Safety meets Cyber Security

SRF1 – Blackout – Live in der Sendung

Ivan Bütler

Compass Security - seit 1999

80 Mitarbeiter in Jona, Zürich, Bern, Basel, Berlin, Toronto

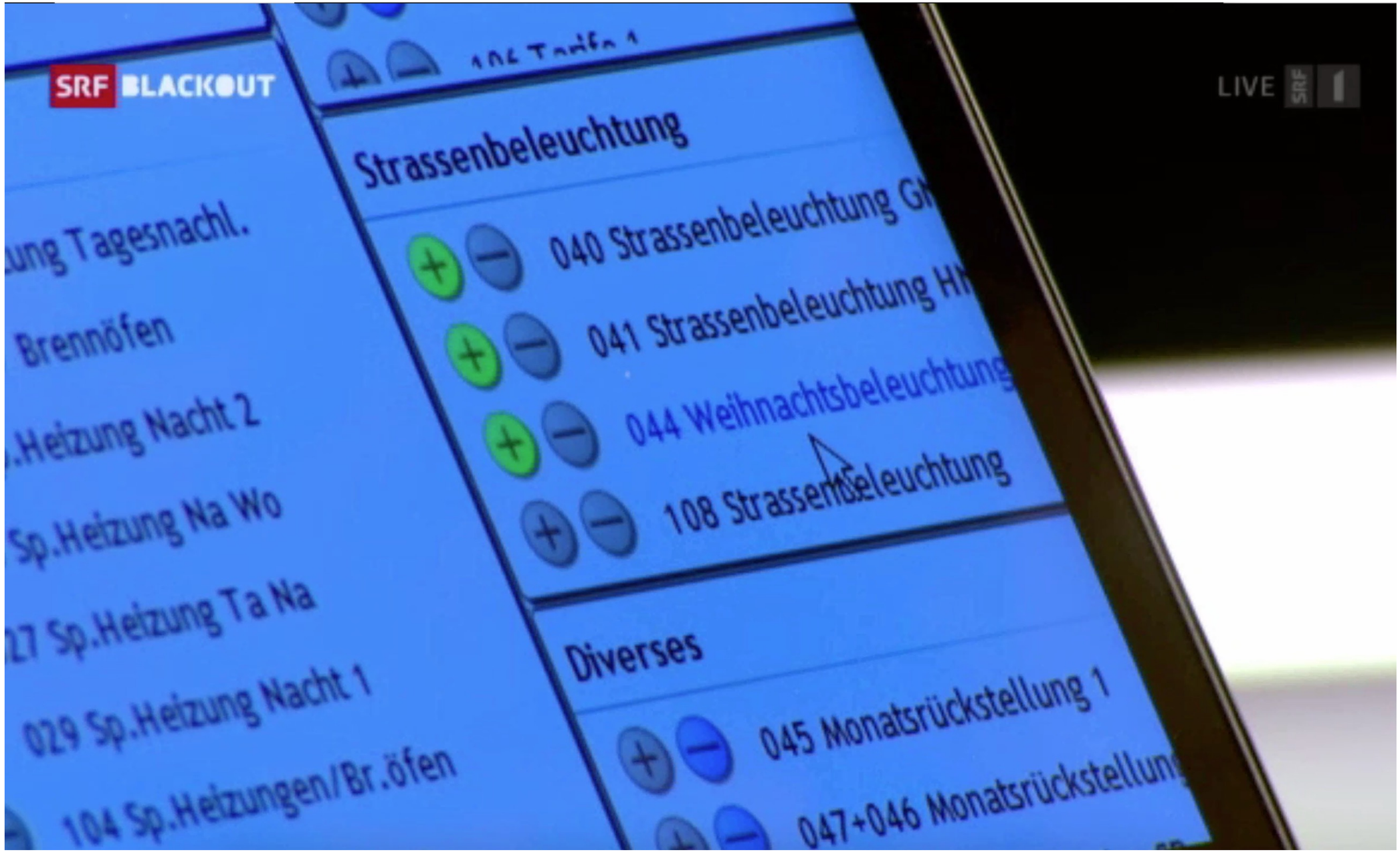
Hacking-Lab™
Hands-On & Capture-the-Flag

VBS Cyber Lehrgang

Die Kandidaten beim Assessment in Jassbach. Bild: VBS

Penetration Tests | Red Teaming | Security Reviews

Cyber Feuerwehr 7/24h (DFIR)


SRF BLACKOUT
LIVE SRF 1
Strassenbeleuchtung
040 Strassenbeleuchtung
041 Strassenbeleuchtung
044 Weihnachtsbeleuchtung
108 Strassenbeleuchtung
Diverses
045 Monatsrückstellung 1
047+046 Monatsrückstellung
ung Tagesnachl.
Brennöfen
.Heizung Nacht 2
Sp.Heizung Na Wo
27 Sp.Heizung Ta Na
029 Sp.Heizung Nacht 1
104 Sp.Heizungen/Br.öfen

RL CySec Rail

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK

Bundesamt für Verkehr BAV
Abteilung Sicherheit

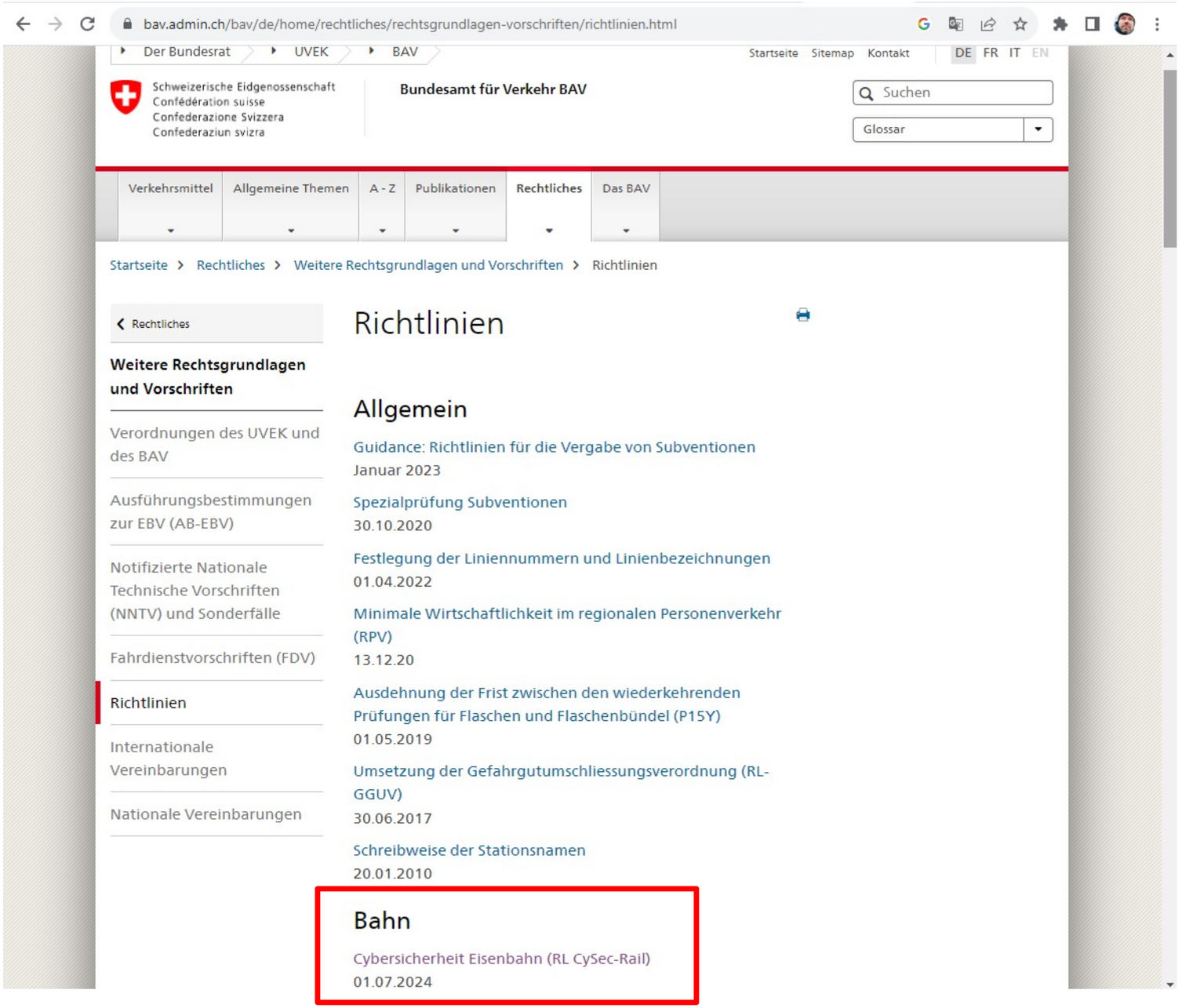
Aktenzeichen: BAV-041.4-3/11/6/15/1/4/1
Datum: 22.09.2023
Version: V1.0

Richtlinie

Cybersicherheit Eisenbahn

RL CySec-Rail

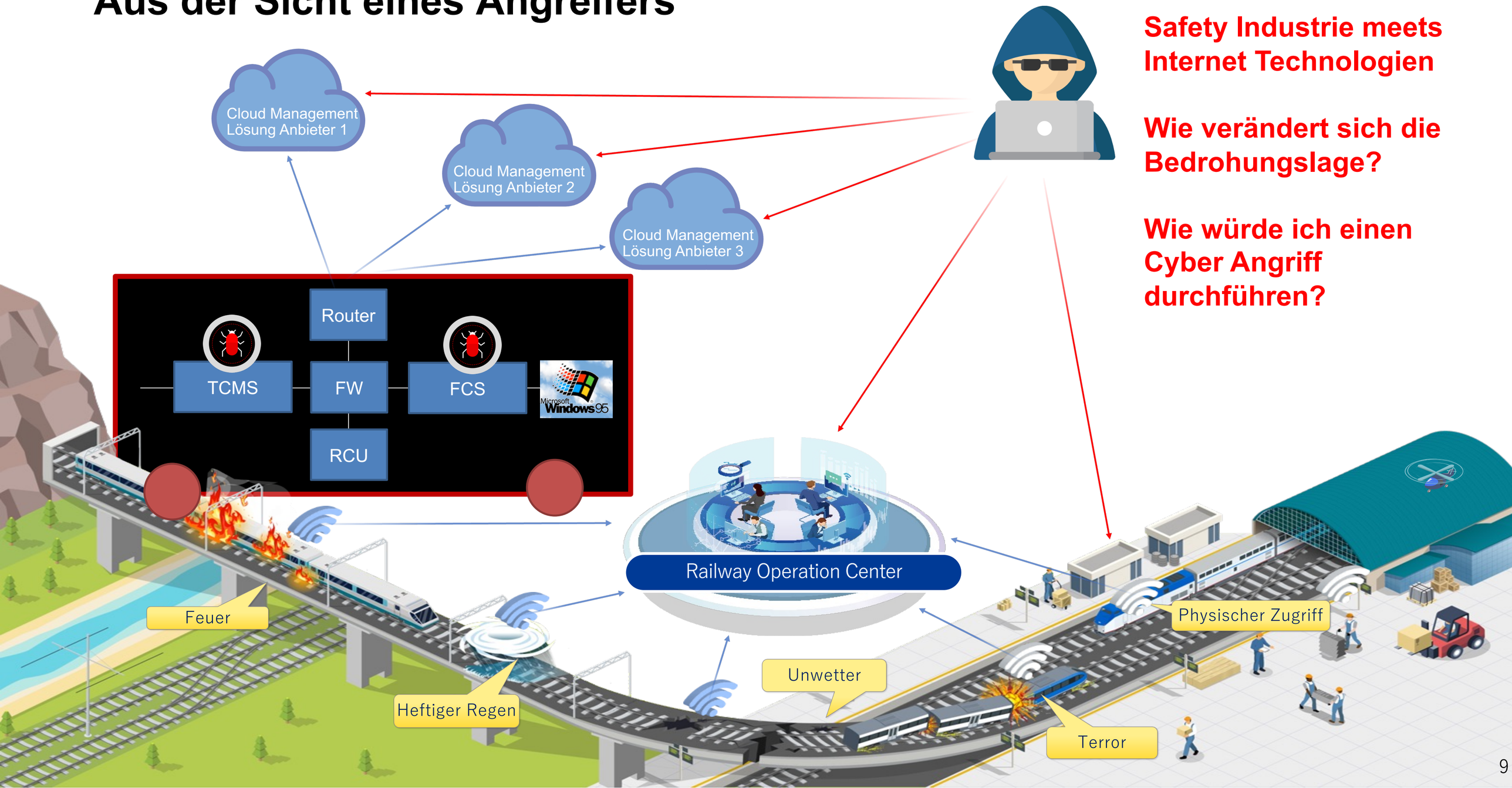
Auf Grundlage von Art. 5c der Verordnung über Bau und Betrieb der Eisenbahnen (Eisenbahnverordnung, EBV – SR 742.141.1) und deren Ausführungsbestimmungen.



Rail Slang

Type	Category	Transit
Operational Systems	Control Systems	Train Control System Bus Control Systems
	SCADA	Traction Power Emergency Ventilation System Monitoring (Pumps, Alarms)
	Signaling	Train Signals Signal Priority Systems
	Communications	Communications DSRC
	Fare Collection Systems	Entry/Exit Gates Ticket Vending Machines, Fare Boxes, Fare Validators, Ticket Encoding
	HVAC/Building Management	HVAC systems (not integral part, but loss could result in failure of critical systems) “People Movers”
Enterprise Data Systems	Business/Revenue/3rd Party systems: Finance, HR, Messaging (email), Archives	Asset Management BYOD
Engineering Systems	Design, Construction	Track Inspection

Aus der Sicht eines Angreifers

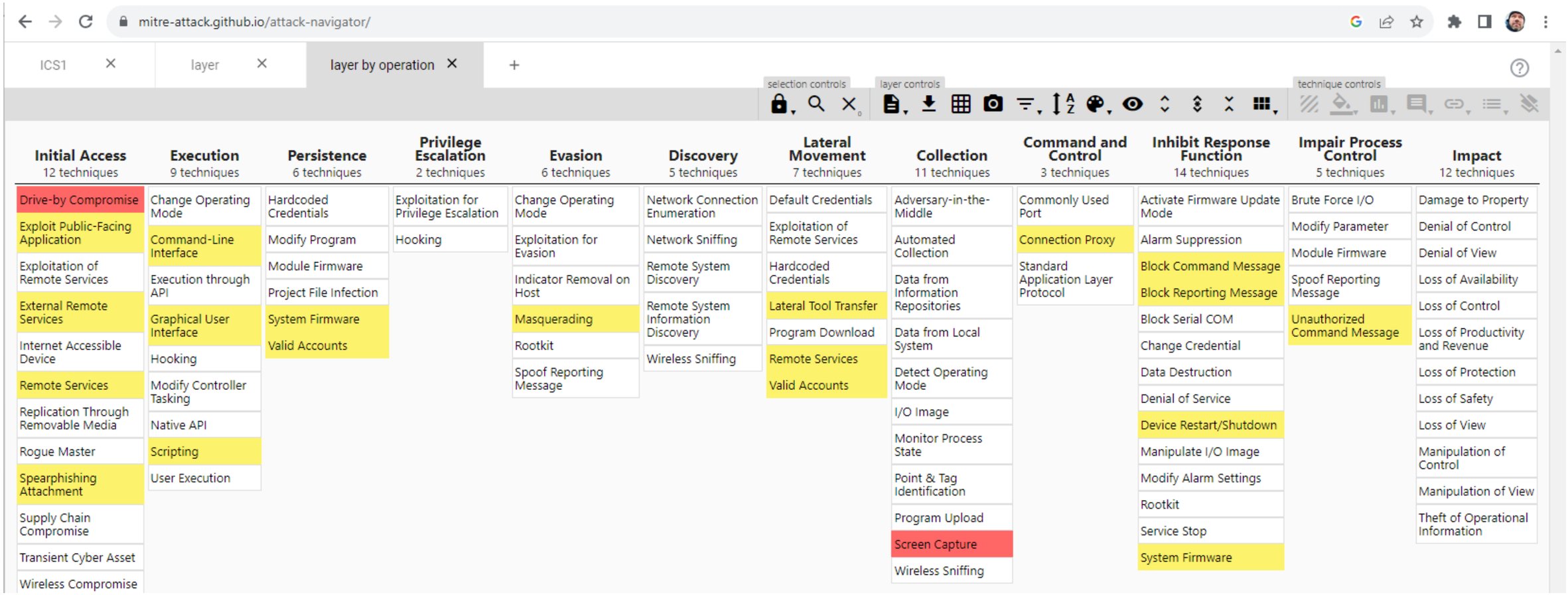


Safety Industrie meets Internet Technologien

Wie verändert sich die Bedrohungslage?

Wie würde ich einen Cyber Angriff durchführen?

Mitre Attack Framework



Shodan IoT Suchmaschine

shodan.io/search?query=railway&page=4

Shodan | Maps | Images | Monitor | Developer | More...

SHODAN | Explore | Downloads | Pricing | railway | Account

TOTAL RESULTS

199

TOP COUNTRIES

India	41
United States	39
Netherlands	14
Germany	12
Singapore	10

More...

View Report | Download Results | Historical Trend | Browse Images | View on Map

Access Granted: Want to get more out of your existing Shodan account? Check out everything you have access to.

301 Moved Permanently

2023-10-23T20:47:54.356935

2a01:488:42:1000:b24d:5511:ffd1:9fa2
railway-service.de
Host Europe GmbH
Germany, Frankfurt am Main

```
HTTP/1.1 301 Moved Permanently
Server: nginx
Date: Mon, 23 Oct 2023 20:47:53 GMT
Content-Type: text/html
Content-Length: 162
Connection: keep-alive
Location: https://railway-service.de
```

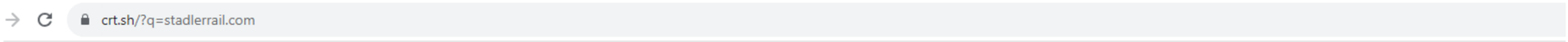
302 Found

2023-10-23T20:44:51.490676

193.47.89.177
HUBER+SUHNER AG
Switzerland, Pfäffikon

```
HTTP/1.1 302 Found
Date: Tue, 24 Oct 2023 11:33:00 GMT
Server: Apache
Location: https://railway-data.hubersuhner.com/
Content-Length: 221
Content-Type: text/html; charset=iso-8859-1
```

Open Source Intelligence



crt.sh Identity Search

Group by Issuer

Criteria	Type: Identity Match: ILIKE Search: 'stadlerrail.com'

Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Common Name	Matching Identities
10701130222	2023-10-10	2023-10-10	2024-01-08	dev.stadlerrail.com	dev.stadlerrail.com
10702310075	2023-10-10	2023-10-10	2024-01-08	dev.stadlerrail.com	dev.stadlerrail.com
10699114849	2023-09-26	2023-09-26	2023-12-25	recruiting.stadlerrail.com	recruiting.stadlerrail.com
10261435770	2023-08-31	2023-08-31	2024-08-31	etk-dev.stadlerrail.com	etk-dev.stadlerrail.com
10261435861	2023-08-31	2023-08-31	2024-08-31	etk-dev.stadlerrail.com	etk-dev.stadlerrail.com
10411762495	2023-08-26	2023-08-26	2023-11-24	oetiker.ch	varem.stadlerrail.com
10394309797	2023-08-26	2023-08-26	2023-11-24	oetiker.ch	varem.stadlerrail.com
10220858221	2023-08-25	2023-08-25	2024-08-25	test-sb20230825.stadlerrail.com	test-sb20230825.stadlerrail.com
10220858219	2023-08-25	2023-08-25	2024-08-25	test-sb20230825.stadlerrail.com	test-sb20230825.stadlerrail.com
10116069205	2023-08-11	2023-08-11	2023-11-09	dev.stadlerrail.com	dev.stadlerrail.com

Default Passwords

https://github.com/scadastrangelove/SCADAPASS

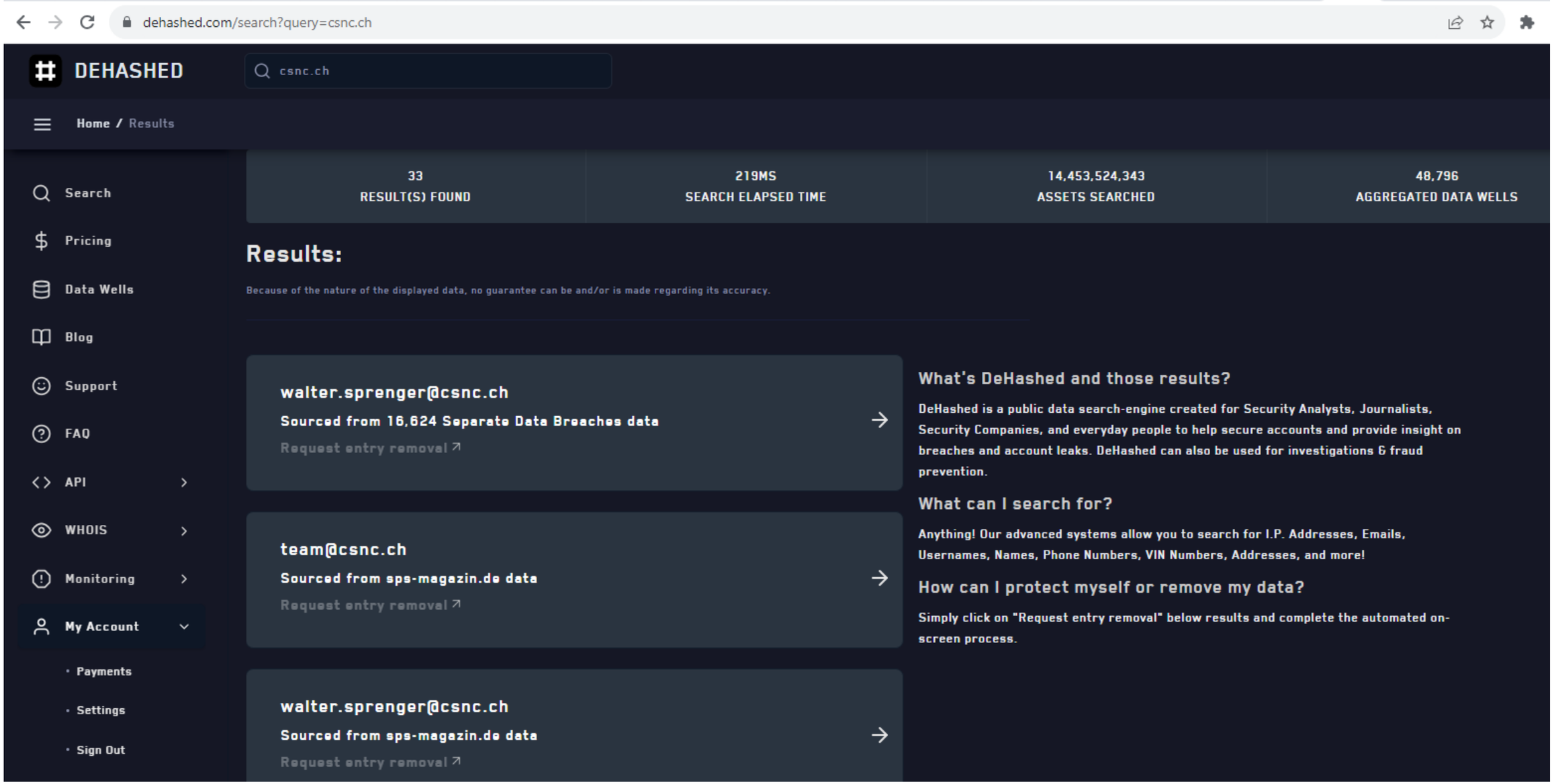
G18 | http://www.router-defaults.com/Router/BinTec--x1200-ip-password-username

	A	B	C	D	E	F
1	#SCADA StrangeLove Default/Hardcoded Passwords List					
2	#Find more at http://www.scada.sl					
3	#Please contact us at scadastrangelove@gmail.com and @scadasl					

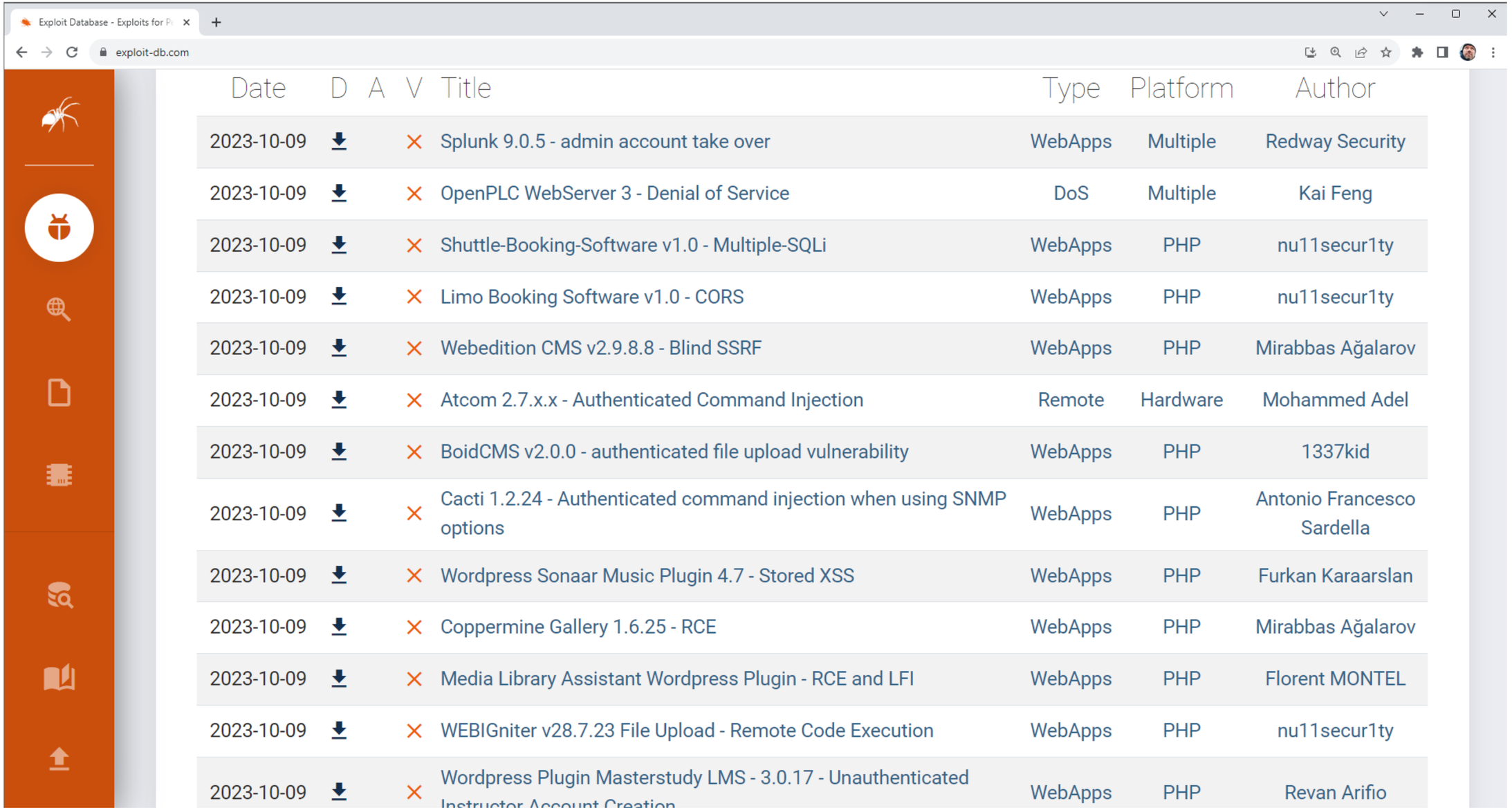
siemens	Simatic S7-300 (pre-2009 versions)	Hardcoded password:, Basisk:Basisk
siemens	Scalance	admin:admin, user:user
siemens	Scalance (x 200, W788-1PRO, W788-2PF	Admin:admin, User:user, for FTP access:
siemens	SyncoTM living Web server OZW772 V2	Administrator:Password
siemens	Siemens WinCC 7.x	winccd:winccpass, wincce:winccpass, DI
siemens	Ruggedcom RMC30	admin:admin
siemens	RuggedSwitch, RS8000 / RS1600 / RS900	admin

19	BinTec Elmeg	any routers	(##unknown - means not known or any ch		Router	
20	BinTec Elmeg	BinTec R230aw	admin:funkwerk		Router	
21	BinTec Elmeg	bintec W2002T-n,	admin:funkwerk, admin:admin		WLAN Access Point f	
22	Contemporary Control Systems	BASRT-B	admin:admin	80/tcp	Router	http
23	Datasensor	UR5i/UR5i SL	root:root	80/tcp	Router	http
24	Digi	DC-ME-01T-S	root:dbps		Networki	http
25	Digi	Digi Connect SP, Digi Connect Wi-SP, Di	root:dbps	80/tcp	Network I	http
26	Digi	Digi Connect ES 4/8 SB with Switch, Digi	root:dbps	80/tcp	Concentra	http

Leaked Passwords

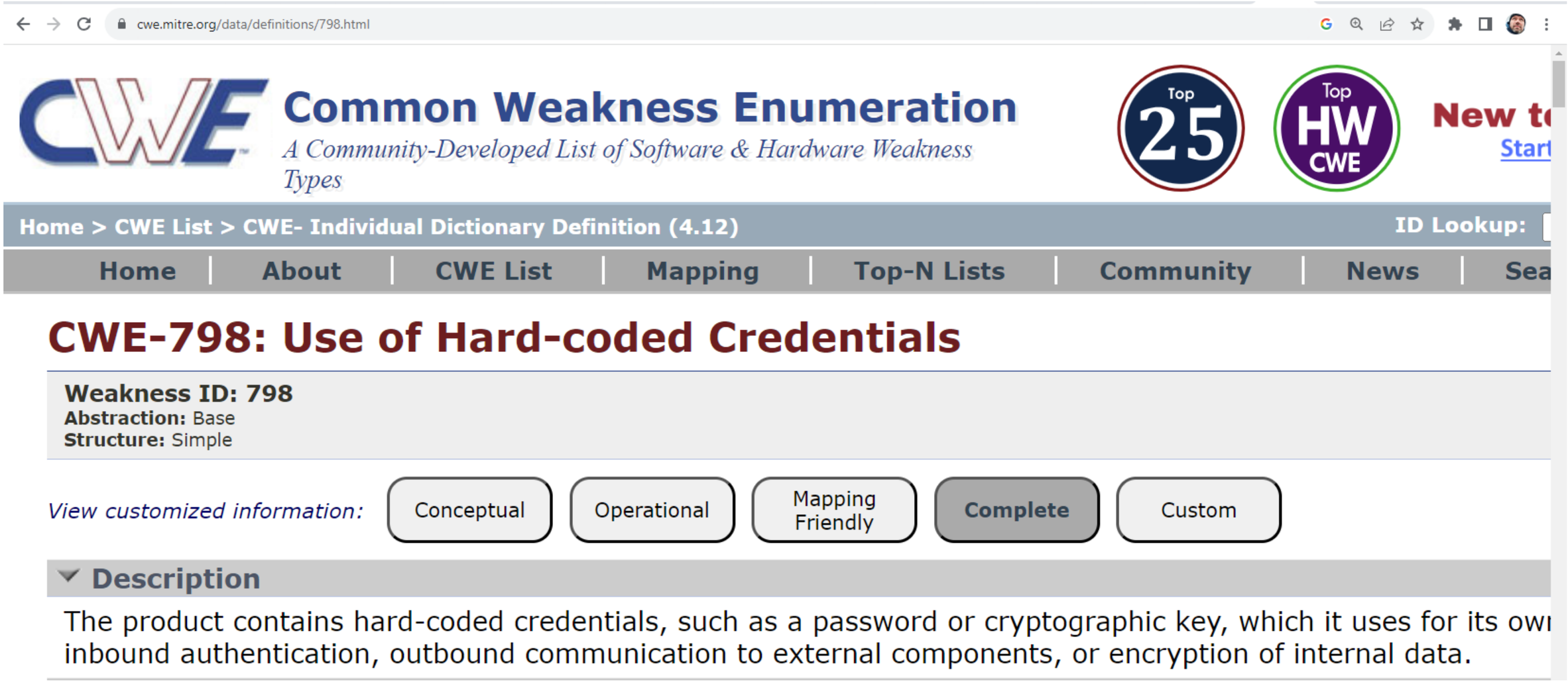


Bekannte Schwachstellen

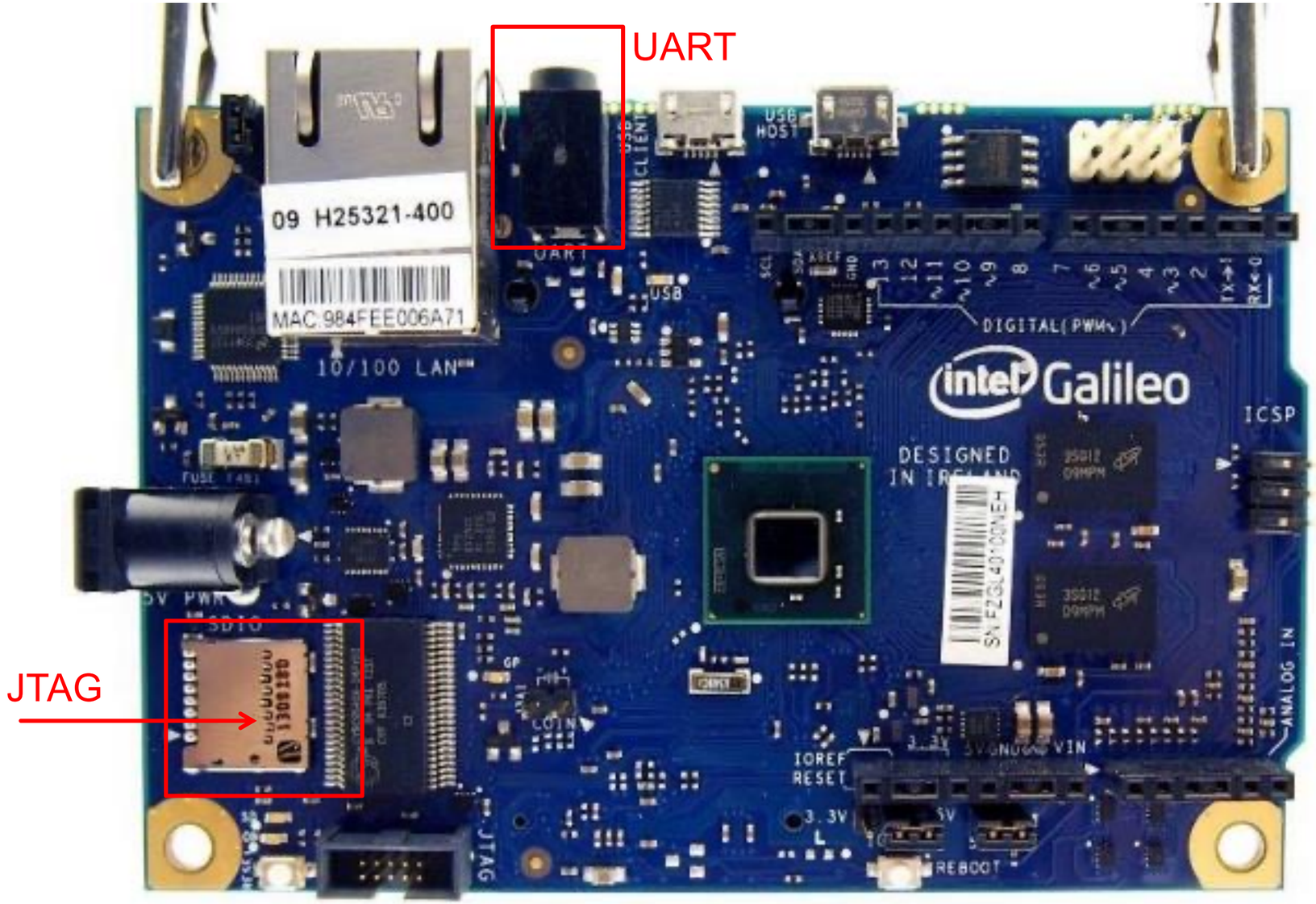


Date	D	A	V	Title	Type	Platform	Author
2023-10-09	⬇		✕	Splunk 9.0.5 - admin account take over	WebApps	Multiple	Redway Security
2023-10-09	⬇		✕	OpenPLC WebServer 3 - Denial of Service	DoS	Multiple	Kai Feng
2023-10-09	⬇		✕	Shuttle-Booking-Software v1.0 - Multiple-SQLi	WebApps	PHP	nu11secur1ty
2023-10-09	⬇		✕	Limo Booking Software v1.0 - CORS	WebApps	PHP	nu11secur1ty
2023-10-09	⬇		✕	Webedition CMS v2.9.8.8 - Blind SSRF	WebApps	PHP	Mirabbas Ağalarov
2023-10-09	⬇		✕	Atcom 2.7.x.x - Authenticated Command Injection	Remote	Hardware	Mohammed Adel
2023-10-09	⬇		✕	BoidCMS v2.0.0 - authenticated file upload vulnerability	WebApps	PHP	1337kid
2023-10-09	⬇		✕	Cacti 1.2.24 - Authenticated command injection when using SNMP options	WebApps	PHP	Antonio Francesco Sardella
2023-10-09	⬇		✕	Wordpress Sonaar Music Plugin 4.7 - Stored XSS	WebApps	PHP	Furkan Karaarslan
2023-10-09	⬇		✕	Coppermine Gallery 1.6.25 - RCE	WebApps	PHP	Mirabbas Ağalarov
2023-10-09	⬇		✕	Media Library Assistant Wordpress Plugin - RCE and LFI	WebApps	PHP	Florent MONTEL
2023-10-09	⬇		✕	WEBIGniter v28.7.23 File Upload - Remote Code Execution	WebApps	PHP	nu11secur1ty
2023-10-09	⬇		✕	Wordpress Plugin Masterstudy LMS - 3.0.17 - Unauthenticated Instructor Account Creation	WebApps	PHP	Revan Arifio

Hard-coded Credentials

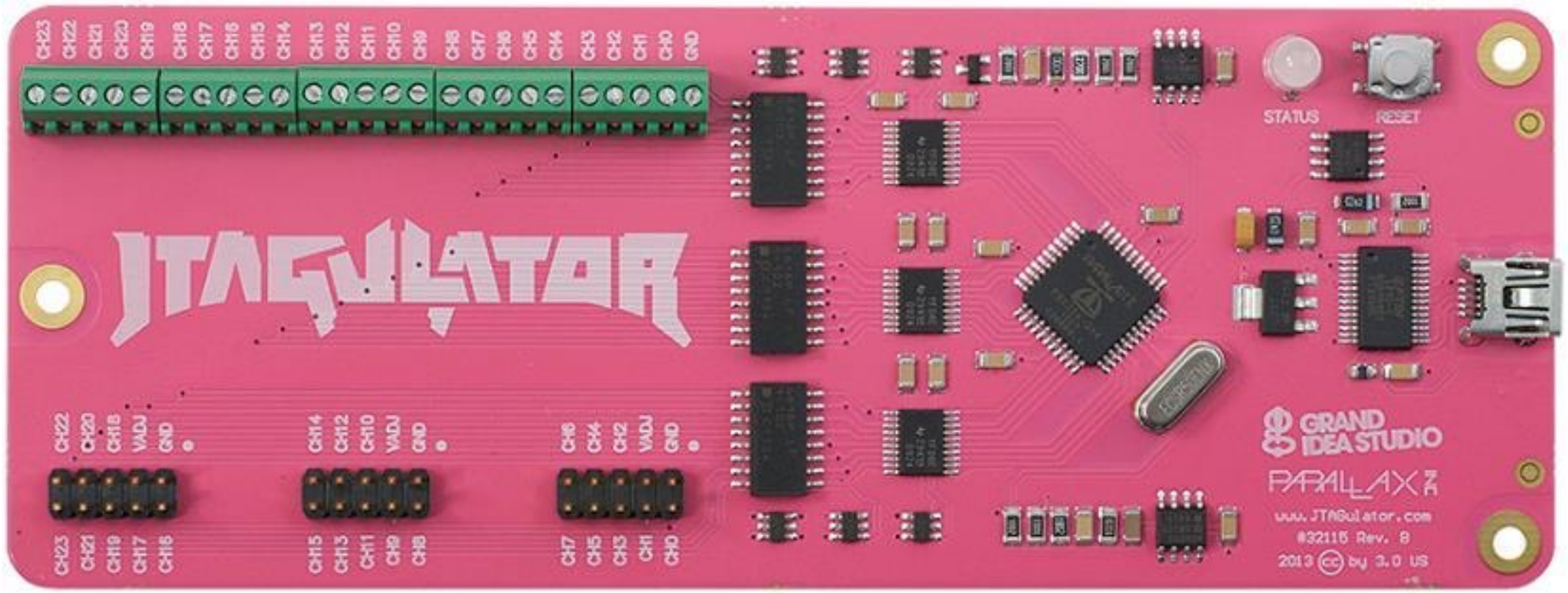


JTAG und UAR Hacking



JTAGulator

On-chip debug (OCD) interfaces can provide chip-level control of a target device and are a primary vector used by engineers, researchers, and hackers to extract program code or data, modify memory contents, or affect device operation on-the-fly

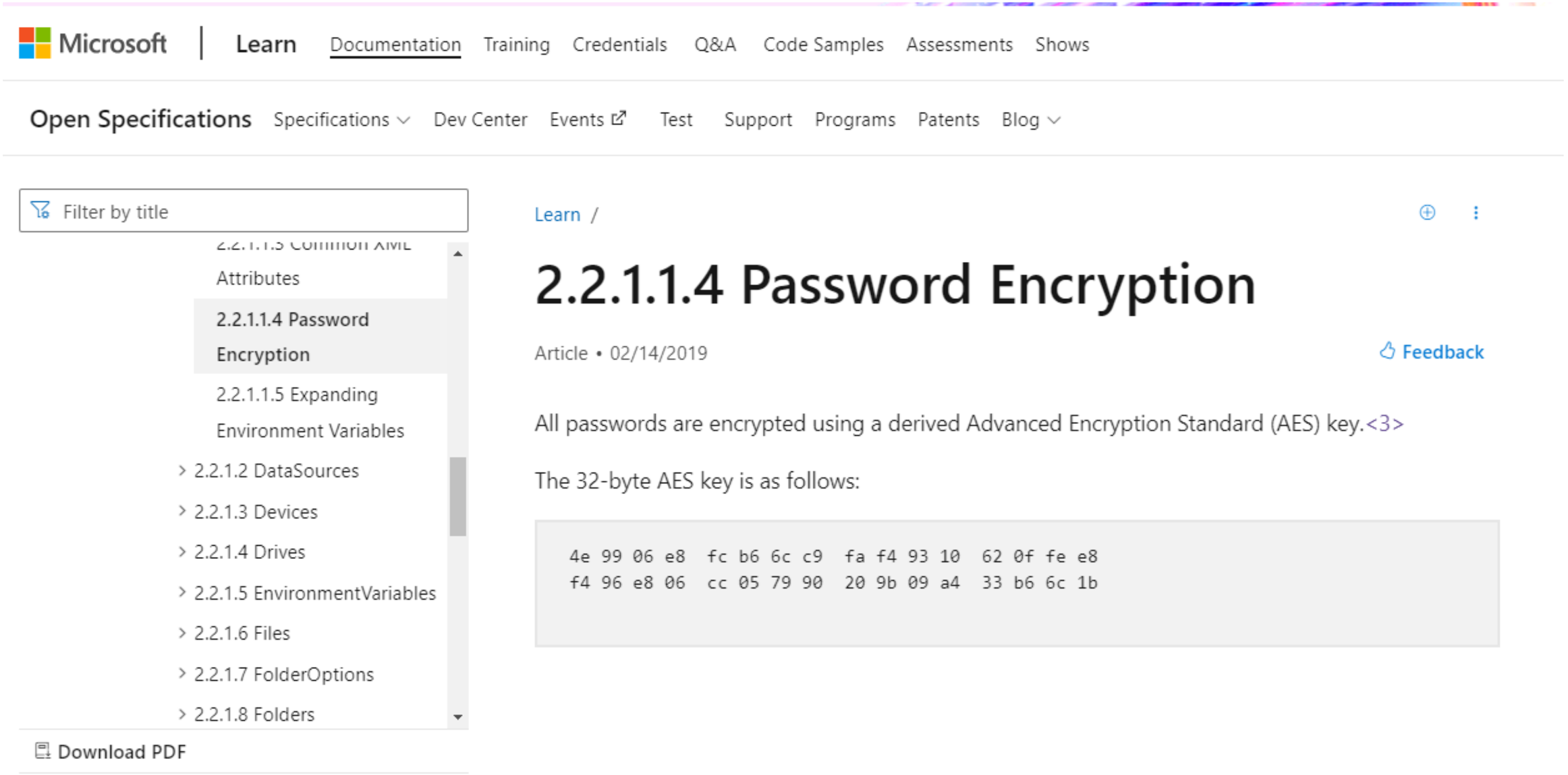


Source http://www.grandideastudio.com/jtagulator/

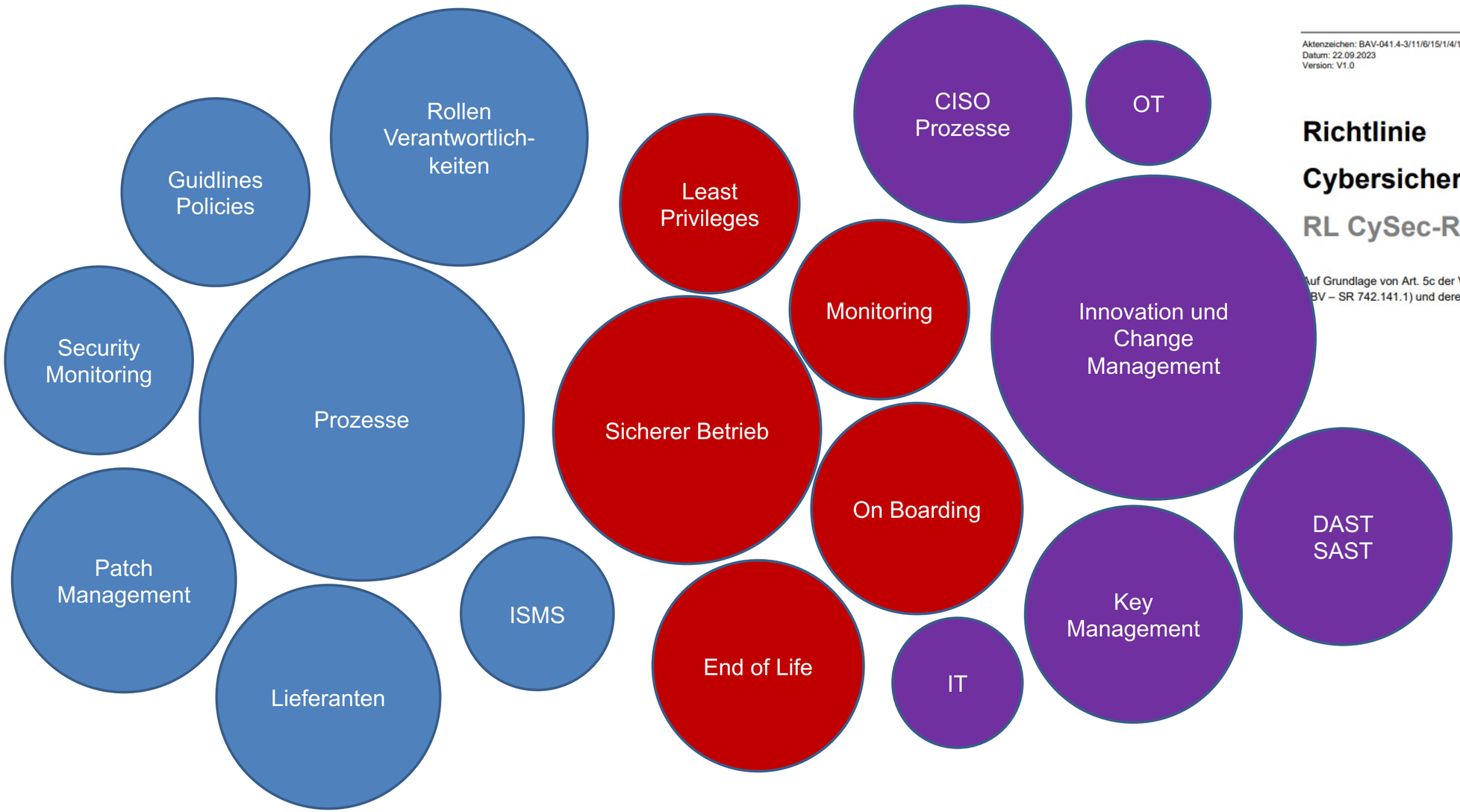
Abhängigkeiten zum Active Directory

Quelle Bild: https://cyberhoot.com/cybrary/active-directory-ad/

AES Decryption



Empfehlungen Cyber Sicherheit



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK

Bundesamt für Verkehr BAV
Abteilung Sicherheit

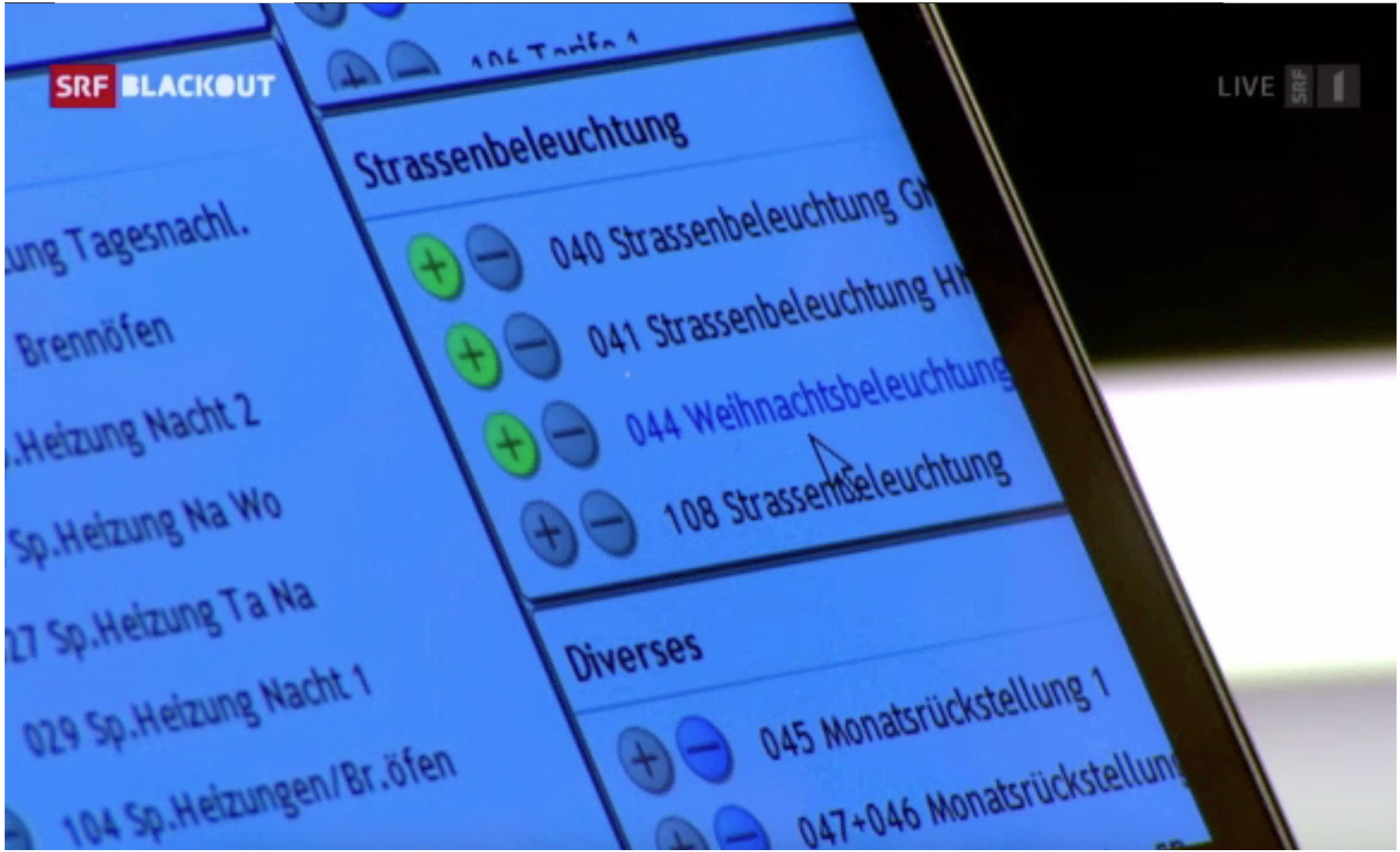
Aktenzeichen: BAV-041.4-3/11/6/15/1/4/1
Datum: 22.09.2023
Version: V1.0

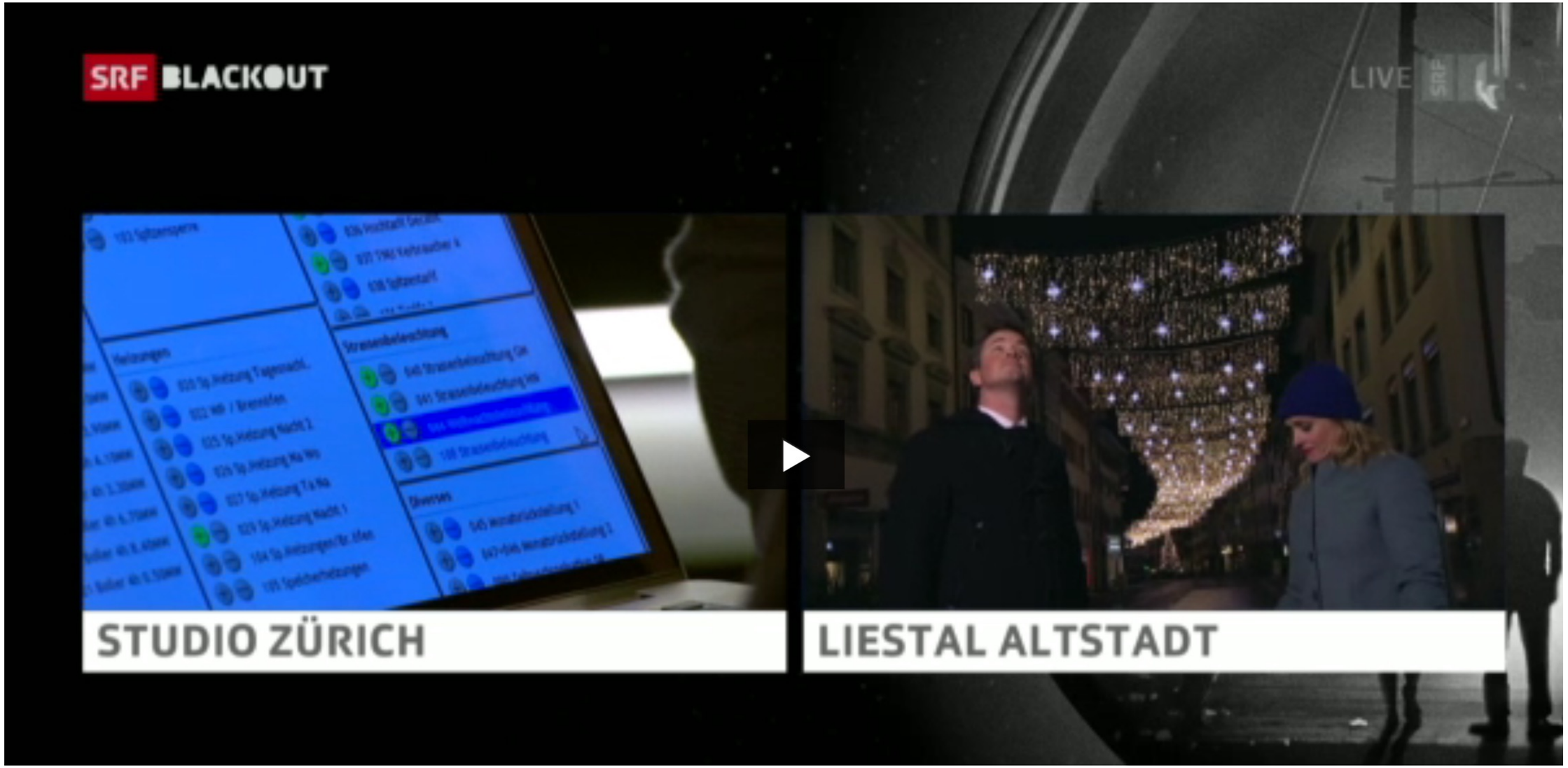
Richtlinie

Cybersicherheit Eisenbahn

RL CySec-Rail

Auf Grundlage von Art. 5c der Verordnung über Bau und Betrieb der Eisenbahnen (Eisenbahnverordnung, EBV – SR 742.141.1) und deren Ausführungsbestimmungen.


SRF BLACKOUT
LIVE SRF 1
Strassenbeleuchtung
040 Strassenbeleuchtung
041 Strassenbeleuchtung
044 Weihnachtsbeleuchtung
108 Strassenbeleuchtung
Diverses
045 Monatsrückstellung 1
047+046 Monatsrückstellung
ung Tagesnachl.
Brennöfen
.Heizung Nacht 2
Sp.Heizung Na Wo
27 Sp.Heizung Ta Na
029 Sp.Heizung Nacht 1
104 Sp.Heizungen/Br.öfen


SRF BLACKOUT
LIVE
STUDIO ZÜRICH
LIESTAL ALTSTADT


SRF BLACKOUT
LIVE SRF
STUDIO ZÜRICH
LIESTAL ALTSTADT

Vielen Dank für Ihre Aufmerksamkeit

Ivan Bütler, Compass Security AG
Ethical Hacking & Penetration Testing
Incident Response

ivan.buetler@compass-security.com
https://www.compass-security.com/