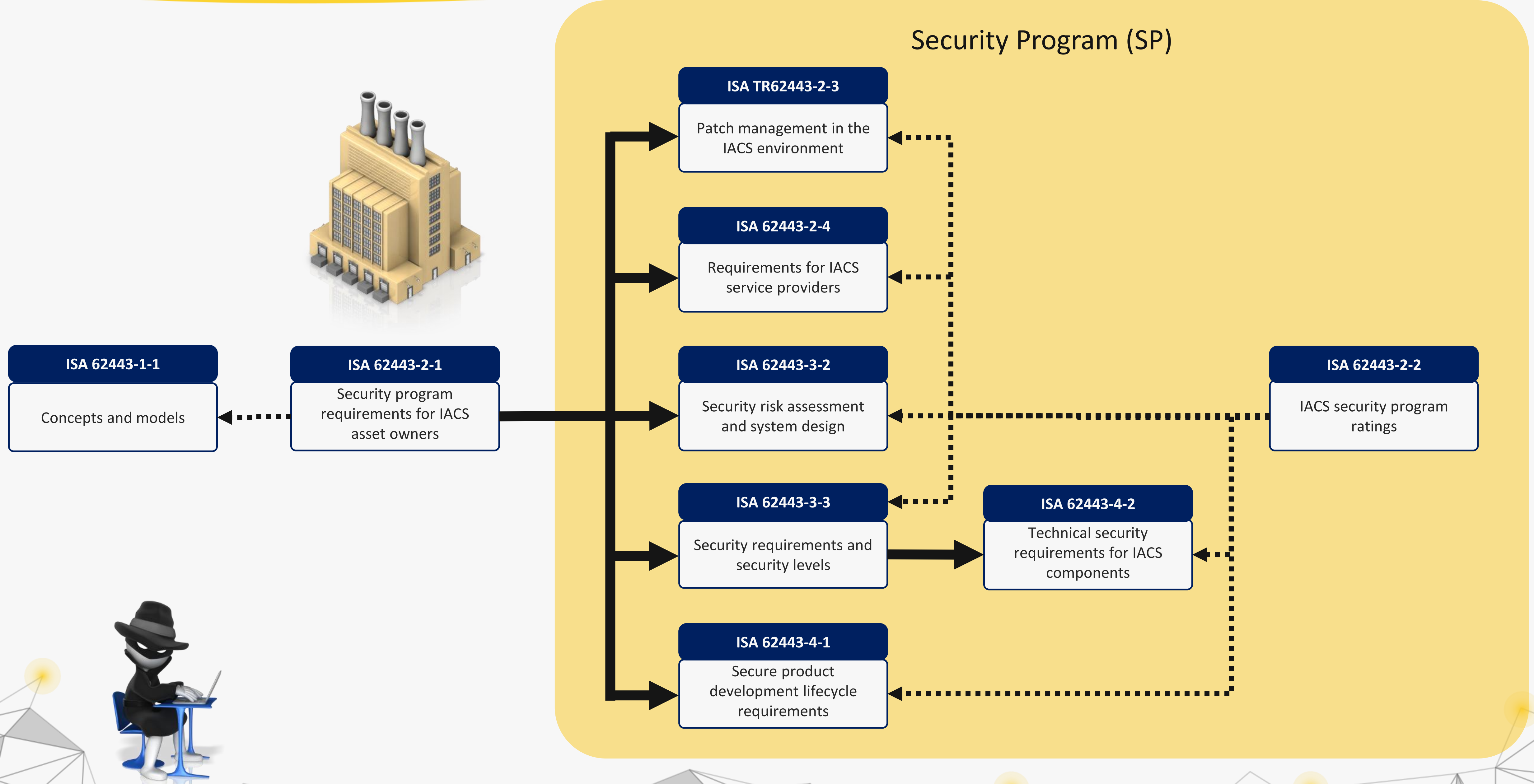
SECTOR	STANDARDS	GOOD PRACTICES
	• ANSI/ISA, Series "ISA-62443: Security for industrial automation and control system" • ISO 27001 Information Technology Security Techniques Information Security Management Systems Requirements • NIST Framework for Improving Critical Infrastructure Cybersecurity	

Mapping to Standards

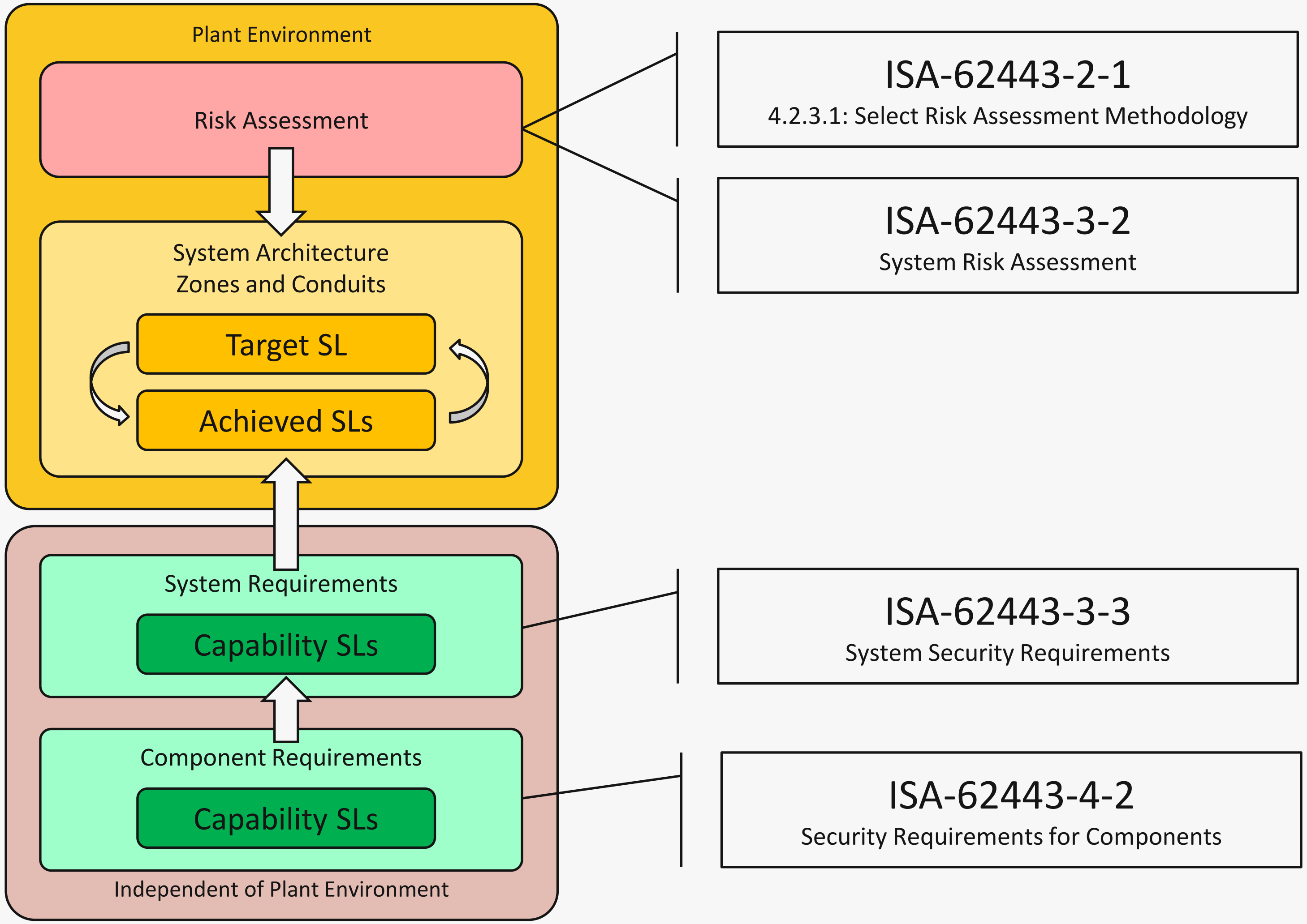
D/N	DOMAIN NAME	SECURITY MEASURE	ISO 27001:2013	NIST CYBER SECURITY FRAMEWORK	ISA/IEC 62443 3-3
Part 1 – Governance and Ecosystem					
1.1	**Information System Security Governance & Risk Management**	Information system security risk analysis	# 8.2 Information security risk assessment (ISO 27001) # 8.3 Information security risk treatment (ISO 27001)	ID.GV-4 ID.RA-1,2,3,4,5,6 D.RM-1,2,3 PR.AT-2	SR 5.2, 5.3,
		Information system security policy	# 5.1 Management direction for information security	ID.GV-1,2,3	–

ISA/IEC 62443

Cybersecurity for Industrial Automation and Control Systems



Security Program (SP)
ISA 62443-1-1
Concepts and models
ISA 62443-2-1
Security program requirements for IACS asset owners
ISA TR62443-2-3
Patch management in the IACS environment
ISA 62443-2-4
Requirements for IACS service providers
ISA 62443-3-2
Security risk assessment and system design
ISA 62443-3-3
Security requirements and security levels
ISA 62443-4-1
Secure product development lifecycle requirements
ISA 62443-4-2
Technical security requirements for IACS components
ISA 62443-2-2
IACS security program ratings



Plant Environment

Risk Assessment

System Architecture
Zones and Conduits

Target SL

Achieved SLs

System Requirements

Capability SLs

Component Requirements

Capability SLs

Independent of Plant Environment

ISA-62443-2-1
4.2.3.1: Select Risk Assessment Methodology

ISA-62443-3-2
System Risk Assessment

ISA-62443-3-3
System Security Requirements

ISA-62443-4-2
Security Requirements for Components

Contact Details

Willy Leuvering

WELP Software bv
PO Box 98
5480AB Schijndel

+31 655 166 126
Willy@welp.nl