Spike Talk in Power Electronic Dominated Grids

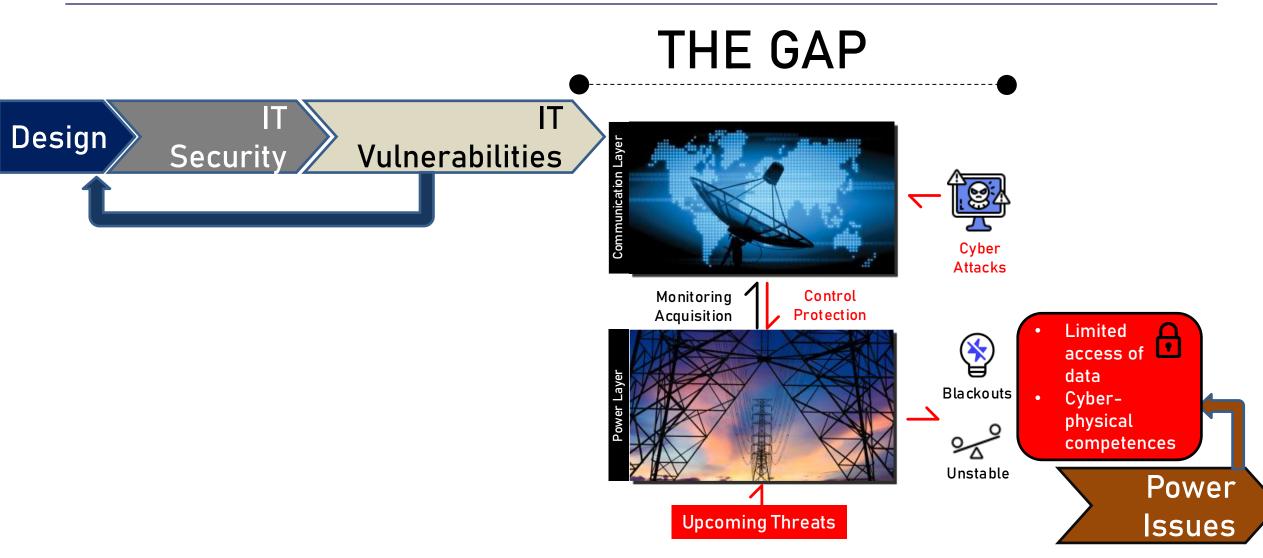
Towards a "One-Stop" Security Solution

Subham Sahoo Assistant Professor, Aalborg University Vice-Leader, Reliability of Power Electronic Converters (ReliaPEC Group) Denmark

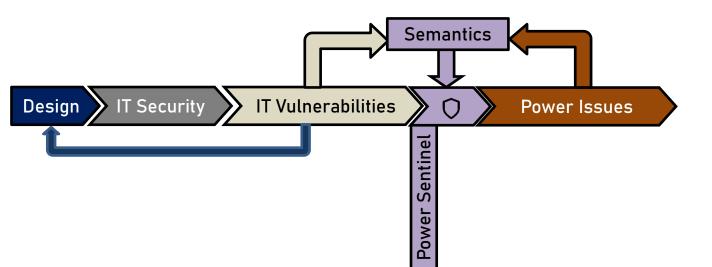


A A L B O R G U N I V E R S I T Y

Closing the gap?



Power Sentinel (TRL 5-6)

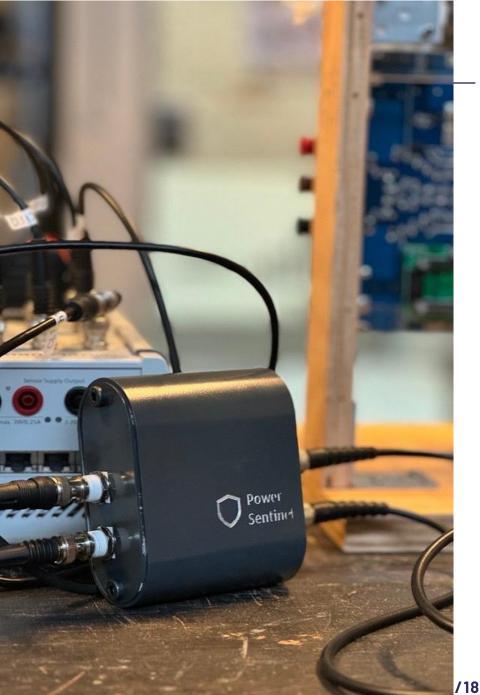


World's 1st NON-INVASIVE GRID EDGE Integrated Technology

Relevant standards passed: IEEE 1547.3 and IEEE C37.240

- Resource-efficient
- Computationally light
- Plug-and-play modularity

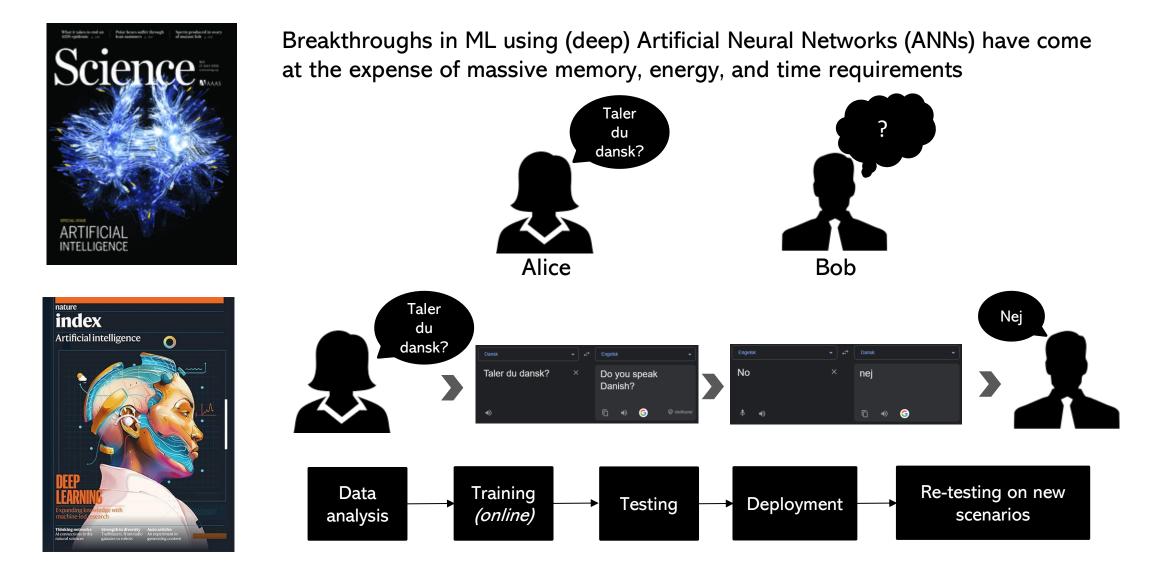




One Stop Solution to Digitalization Issues?

Criticality of ICT in Power Electronic Grids

Machine Learning Today

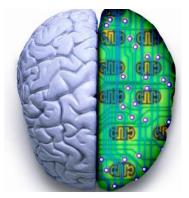


Beyond ANN

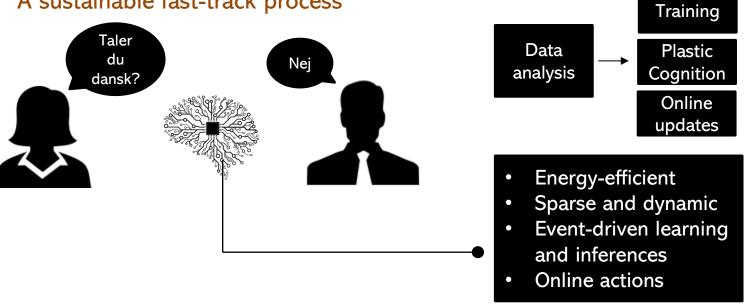


13 Million Watts 5600 sq. ft. & 340 tons 10¹⁰ ops/J

20 Watts 2 sq. ft. & 1.4 Kg 10¹⁵ ops/J



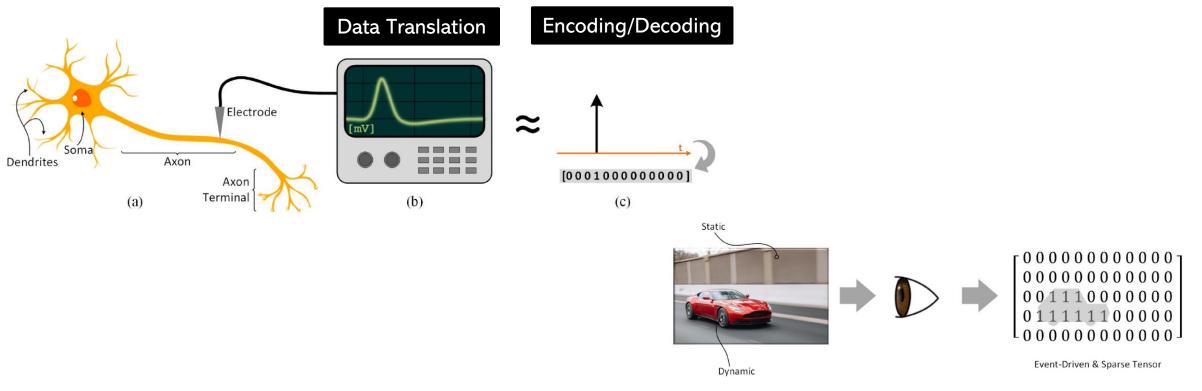
A sustainable fast-track process



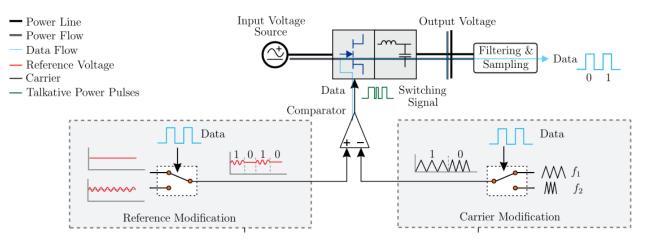
► Actually..

The electrical modeling of neurons in our brain are quite different from the ones using in a typical ML algorithm.

- Neurons in the brain sense, process, and communicate over time using sparse binary signals (spikes or action potentials).
- This results in a dynamic, sparse, event-driven learning and inference.
- Spiking signals minimize energy per bit.



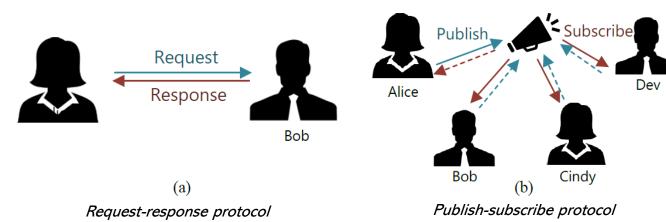
Information Embedded in Power



Talkative Power^{1,2}

1. M. Liserre, H. Beiranvand, Y. Leng, R. Zhu and P. A. Hoeher, "Overview of Talkative Power Conversion Technologies," *IEEE Open Journal of Power Electronics*, vol. 4, pp. 67-80, 2023, doi: 10.1109/0JPEL.2023.3237709.

2. M. Angjelichinoski, Č. Stefanović, P. Popovski and F. Blaabjerg, "Power talk in DC micro grids: Constellation design and error probability performance," 2015 IEEE International Conference on Smart Grid Communications (SmartGridComm), Miami, FL, USA, 2015.

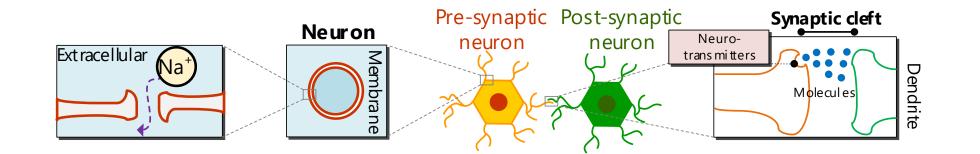


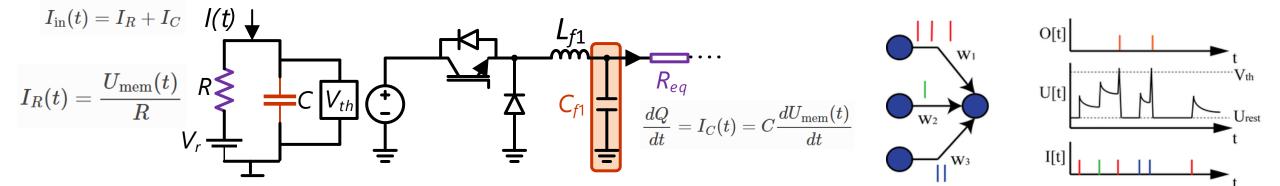
Inferential Communication

SUBHAM SAHOO, ReliaPEC GROUP, AAU ENERGY, AALBORG UNIVERSITY -

-/18

Biologically Plausible Neurons/Converters

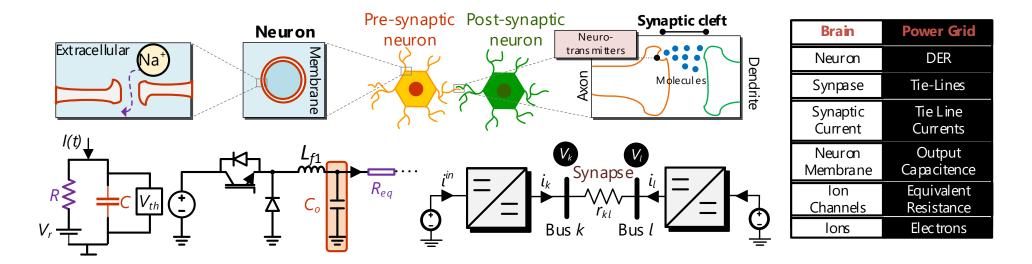


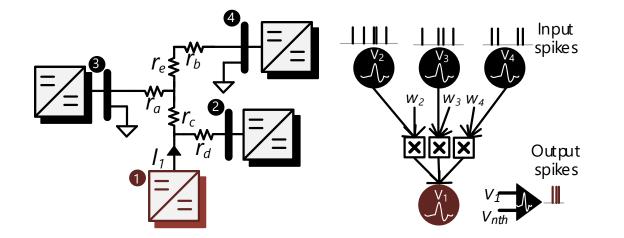


Leaky Integrate-and-Fire (LIF) Neuron

$$RCrac{dU_{
m mem}(t)}{dt} = -U_{
m mem}(t) + RI_{
m in}(t)$$

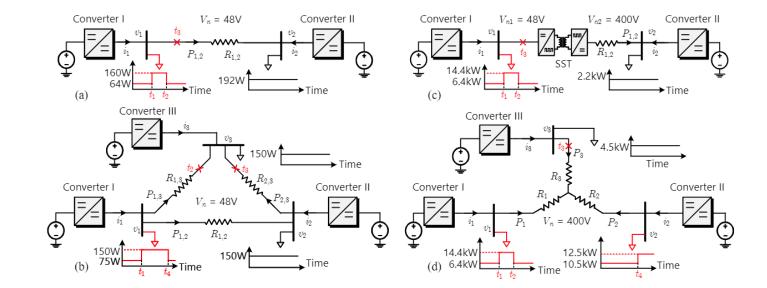
Fine Grained Parallelism

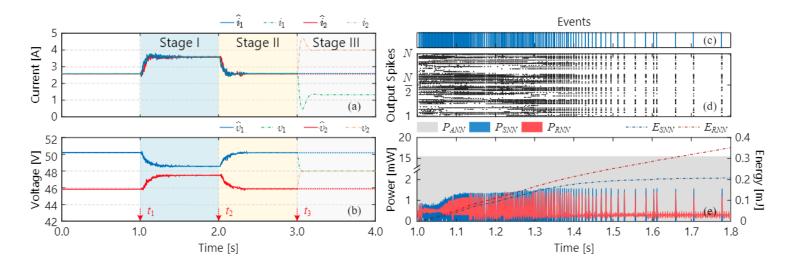




Network of Converters have now become a network of neurons

► Performance Evaluation



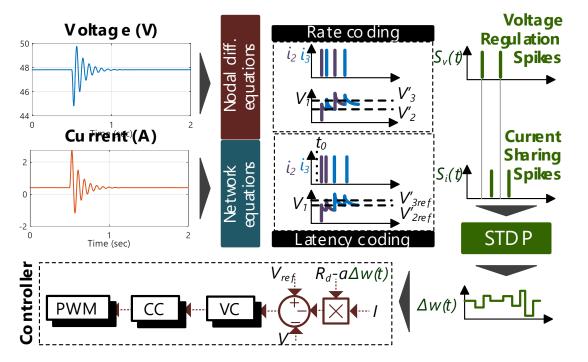


Source: X Diao, Y Song, S Sahoo, Y Li, « Neuromorphic Event-Driven Semantic Communication in Microgrids» *IEEE Trans. Smart Grid*, vol. 15, no. 5, pp. 4300-4314, 2024.

Upto 84% "compute" energy savings due to computation for a given mission profile

-/18

Spiking Neuron Replicated as Energy Source



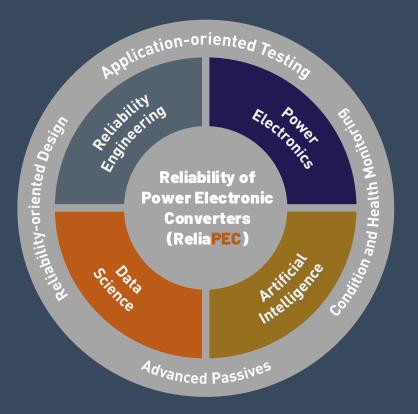
- We model each source as a LIF neuron
- It can respond to both input and output disturbances
- Only the remote sources will respond to a given disturbance based on the voltage fluctuations and its spatial decay
- Timing based learning rules to change the conductance of the modeled neuron and change power generation
- Multi-agent networked control, adaptation, protection, flexibility is possible with minimal energy consumption per inference

Source: S Sahoo, "Spike Talk – Genesis and Neural Coding Scheme Translations", *arXiv preprint arXiv:2408.00773*, 2024.

-/18



Contact Subham Sahoo ReliaPEC Group <u>sssa@energy.aau.dk</u> +45 9141 0380





Cybersecurity in Power Electronic Dominated Grids

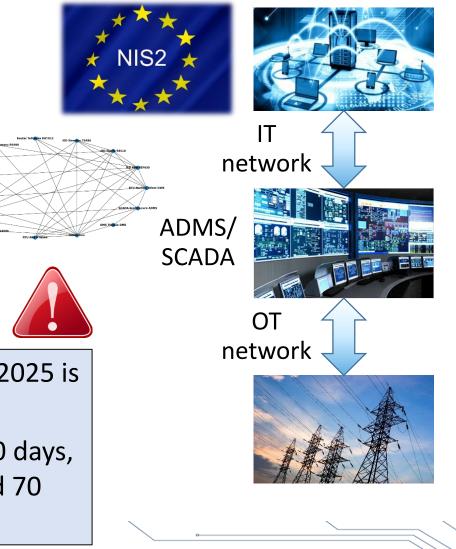
Challenges and Advances in Cybersecurity of Electricity Distribution Ecosystems: the Case of Slovenia

Andrej Bregar

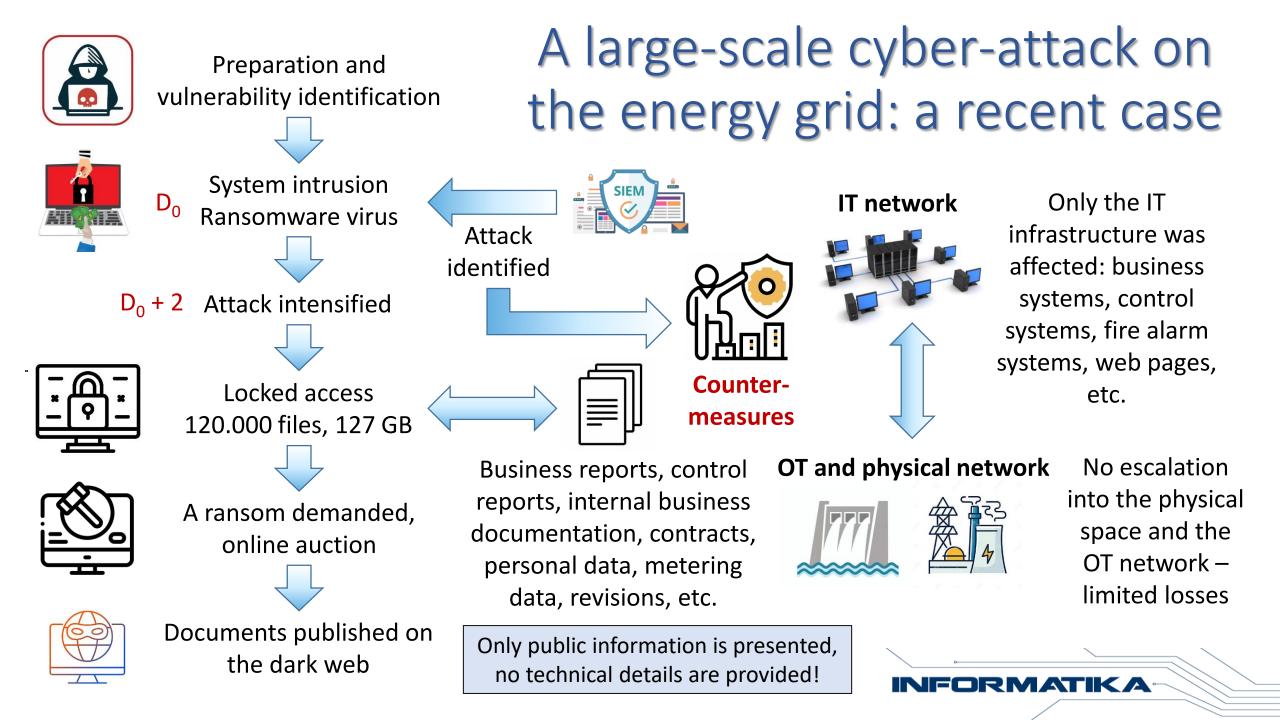
INFORMATIKA

Cybersecurity in energy ecosystems

- Critical infrastructure is strategically important
- Increase in the attack surface of energy systems
- High-impact cyber-attacks result in the disruption of business continuity in energy distribution, cascading effects, and substantial damage to infrastructure
 - Stuxnet, Ukrainian electricity grid ...
 - Hybrid war
- NIS 2 Directive: Boosting the protection of essential infrastructure by tightening risk assessments and reporting requirements
 - The estimated global cost of the cyber criminal in 2025 is 10.5 billion EUR
 - The average response time to a cyber-attack is 280 days, which includes 210 days to detect the incident and 70 days for eradication, containment, and recovery



INFORMATIK A



Cyber-attack countermeasures

- Reporting
 - National CSIRT
 - Government Information Security Office
 - Other relevant governmental institutions and offices
 - Owners and stakeholders in the EPES ecosystem
- Incident response
 - Participation of relevant internal, external, and national cybersecurity teams
 - Technical countermeasures for incident analysis, containment, and eradication

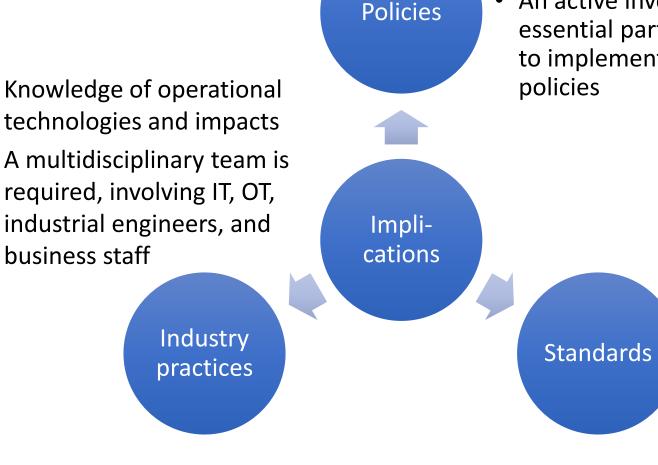
Detection 8 Analysis Eradication

- Recovery of targeted business systems, identification and analysis of IoCs
- Generic instructions for all EPES stakeholders
- What was achieved?
 - IT and OT systems operational, energy production and supply not disrupted
 - Business data recovered, no major business damage

Cybersecurity requirements for energy grids

N	AXIMIZED /	AVAILABILIT	Ϋ́		MINIMIZ	ED RISKS	
Application resilience	Network resilience	Access control	Information security	Change management	Vulnerability assessment	Incident reporting	Training
Continuous operations	Real-time demands	Cascading effects	Integration of new and legacy technologies	Recovery from attacks	Identification of anomalies	Process network (OT)	Counter- attacks
				SECURITY BY DESIGN		ORMATI	KA

Implications



- Aligned with NIST and SANS response plans
- An active involvement of all essential parties is necessary to implement cybersecurity policies



- Specific standards, e.g., ISO/IEC 62443-4-1 (secure development of products used in industrial automation and control systems)
- Generic standards, e.g., ISO 27035, Part 3 (guidelines for IR operations)
- NIS 2 Directive
- NCC (Network Code on Cybersecurity)
- CER Directive (Critical Entities Resilience)

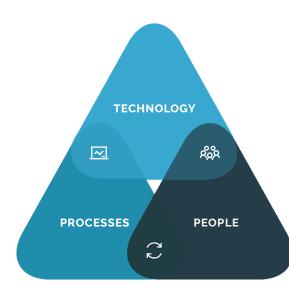
INFORMATIK A

CRA (Cyber Resilience Act)

National energy SOC

- National SOC for the energy ecosystem
- SOCs of major energy stakeholders
- SOCs of other major providers of critical infrastructure
- National CSIRT
- Governmental offices and institutions
- Communities



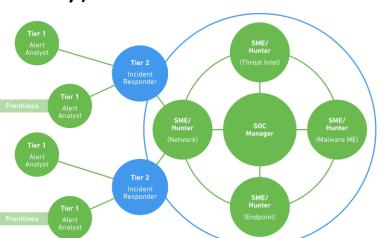


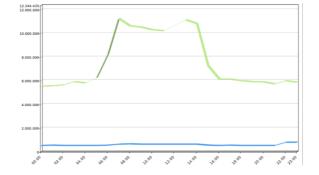
- Consolidation of resources and capabilities
- Improved and more agile detection and response
- Enhanced CTI exchange, stakeholder coordination, and alerting
- Centralized cyber risk management
- Single entering point
- Uniform protocols for reporting, collaboration, and response
- Regulatory compliance

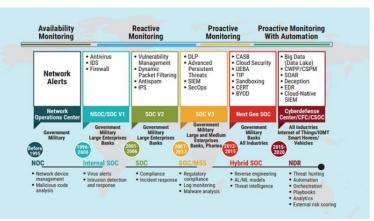


Proactive NG-SOC of Informatika

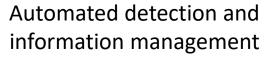
- Proactive cyber defense acting in anticipation of attacks, getting in front of them, neutralizing them early instead of waiting for the damage to occur
- 24/7/365, HA (High Availability)
- Slovenian DSOs
- IT-OT integration
- Multi-tier organization
- Large number of events
 - 5k+/- EPS
 - June: 7.189.513.374 events
 - July: 6.909.223.750 events
 - August: 6.625.410.913 events

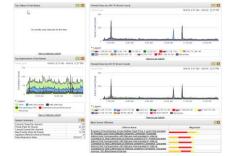






Protecting the IT-OT integrated energy system



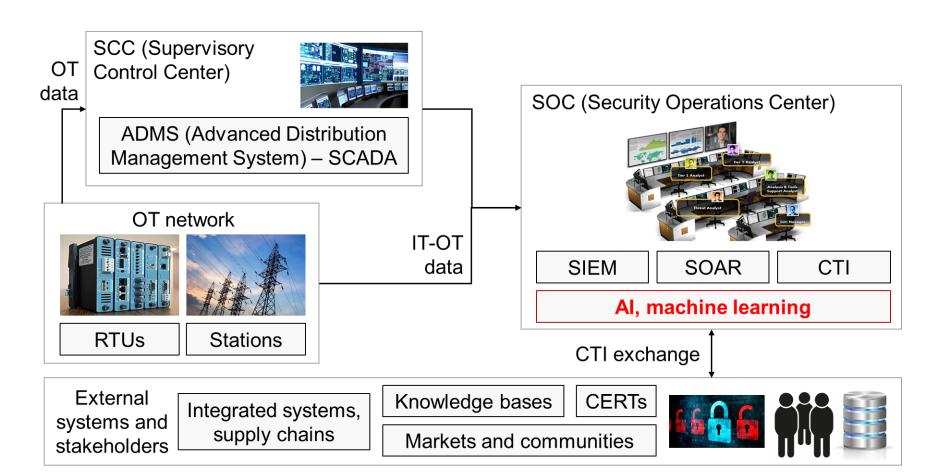


User behavior analytics



Automated response and playbooks







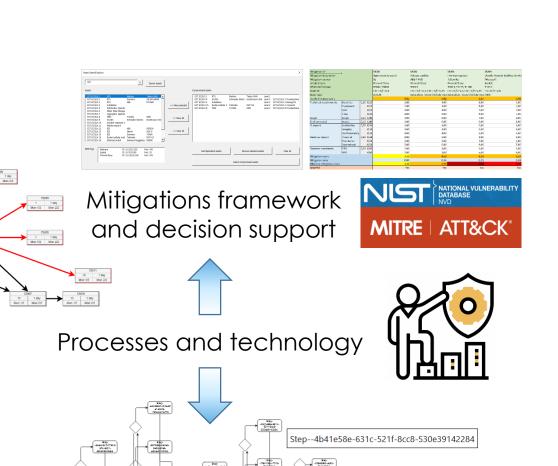
Complementary reactive and proactive approach

Cyber threats & attacks

Ð

Assets

Threat Sharing



Cooperation governance

CM01 LRYMAN NOT SPEC HOURS

CM02 EXPERT 1 day Mon 1/2 Mon 2

CM03
1 1 day
Mon 1/2 Mon 2/2

Cybersecurity

REACTIVE

ATIVNI CENTER

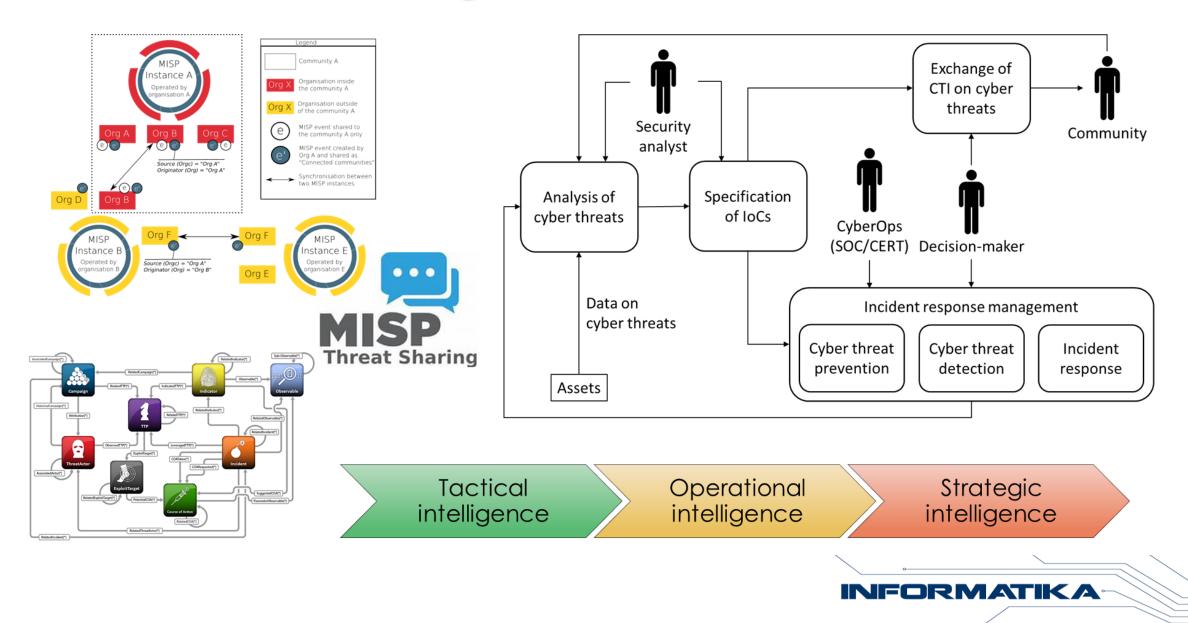
INFORMATIKA

EPES stakeholders

Incident response, reporting, and CTI

INFORMATIKA

CTI exchange in the communities



Integration of security systems and tools

List Events

Add Event

Import from.

REST client

List Attributes

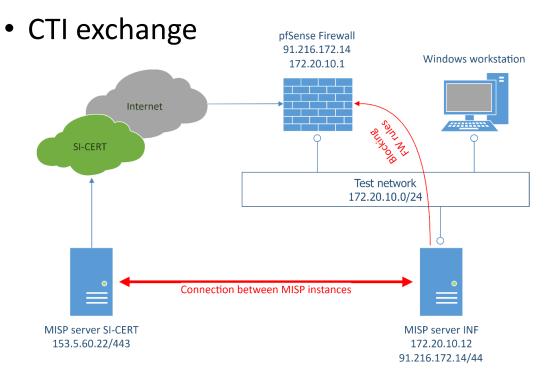
View Proposals

Events with

View dele

Export

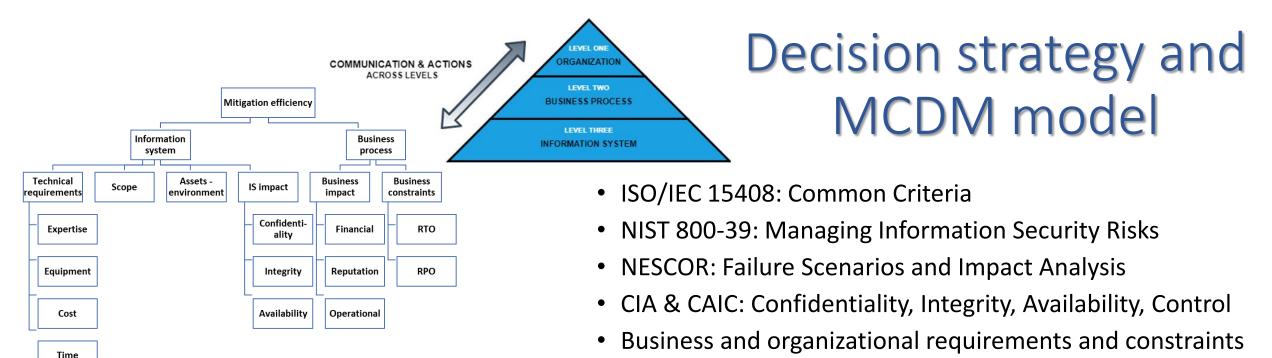
- Tools: MISP, SIEM, NG-FW, etc.
- Standard databases: NVD, MITRE ATT&CK, etc.
- Automated cyber-attack prevention and response
- Standardized reporting of incidents to CERTs
- Coordination between SOCs and CERTs



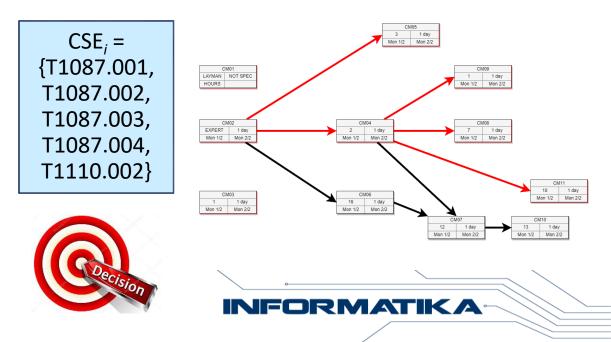
0	Date 1	Context	Category	Туре	Value	Tags
0	2024-05-24	3547b1 🖬	Payload delivery	sha256	11d571082ca1ef8ba52ed3b5301a57aaf5089tdr4be39b7ae760af544e7a377	5 🛛 +
	2024-05-24	84edfe 🗾	Object name: noki () References: 0 🖬			
0	2024-05-24	e39459 F	Other	report-incident-category: text	C4	8 +
0	2024-05-24	087a01 📰	Other	report-compromised-service: text	Bistvena stortlev ZinfV	8 +
0	2024-05-24	1e726d 📰	Other	report-crossborder-influence: text	NE	3+
0	2024-05-24	827191 🜑	Other	report-incident-source: text	Spletno mesto	3+
0	2024-05-24	443813	Other	report-incident-type: text	Izsiljevalski virus	Ø +
0	2024-05-24	b862af 🗬	Other	report-voluntary: text	Prvo poročilo o incidentu zavezanca	3+
0	2024-05-24	39c600 📰	Other	reporter-organization: text	Informatika d.o.o.	Ø +
0	2024-05-24	103b3f 🖝	Other	reporter-name: text	VOC	Ø +
0	2024-05-24	0d0e57	Other	reporter-phone-number: text	027071158	Ø +
0	2024-05-24	39cfdc 📻	Other	reporter-e-mail: text	voc@informatika.sl	Ø +
	Dashboard	Galaxies	Input Filter:	s Global Ac	tions Sync Actions Admin	introt

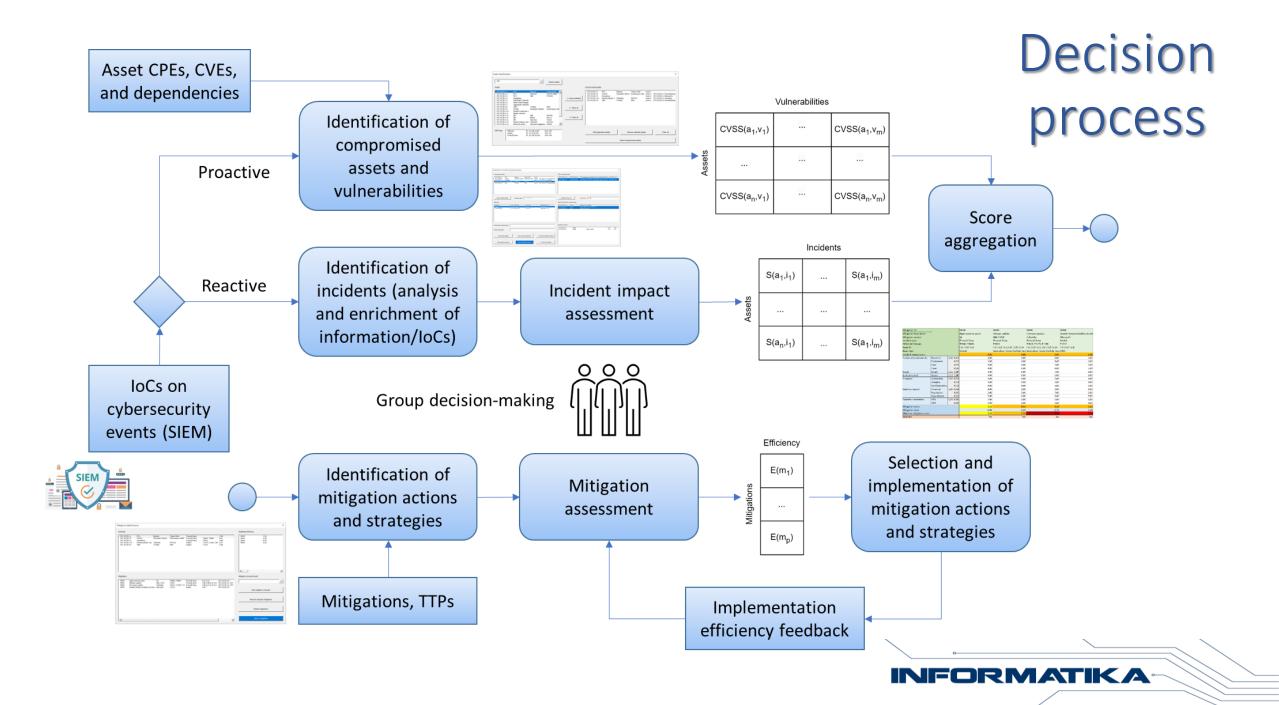
Automation Check out the OpenAPI spec of the MISP Automation API here. Dump Current Database Schema: MISP/app/Console/cake Admin dumpCurrentDatabaseSchema Scan Attachment MISP/app/Console/cake Admin scanAttachment [input] [attribute_id] [job_id] Clean Excluded Correlations: MISP/app/Console/cake Admin cleanExcludedCorrelations [job_id] Search Attributes Automating certain console tasks If you would like to automate tasks such as caching feeds or pulling from server instances, you can do PullAll: MISP/app/Console/cake Server pullAll [user_id] [full|update] Pull: MISP/app/Console/cake Server pull [user_id] [server_id] [full|update PushAll: MISP/app/Console/cake Server pushAll [user_id] View periodic summa Push: MISP/app/Console/cake Server push [user_id] [server_id] Cache Server: MISP/app/Console/cake server cacheServer [user_id] [server_id] Cache All Servers: MISP/app/Console/cake server cacheServerAll [user id] List All Feeds: MISP/app/Console/cake Server listFeeds [ison|table] View Feed: MISP/app/Console/cake Server viewFeed [feed id] [json|table] Toggle Feed Fetching: MISP/app/Console/cake Server toggleFeed [feed_id]

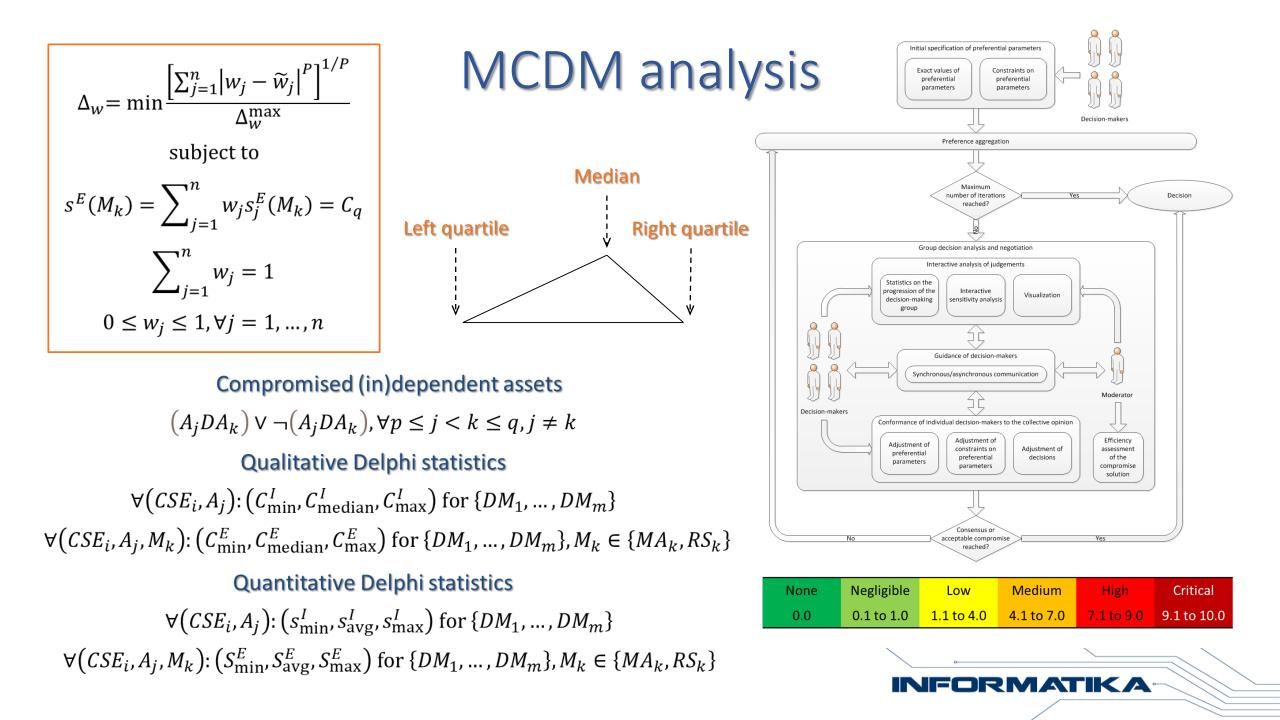
INFORMATIKA



High-level criteria Sub-criteria Measured impact SIEM magnitude 1st model: CVSS V2.0/V3.1 Safety concern Public safety concern Incident impact Workforce safety concern **Ecological concern** assessment System scale Impact on EPES Negative impact on generation capacity Negative impact on energy market Negative impact on transmission system Negative impact on customer service Destroys goodwill toward utility Privacy loss of stakeholders 2nd model: **Financial** impact Financial impact on utility Mitigation Restoration costs Immediate economic damage assessment and Long term economic damage selection Asset criticality Resilience of the compromised asset Relevance of the compromised asset







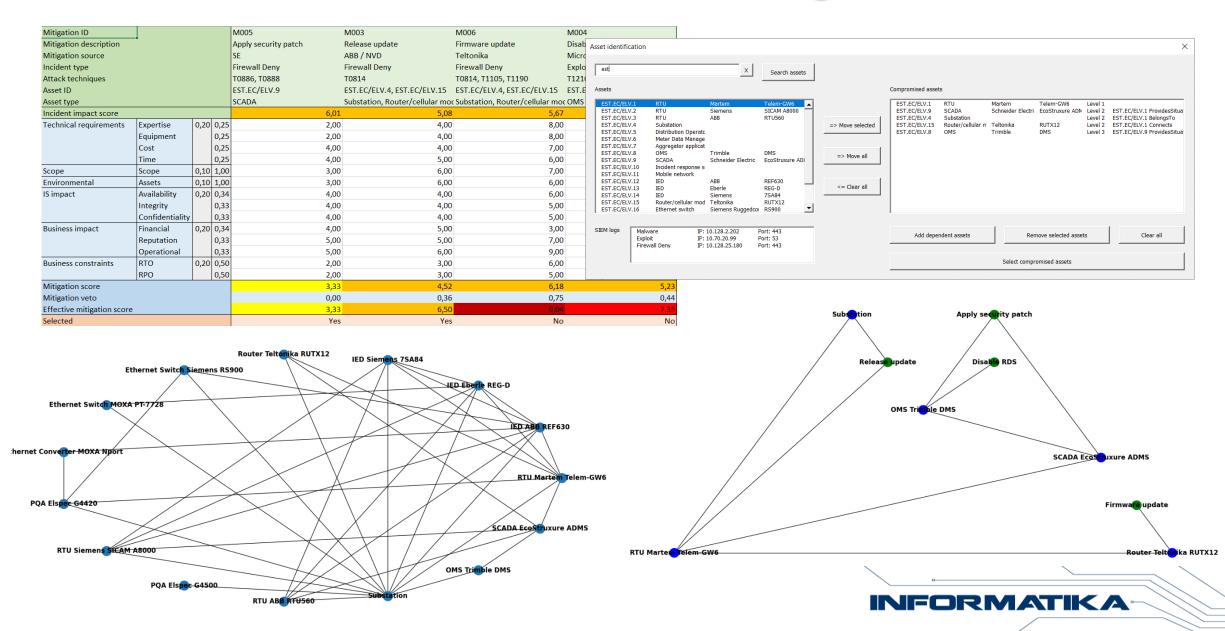
3 4 5	A A A A A A A A A A A A A A A A A A A	В		C EST.EC/	D FLV 1		EST.EC/E	E		EST.EC/EL	F V 4		EST.EC/EL	G V 15		EST.EC/ELV	H (8	
	2 Asset type			RTU			SCADA			Substation				ellular mode	em	OMS		
	3 Asset vendo	or		Marten	n			er Electric					Teltonika			Trimble		
	4 Asset produ			Telem-0				xure ADMS					RUTX12			DMS		
	5 Asset level			Level 1			Level 2			Level 2			Level 2			Level 3		
	6 Dependenc	v						ELV.1 Provi	idesSituatio		V.1 Belone	zsTo		V.1 Connec	ts		.9 Provides	Situat
	7 Incident typ			Exploit			Exploit			Firewall D		510	Firewall D			Exploit	15 TTOTACS	oncourt
	8 Attack tech						T0886, 1	0888		T0814				105, T1190)	T1210		
		t/vulnerability impact		Medium	n		High			High			Low			Medium Medium		
-	10 26 Impact 11 27 Measur	od impact		High			High High			High Low			Low High			High		
	12 28 SIEM m			Medium	n		High			Low			High			High		
	13 29 CVSS V2			High			High			Medium			Medium			High		
-	14 30 Impact			Low			Medium			High			Low			Medium		
-	15 31 Negativ			Low			High			High			Low			Medium		
T	16 32 Negativ	e impact on generation cap	acity	Medium	n		⊤ şh			High			Low			Medium		
· · .		e impact on energy market		Low			Medium	(High			Medium			Low		
		e impact on transmission sy		Mediu	m		High			High			Medium			High		
		e impact on customer services and sublities	e .	High			High			Medium			Low			Medium		
		s goodwill towards utility		Low			Medium Medium			High Medium			Low Medium			Medium Low		
	21 37 Privacy 22 38 Financia	loss of stakeholders		Low			High			High			Low			Medium		
		al impact on utility		Low			High			High			Low			Medium		
	24 40 Restora			Low			Medium	1		High			Low			Medium		
		ate economic damage		Medium	n		High			High			Medium			Low		
		rm economic damage		Medium			Medium	1		Medium			Low			Medium		
	27 43 Concerr	n		Medium	n		Medium	(High			Low			Low		
	28 44 Safety c			High			High			High			Low			Medium		
	29 45 Public si			Medium	n		High			High			Low			Medium		
	30 46 Workfor 31 47 Ecologic	rce safety concern		High			High			High			Medium			Medium		
	31 47 Ecologic 32 48 System			Low Medium	n		Low High			High High			Low Low			Low Medium		
	33 49 Asset cr			Medium			High			High			Medium			High		
		ce of the compromised asse	t	Medium			Medium			Medium			High			High		
		nce of the compromised asse		Medium			High			High			Low			Medium		
	36 Impact sco	re		Medium	n		High			High			Low			Medium		
8 D	Delphi statistics			Min	Mean	Max	Min	Mean	Max	Min	Mean	Max	Min	Mean	Max	Min	Mean	N
9	1 Incident/vuln	erability impact	1,00	5,99	6,99	8,67	3,93	5,81	7,08	3,20	5,53	6,93	4,29	6,26	8,11	3,32	5,45	7,
10	2 Measured im	pact	0,15	7,42	7,42	7,42	8,17	8,17	8,17	2,67	2,67	2,67	7,33	7,33	7,33	8,67	8,67	8,
	3 SIEM magnite		0,50	7,33	7,33	7,33	7,33	7,33	7,33	5,33	5,33	5,33	5,33	5,33	5,33	7,33	7,33	7,
	4 CVSS V2.0/V3		0,50	7,50	7,50	7,50	9,00	9,00	9,00	0,00	0,00	0,00	9,33	9,33	9,33	10,00	10,00	10,
	5 Safety concer		0,10	5,50	7,00	9,00	3,00	5,50	6,50	3,00	6,50	8,00	3,50	6,50	8,00	2,00	5,50	7,
	6 Public safety		0,50 0,50	6,00	7,00	9,00	2,00	6,00	7,00	3,00	6,00	8,00	3,00	6,00	8,00	2,00	5,00	7,
	7 Workforce sa 8 Ecological cor		0,10	5,00 3,00	7,00 5,00	9,00 10,00	4,00 6,00	5,00 7,00	6,00 8,00	3,00 6,00	7,00 8,00	8,00 9,00	4,00 4,00	7,00 8,00	8,00 10,00	2,00 5,00	6,00 6,00	7, 9,
	9 System scale	noem	0,10	7,00	8,00	9,00	4,00	6,00	7,00	5,00	6,00	7,00	5,00	6,00	9,00	2,00	5,00	6,
	LO Impact on EP	ES	0,20	5,40	6,90	8,15	2,15	4,05	5,80	2,15	4,65	6,65	2,60	4,45	6,80	1,50	3,65	5
		act on generation capacity		8,00	8,00	8,00	3,00	6,00	7,00	3,00	6,00	7,00	5,00	6,00	8,00	2,00	5,00	6,
20 1	12 Negative imp	act on energy market	0,15	7,00	8,00	9,00	2,00	5,00	7,00	3,00	6,00	8,00	5,00	6,00	8,00	2,00	5,00	6,
21 1	13 Negative imp	act on transmission system	0,15	4,00	7,00	8,00	1,00	4,00	5,00	2,00	3,00	7,00	1,00	3,00	6,00	1,00	2,00	З,
		act on customer service	0,15	5,00	7,00	8,00	3,00	4,00	5,00	1,00	4,00	5,00	1,00	4,00	6,00	1,00	3,00	6,
		dwill towards utility	0,20	6,00	8,00	10,00	3,00	4,00	7,00	2,00	6,00	9,00	3,00	6,00	9,00	2,00	5,00	8,
	16 Privacy loss of		0,20	3,00	4,00	6,00	1,00	2,00	4,00	2,00	3,00	4,00	1,00	2,00	4,00	1,00	2,00	4,
	17 Financial imp		0,20	6,00	7,25	9,25	3,00	5,50	7,50	3,00	6,25	8,00	3,75	6,25	8,00	2,25	4,75	7,
	18 Financial imp 19 Restoration c		0,25 0,25	8,00 6,00	8,00 8,00	9,00 10,00	3,00 4,00	6,00 6,00	7,00 7,00	3,00 3,00	6,00 8,00	7,00 10,00	3,00 3,00	6,00 8,00	7,00 9,00	2,00 3,00	5,00 6,00	7, 7,
		conomic damage	0,25	6,00	7,00	10,00	4,00	6,00	10,00	5,00	8,00	10,00	7,00	8,00	9,00	3,00	6,00	7, 9,
		onomic damage	0,25	4,00	6,00	8,00	1,00	4,00	6,00	1,00	3,00	5,00	2,00	3,00	6,00	1,00	2,00	6
	22 Asset criticali		0,15	7,00	7,00	8,50	2,50	5,50	7,00	2,50	6,00	8,00	4,50	6,50	9,00	2,50	5,50	8,
		the compromised asset	0,50	6,00	6,00	8,00	2,00	6,00	7,00	3,00	6,00	9,00	4,00	6,00	9,00	3,00	5,00	6,
32 2	24 Relevance of	the compromised asset	0,50	8,00	8,00	9,00	3,00	5,00	7,00	2,00	6,00	7,00	5,00	7,00	9,00	2,00	6,00	10,
33 Ir	mpact score			5,99	6,99	8,67	3,93	5,81	7,08	3,20	5,53	6,93	4,29	6,26	8,11	3,32	5,45	7
ident/v	vulnerability in	npact																
terion II		2			5			8		9			10			17		
rront	reight	0,16			0,13			0,03		0,09			0,31		(),14		0,
nent we		Measured impact	S	Safety conc	cern	Ecolog	ical conce	m	System s		Imp	act on EPI	ES	Financial		A	sset critica	lity
		1/1		2/1			6/1		4/1			1/4		1/			1/1	
easured		1/2		1/1			4/1		2/1			1/2		2/			1/2	
easured fety con	ncern			1/4			1/1		1/4			1/8		1/			1/6	
easured fety con ological	ncern I concern	1/6										1/3		1/				
easured Ifety con cological	ncern I concern ale	1/6 1/4		1/2			4/1		1/1					1/			1/1	
easured ifety con cological istem sca	ncern I concern ale 1 EPES	1/6 1/4 4/1		1/2 2/1			8/1		3/1			1/1		4/	1		2/1	
leasured afety con	ncern I concern ale 1 EPES impact	1/6 1/4		1/2											'1 '1			

Incident/Wintership/ingrat Add child criterion Incident/Wintership/ingrat Add child criterion Incident/Wintership/ingrat Add child criterion Incident/Wintership/ingrat Indicator criterion Incident Criterion Research Indicator criterion	a structuring		×
Wessured in pact Common platform enumeration Workfore safety concent Workfore safety concent Workfore safety concent Safety concent	Incident/vulnerability impact	Add shild sritaria	
 CVS V2.40/3/V4.0 Set votions Set votions		Add child criterio	
Add skilling criterion Mode criterion Mod			common platform enumeration
Image: set output ou		والمعادية والمراجع المراجع	
Workforce starty concent Useden citerion We citerion up We citerion We citerion up We citerion up We citerion up We citerion We citerion up We citerion We citerion up We citerion up We citerion up We citerion We citerion up We citerion up We citerion up We citerion up </td <td></td> <td>Add sibling criteri</td> <td></td>		Add sibling criteri	
Ecological concern Fecological concern Fequee marked Fequee			
System scale S			
Impact on EFES Impact on energy match Impact on energy match on energy match Impact on energy match on energy match Impact on energy match on energy		Delete criterion	
We gate impact on generation capacity legates impact on transmission system gegates impact on transmission system gegates impact on transmission system gegates impact on utility lestrong body it wards still y lestrong			
Image: Second and CVE management Image: Second and CVE management <td< td=""><td></td><td></td><td></td></td<>			
Megate impact on customer service betrys good/united impact on utility Financel impact on utility	Negative impact on energy market	Move criterion u	
Megatare impact on customer service bestrys good/miced impact on utility Financeal impact on utity Financeal impact on utility Financeal im	Wegative impact on transmission system		DATABASE
Privacy fies of stabeholders Privacy field and P			
Inancial impait Inancial impait Restoration cosis Inondete consonic damage Long term economic damage Restlence of the compromised asset Restle		Move criterion do	wn
Financial impact on utility Regroup criterion Immediate economic damage			
Restoration costs Long term economic damage Long term	T		
Long term economic damage L		Regroup criterio	
Long term economic damage L			
Asset critically earch and CVE management Asset CVEs Add exidence CVEs from NVD Remove selected CVEs from asset CVE 201-1225 Mint Rever VXWorls 6.4, and As, b, and CVES CVE 201-1225 Mint Rever VXWorls 6.4, and As, b, and CVES CVE 201-1225 Mint Rever VXWorls 6.4, and As, b, and CVES CVE 201-1225 Mint Rever			
earch and CVE management earch and CVE managem			
x Search asset s Asset CVEs T. EC/ELV.12 cpe:2.30::abb:relk ED ABB REF630 T. EC/ELV.13 cpe:2.30::abb:relk ED ABB REF630 Image: CVE 2019-12256 Wind River VXWorks 6.9 and vo? has a CVSs: 7.5 T. EC/ELV.13 cpe:2.31::stemens ED CVE 2019-12256 Wind River VXWorks 6.9 and vo? has a CVSs: 7.5 T. EC/ELV.13 cpe:2.31::stemens ED CVE 2019-12256 Wind River VXWorks 6.9 and vo? has a CVSs: 7.5 T. EC/ELV.13 cpe:2.31::stemens ED CVE 2019-12256 Wind River VXWorks 6.9 and vo? has a CVSs: 7.5 T. EC/ELV.13 cpe:2.31::stemens ED CVE 2019-12260 Wind River VXWorks 6.9 (A.6, 7.6, 8, CVS: 7.5 T. EC/ELV.13 cpe:2.31::stemens FEI CC/ELV.3 CVE 2019-12260 Wind River VXWorks 6.9, 4.6, 7.6, 8, CVS: 7.5 T. EC/ELV.13 cpe:2.31::stemens RTU MAR EST.EC/ELV.3 CVE 2019-12260 Wind River VXWorks 6.9, 4.6, 7.6, 8, CVS: 7.5 T. EC/ELV.2 cpe:2.31::stemens RTU MAR EST.EC/ELV.3 CVE 2019-12260 Wind River VXWorks 6.9, 4.6, 7.6, 8, CVS: 7.5 T. EC/ELV.3 cve:2.01::stemens Stort MVD Remove selected CVEs fro	Resilience of the compromised asset		
s Asset CVEs s Asset CVEs T.E.G/ELV.13 CPE-23.0:abb:relk ED ED <td< td=""><td>earch and CVE management</td><td></td><td>×</td></td<>	earch and CVE management		×
s Asset CVEs s Asset CVEs T.E.G/ELV.13 CPE-23.0:abb:relk ED ED <td< td=""><td></td><td></td><td></td></td<>			
s Asset CVEs s Asset CVEs T.E.G/ELV.13 CPE-23.0:abb:relk ED ED <td< td=""><td>Y .</td><td></td><td></td></td<>	Y .		
T. C/CEV.112 cpe:2.3:usabbrelic ED		Search assets	
T.EC/EU.V.3 E/D Eberie REG-D T.EC/EU.V.3 CVE-2019-12258 Wind River VXWorks 6.6, 61, 63, 69, OVSS: 5 T.EC/EU.V.15 cpe:2.3:htelbonia Router/cellular mo Telsonika T.EC/EU.V.15 cpe:2.3:htelbonia Scale Jensonia CVE-2019-12263 Wind River VXWorks 6.6, 40, 66, 67, 68, 69 CVSS: 7.5 T.EC/EU.V.3 cvE-2019-12263 Wind River VXWorks 6.6, 67, 68, 69 CVSS: 5.6 CVE-2019-12263 Wind River VXWorks 6.6, 67, 68, 69 CVSS: 5.8 T.EC/EU.V.3 cvE-2019-12263 Wind River VXWorks 6.6, 67, 68, 69 CVSS: 5.8 EST.EC/EU.V.3 CVE-2019-12263 Wind River VXWorks 6.6, 67, 68, 69 CVSS: 5.8 EST.EC/EU.V.3 cvE-2019-12263 Wind River VXWorks 6.6, 67, 68, 69 CVSS: 5.8 EST.EC/EU.V.3 CVE-2019-12263 Wind River VXWorks 6.6, 67, 68, 69 CVSS: 5.8 T.EC/EU.V.4 <td< td=""><td>s</td><td>Ass</td><td>et CVEs</td></td<>	s	Ass	et CVEs
T.EC/EUV.13 ED Eberie REG-D T.EC/EUV.14 Ger2.31:hteltonika Subtractional Standard Standa	T EC/ELV 12 could supply the ED APP	DEE620	CT_EC/ELV/2 CVE_2010_122E6 Wind Biver VMMerks 6.0 and w7 bac a CVCC+7.5
T.EC/EUV.14 cpe:2.3:h:demens ED Siemens 75.84 T.EC/EUV.15 cpe:2.3:h:demons Retriever/cellular mo Telonika RMTX12 T.EC/EUV.15 cpe:2.3:h:demons Ethernet switch Siemens Ruggedo RS900 T.EC/EUV.16 cpe:2.3:h:demons Ethernet switch MOXA Nport sep: T.EC/EUV.12 cpe:2.3:h:demons Ethernet switch MOXA Nport sep: Power Quality Anal Espec C4420 Siemens Siemens Siemens T.EC/EUV.12 cpe:2.3:h:demons RTU Siemens Siemens Siemens Siemens Siemens Siemens Siemens Siemens Siemens CVE:2019-1226 Wind Rver VWorks 6.9, 6.6, 6.7, 6.8, 6.9 CVSS: 7.5 T.EC/EUV.13 cpe:2.3:h:demons FTU Siemens			
T.EC/EUV.16 cp::2.3:b:siemens Ethernet switch Siemens Ruggedo R5900 T.EC/EUV.17 cp::2.3:b:siemens Serial-Ethernet Co. MXA Nport serial T.EC/EUV.18 cp::2.3:b:siemens Serial-Ethernet Co. MXA Nport serial T.EC/EUV.19 cp::2.3:b:siemens Serial-Ethernet Co. MXA Nport serial T.EC/EUV.29 cp::2.3:b:siemens RTU Siemens Sickal To T.EC/EUV.29 cp::2.3:b:siemens RTU Siemens Sickal To T.EC/EUV.29 cp::2.3:b:siemens RTU Siemens Sickal To T.EC/EUV.29 cp::2.3:b:rsiemens RTU Siemens Sickal To T.EC/EUV.29 cp::2.3:b:rsiemens RTU Siemens Sickal To T.EC/EUV.29 cp::2.3:b:rsiemens RTU Siemens Sickal To T.EC/EUV.3 cv:2:0:1:2:1:2:2:5 Improper Input Validation vulnerability CVS: 5:5 T.EC/EUV.4 Substation Search CVE ID Remove selected CVEs from NVD Remove selected CVEs from asset Clear all //D search X Search CVE ID Search CVE ID CVE-2001-0832 </td <td></td> <td></td> <td>EST.EC/ELV.3 CVE-2019-12259 Wind River VxWorks 6.6, 6.7, 6.8, 6.9 CVSS: 5</td>			EST.EC/ELV.3 CVE-2019-12259 Wind River VxWorks 6.6, 6.7, 6.8, 6.9 CVSS: 5
T.EC/EU.V.17 cp::2.3:b:moxa;pt Ethernet switch MOXA PT-778 r.EC/EU.V.19 cp::2.3:b:moxa;p: Serial-Ethernet Co: MOXA PT-778 r.EC/EU.V.19 cp::2.3:b:moxa;p: Serial-Ethernet Co: Not Series C420 r.EC/EU.V.20 cp::2.3:b:moxa;p: Serial-Ethernet Co: Not Series C420 T.EC/EU.V.20 cp::2.3:b:moxa;pt Stimmens SICAM A EST.EC/EU.V.3 CVE-2019-12263 Wind River VWWorks 6.5, 6.6, 6.7, 6.8, CVSS; 5 T.EC/EU.V.20 cp::2.3:b:moxa;pt Ethernet Switch Ad8 RTU500 CVE-2021-27196 Wind River VWWorks 6.5, 6.6, 6.7, 6.8, CVSS; 5 T.EC/EU.V.3 cp::2.3:b:moxa;pt Ethernet Switch Rtu Rtu Stimmens CVE-2021-27196 Wind River VWWorks 6.5, 6.7, 6.8, CVSS; 5 EST.EC/EU.V.3 cp::2.3:b:moxa;pt Rtu Ad8 Rtu/1500 CVE-2021-27196 Wind River VWWorks 6.5, 6.6, 6.7, 6.8, CVSS; 5 Search CVE Search CVE in All Selected CVEs from NVD Remove selected CVEs from asset Clear all //D search Search CVE ID VVD CVEs CVE-2001-0832 Vulnerability in Oracle 8.0, x through 9.0,1; V.0 2.1 CVE-2005-027			EST.EC/ELV.3 CVE-2019-12260 Wind River VxWorks 6.9 and vx7 has a CVSS: 7.5
T.EC/EU.18 cpe:2.3:h:moxa:np Serial=Ethernet Cor MOXA Nport ser T.EC/EU.12 cpe:2.3:h:moxa:np Serial=Ethernet Cor MOXA Nport ser T.EC/EU.2 cpe:2.3:h:moxa:np Serial=Espec G420 T.EC/EU.2 cpe:2.3:h:moxa:np Siemens SICMA A T.EC/EU.4 Substation FT.EC/EU.3 CVE-2021-2216 Wind Never VXWorks 6.5, 6.6, 7.6, 8, CVSS: 5 T.EC/EU.4 Substation FT.EC/EU.3 CVE-2021-2219 Improper Input Validation vulnerability CVSS: 5 T.EC/EU.4 Substation FT.EC/EU.3 CVE-2021-2219 Improper Input Validation vulnerability CVSS: 5 T.EC/EU.4 Substation FT.EC/EU.3 CVE-2021-221-2219 Improper Input Validation vulnerability CVSS: 5 T.EC/EU.4 Substation FT.EC/EU.3 CVE-2021-221-2219 Improper Input Validation vulnerability CVSS: 5 T.EC/EU.4 Search CVE ID VVD CVEs <td< td=""><td></td><td></td><td></td></td<>			
T. EC/ELV.2 cpe:2.3:h:siemens StiCAM AT T. EC/ELV.3 CVE-2021-27196 Improper Input Validation vulnerability CVSS: 5 T. EC/ELV.3 cpe:2.3:h:siemens StiCAM AT StiCAM AT StiCAM AT T. EC/ELV.4 Substation SticAM AT StiCAM AT StiCAM AT Copy selected CPE to NVD search Retrieve current CVEs of selected asset Add selected CVEs from NVD Remove selected CVEs from asset Clear all CVE 2001-0832 Vulnerability in Oracle 8.0.x through 9.0.1 on Unix allow: V2.0 2.1 CVE 2001-0832 Vulnerability in Oracle 8.0.x through 9.0.1 in VD.0 7.2 CVE ID X Search CVE ID CVE-2001-0832 Vulnerability in Oracle 8.0.x through 9.0.1 in VD.0 7.2 VE ID X Search CVE ID CVE-2001-0832 Vulnerability in Oracle 8.0.x through 9.0.1 in V2.0 7.2 VE ID X Search CVE ID CVE-2002-0237 SQL injection vulnerability in Oracle 8.0.x through 9.0.1 in V2.0 7.2 VE ID X Search keywords CVE-2002-7237 Multiple buffer overflow in othrcre in Oracle 8.0.x through 9.0.1 in V2.0 7.2 VE ID X Search keywords X <			EST.EC/ELV.3 CVE-2019-12261 Wind River VxWorks 6.7 though 6.9 an CVSS: 7.5
T.EC/ELV.20 Power Quality Anal Elspec G4500 T.EC/ELV.3 cpe:2.3:h:abbrtu5 RTU ABB RTU500 T.EC/ELV.4 Substation Image: Comparison of the com	T.EC/ELV.18 cpe:2.3:h:moxa:np Serial-Ethernet Coi MOXA	PT-7728 E Nport ser	EST.EC/ELV.3 CVE-2019-12261 Wind River VxWorks 6.7 though 6.9 an CVSS: 7.5 SST.EC/ELV.3 CVE-2019-12262 Wind River VxWorks 6.6, 6.7, 6.8, 6.9 CVSS: 7.5 SST.EC/ELV.3 CVE-2019-12263 Wind River VxWorks 6.9 and vx7 has CVSS: 6.8
T.EC/ELV.3 cpe:2.3:h:abbs/tub RTU ABB RTU560 T.EC/ELV.4 Substation Substation Image: Control of the state of	T.EC/ELV.18 cpe:2.3:h:moxa:nr Serial-Ethernet Coi MOXA T.EC/ELV.19 Power Quality Anal Elspec	PT-7728 E Nport ser E G4420 E	EST.EC/ELV.3 CVE-2019-12261 Wind River VXWorks 6.7 though 6.9 an CVSS: 7.5 EST.EC/ELV.3 CVE-2019-12262 Wind River VXWorks 6.6, 6.7, 6.8, 6.9 CVSS: 7.5 EST.EC/ELV.3 CVE-2019-12263 Wind River VXWorks 6.6, 6.7, 6.8, 6.9 CVSS: 7.5 EST.EC/ELV.3 CVE-2019-12263 Wind River VXWorks 6.9, 4.4 and wc7 has CVSS: 6.8 EST.EC/ELV.3 CVE-2019-12265 Wind River VXWorks 6.5, 6.6, 6.7, 6.8, CVSS: 5
Add selected CPE to NVD search Retrieve current CVEs of selected asset Add selected CVEs from NVD Remove selected CVEs from asset Clear all //D search NVD CVEs PE name pe:2.3:a:oracle:database_server:-+*;****** × Search CPE name NVD CVEs VE ID X Search CVE ID OVE-2001-0832 Wulnerability in Oracle 8.0.x through 9.0.1 on Unix allow: V2.0 7.2 VE ID X Search CVE ID OVE-2001-0833 Multiple buffer overflow in otrcrep in Oracle 8.0.x through 9.0.1 i V2.0 7.2 eywords X Search CVE ID OVE-2005-0727 Nulnerability in Oracle Databases 9.2 V2.0 7.5 eywords X Search keywords V2.0 7.2 4.0 VE description Multiple unspecified vulnerabilities in the Vorkspace Mar V2.0 6.5 V2.0 6.6 VE description CVE-2007-5531 SQL injection vulnerability in the Vorkspace Mar V2.0 6.5 0.7 6.5 VE description CVE-2007-5531 SQL injection vulnerability in the Vorkspace Mar V2.0 6.5 0.7 6.5 VE description CVE-2007-5531 SQL injection vulnerability in the Vorkspace Mar V2.0 6.5	T.EC/ELV.18 cpe:2.3:h:moxa:nr Serial-Ethernet Coi MOXA T.EC/ELV.19 Power Quality Anal Elspec T.EC/ELV.2 cpe:2.3:h:siemens RTU Siemens	PT-7728 Nport ser G4420 SICAM A	EST.EC/ELV.3 CVE-2019-12261 Wind River VXWorks 6.7 though 6.9 an CVSS: 7.5 EST.EC/ELV.3 CVE-2019-12262 Wind River VXWorks 6.6, 6.7, 6.8, 6.9 CVSS: 7.5 EST.EC/ELV.3 CVE-2019-12263 Wind River VXWorks 6.6, 6.7, 6.8, 6.9 CVSS: 7.5 EST.EC/ELV.3 CVE-2019-12263 Wind River VXWorks 6.9, 4.4 and wc7 has CVSS: 6.8 EST.EC/ELV.3 CVE-2019-12265 Wind River VXWorks 6.5, 6.6, 6.7, 6.8, CVSS: 5
Dopy selected CPE to NVD search Retrieve current CVEs of selected asset Add selected CVEs from NVD Remove selected CVEs from asset Clear all 70 search PFE name pe:2.3:a:oracle:/database_server:-:******** X Search CPE name VVD CVEs VE ID X Search CVE ID Withfer overflow in otrcrep in Oracle 8.0.x through 9.0.1 a V2.0 7.2 VE ID X Search CVE ID Withfer overflows in the XML Database (XOB) fun V2.0 2.1 VVE ID X Search CVE ID Withfer overflows in the XML Database (XOB) fun V2.0 7.2 VCF-2005-0297 SQL injection vulnerability in Oracle Database 91 and 10; V2.0 7.5 VCF-2005-701 Directory traversal vulnerability in Oracle Databases 94 v2.0 5.0 VCF-2005-7021 Absolute path traversal vulnerability in Oracle Database 94 v2.0 6.0 CVF-2005-7510 Multiple burgencifed vulnerability in Oracle Database 94 v2.0 6.5 VE description CVF-2007-5510 Multiple outrerability in Workspace Manager for 07 V2.0 6.5 CVF-2007-5937 Buffer overflow in MDSYS.SDD_CS in Oracle Database 94 v2.0 6.5 CVF-2007-5937 Unspecified vulnerability in the Logical Standby component in Oracle Dat	T.EC/ELV.18 cpe:2.3:h:moxa:n; Serial-Ethernet Cor MOXA T.EC/ELV.19 Power Quality Anal Elspec T.EC/ELV.2 cpe:2.3:h:siemens RTU Siemens T.EC/ELV.20 Power Quality Anal Elspec	PT-7728 PT-778 PT-7	EST.EC/ELV.3 CVE-2019-12261 Wind River VxWorks 6.7 though 6.9 an CVSS: 7.5 EST.EC/ELV.3 CVE-2019-12262 Wind River VxWorks 6.6, 6.7, 6.8, 6.9 CVSS: 7.5 EST.EC/ELV.3 CVE-2019-12263 Wind River VxWorks 6.9.4 and vx7 has CVSS: 6.8 EST.EC/ELV.3 CVE-2019-12265 Wind River VxWorks 6.5, 6.6, 6.7, 6.8, CVSS: 5
D search NVD CVEs PFE name pe:2.3:a:oracle:database_server::******** x Search CPE name VVE ID x Search CVE ID ewwords x Search CVE ID ewwords x Search keywords VVE description x Search keywords x VVE 2007-5921 SQL injection vulnerability in Oracle Database V2.0 6.5 VVE 2007-5925 Oracle Database server 10g Release 2 allows local user v2.0 6.5 VVE 2007-5926 SQL injection vulnerability in Vorksp	T.EC/EU.V18 cpe:2.3:h::moxa:nc Serial-Ethernet Cor MOXA T.EC/EU.V2 Power Quality Anal Elspec T.EC/EU.V2 cpe:2.3:h::siemens RTU Siemens T.EC/EU.V2 power Quality Anal Elspec T.EC/EU.V2 power Quality Anal Elspec T.EC/EU.V3 oper2.3:h:sibbrrtu5 RTU A88	PT-7728 PT-778 PT-7	EST.EC/ELV.3 CVE-2019-12261 Wind River VXWorks 6.7 though 6.9 an CVSS: 7.5 EST.EC/ELV.3 CVE-2019-12262 Wind River VXWorks 6.6, 6.7, 6.8, 6.9 CVSS: 7.5 EST.EC/ELV.3 CVE-2019-12263 Wind River VXWorks 6.6, 6.7, 6.8, 6.9 CVSS: 7.5 EST.EC/ELV.3 CVE-2019-12263 Wind River VXWorks 6.9, 4.4 and wc7 has CVSS: 6.8 EST.EC/ELV.3 CVE-2019-12265 Wind River VXWorks 6.5, 6.6, 6.7, 6.8, CVSS: 5
D search NVD CVEs PFE name pe:2.3:a:oracle:database_server::******** x Search CPE name VVE ID x Search CVE ID ewwords x Search CVE ID ewwords x Search keywords VVE description x Search keywords x VVE 2007-5921 SQL injection vulnerability in Oracle Database V2.0 6.5 VVE 2007-5925 Oracle Database server 10g Release 2 allows local user v2.0 6.5 VVE 2007-5926 SQL injection vulnerability in Vorksp	T.EC/EU.V18 cpe:2.3:h::moxa:nc Serial-Ethernet Cor MOXA T.EC/EU.V2 Power Quality Anal Elspec T.EC/EU.V2 cpe:2.3:h::siemens RTU Siemens T.EC/EU.V2 power Quality Anal Elspec T.EC/EU.V2 power Quality Anal Elspec T.EC/EU.V3 oper2.3:h:sibbrrtu5 RTU A88	PT-7728 PT-778 PT-7	ST.EC/ELV.3 CVE-2019-12261 Wind River VXWorks 6.7 though 6.9 an CVSS: 7.5 ST.EC/ELV.3 CVE-2019-12262 Wind River VXWorks 6.6, 6.7, 6.8, 6.9 CVSS: 7.5 ST.EC/ELV.3 CVE-2019-12263 Wind River VXWorks 6.9, 4 and vx7 has CVSS: 6.8 ST.EC/ELV.3 CVE-2019-12265 Wind River VXWorks 6.9, 4 and vx7 has CVSS: 6.8 ST.EC/ELV.3 CVE-2019-12265 Wind River VXWorks 6.5, 6.6, 6.7, 6.8, CVSS: 5 ST.EC/ELV.3 CVE-2021-27196 Improper Input Validation vulnerability CVSS: 5
PE name pe:2.3:a:orade:database_server::******* × Search CPE name VVD CVEs VE ID x Search CVE ID VC + 2001-0832 Wulnerability in Oracle 8.0.x through 9.0.1 or Unix allows: V2.0 2.1 VE ID x Search CVE ID VC + 2003-0727 Multiple Under overflows in the XML Database (XDB) fm V2.0 2.1 VE ID x Search CVE ID Differ overflows in the XML Database (XDB) fm V2.0 2.1 VE ID x Search keywords CVE-2003-027 SQL injection vulnerability in Oracle Database 91 and 10; V2.0 7.5 eywords x Search keywords CVE-2005-071 Directory traversal vulnerability in Oracle Database 54: V2.0 10.0 CVE-2005-0721 Multiple unspecified vulnerability in Oracle Database 54: V2.0 10.0 CVE-2005-071 Urspecified vulnerability in the Logical Standby component in Oracle Database 54: V2.0 6.5 CVE-2007-5511 SQL injection vulnerability in Oracle Database 70: V2.0 6.5 CVE-2007-5511 SQL injection vulnerability in the Logical Standby component in Oracle Database 70: V2.0 6.5 CVE-2007-5531 SQL injection vulnerability in the Logical Standby component in CVE-2007-5534 0racle allows remote attackers to obtain server memory V2.0	T.EC/EU.V18 cpe:2.3:h::moxa:nc Serial-Ethernet Cor MOXA T.EC/EU.V2 Power Quality Anal Elspec T.EC/EU.V2 cpe:2.3:h::siemens RTU Siemens T.EC/EU.V2 power Quality Anal Elspec T.EC/EU.V2 power Quality Anal Elspec T.EC/EU.V3 oper2.3:h:sibbrrtu5 RTU A88	PT-7728 PT-778 PT-7	ST.E.C/ELV.3 CVE-2019-12261 Wind River VXWorks 6.7 though 6.9 an CVSS: 7.5 ST.E.C/ELV.3 CVE-2019-12262 Wind River VXWorks 6.6, 6.7, 6.8, 6.9 CVSS: 7.5 ST.E.C/ELV.3 CVE-2019-12263 Wind River VXWorks 6.5, 6.4 and vor has CVSS: 6.8 ST.E.C/ELV.3 CVE-2019-12265 Wind River VXWorks 6.5, 6.6, 6.7, 6.8, CVSS: 6.8 Wind River VXWorks 6.5, 6.6, 6.7, 6.8, CVSS: 5 ST.E.C/ELV.3 CVE-2021-27196 Improper Input Validation vulnerability CVSS: 5
PE name pe:2.3:a:orade:database_server::******** × Search CPE name VVD CVEs VE ID x Search CPE ID VE ID x Search CVE ID VCV=2001-0832 Suffer overflow in otrcre pin Oracle 8.0.x through 9.0.1 averflow in the XML Database (XDB) for V2.0 VE ID x Search CVE ID eywords x Search keywords VE code-cole 0.01 oracle 0.01 babase (XDB) for V2.0 2.1 VE description Viet code-cole 0.01 oracle 0.01 babase (XDB) for V2.0 5.0 VE description Viet code-cole 0.01 oracle 0.01 babase (XDB) for CV2.0 6.5 VE-2007-5511 SQL injection vulnerability in Oracle 0.01 babase (XDB) for V2.0 6.5 VVE-2007-5515 SQL injection vulnerability in oracle 0.01 babase (XDB) for V2.0 6.5 VVE-2007-5515 SQL injection vulnerability in oracle 0.01 babase (XDB) for V2.0 6.5 VVE-2007-5515 SQL injection vulnerability in oracle 0.01 babase (XDB) for V2.0 6.5 VVE-2007-5515 SQL injection vulnerability in oracle 0.01 babase (XDB) for V2.0 6.5	T.EC/EUV.18 cpe:2.3:h:moxa:nr Serial-Ethernet Cor MOXA T.EC/EUV.19 power Quality Anal Elspec T.EC/EUV.2 cpe:2.3:h:siemens RTU Siemens T.EC/EUV.2 cpe:2.3:h:siemens RTU Siemens T.EC/EUV.2 Siemens T.EC/EUV.2 cpe:2.3:h:sibb:rtuS RTU A88 T.EC/EUV.4 Substation Sibbstation Sibbstation	PT-7728 Nport ser G4420 SICAM AF G4500 RTU550	STF.EC/ELV.3 CVE-2019-12261 Wind River VXWorks 6.7 though 6.9 an CVSS: 7.5 STF.EC/ELV.3 CVE-2019-12262 Wind River VXWorks 6.6, 6.7, 6.8, 6.9 CVSS: 7.5 STF.EC/ELV.3 CVE-2019-12263 Wind River VXWorks 6.9.4 and vx7 has CVSS: 6.8 STF.EC/ELV.3 CVE-2019-12265 Wind River VXWorks 6.9.4 and vx7 has CVSS: 5 STF.EC/ELV.3 CVE-2019-12265 Wind River VXWorks 6.5, 6.6, 6.7, 6.8, CVSS: 5 ST.EC/ELV.3 CVE-2021-27196 Improper Input Validation vulnerability CVSS: 5
VE ID X Search CVE ID CVE-2001-0832 Vulnerability in Oracle 8.0.x through 9.0.1 on Unix allows V2.0 2.1 VE ID X Search CVE ID Search CVE ID CVE-2001-0832 Suffer overflows in the XML Database (XDB) fun V2.0 2.1 eywords X Search CVE ID Oracle 3.0.x through 9.0.1 on Unix allows V2.0 2.1 eywords X Search keywords Oracle 3.0.x through 9.0.1 on Unix allows V2.0 2.1 VE description X Search keywords Oracle 3.0.x through 9.0.1 on Unix allows V2.0 2.1 VE description X Search keywords V2.0 5.0 Oracle 3.0.x through 9.0.1 on Unix allows V2.0 5.0 VE description VC V2.0 6.1 Oracle 3.0.x through 9.0.1 on Unix allows V2.0 6.0 VE description VC CVE-2005-751 Multiple unspecified vulnerability in Oracle 3.0.x through 9.0.1 on Unix allows V2.0 6.5 VE description VC CVE-2007-551 SQL injection vulnerability in Oracle 3.0.x through 9.0.1 on Unix allows V2.0 6.5 VE description VC-2007-551 SQL injection vulnerability in Oracle 3.0.x through	T.EC/EU.V.18 cpe:2.3:h::moxa:nc Serial-Ethernet Cor MOXA T.EC/EU.V.2 cpe:2.3:h::siemens Power Quality Anal Elspec T.EC/EU.V.2 cpe:2.3:h::abbrtus RTU Siemens T.EC/EU.V.2 cpe:2.3:h::abbrtus RU ABB T.EC/EU.V.4 Substation	PT-7728 Nport ser G4420 SICAM AF G4500 RTU550	STF.EC/ELV.3 CVE-2019-12261 Wind River VXWorks 6.7 though 6.9 an CVSS: 7.5 STF.EC/ELV.3 CVE-2019-12262 Wind River VXWorks 6.6, 6.7, 6.8, 6.9 CVSS: 7.5 STF.EC/ELV.3 CVE-2019-12263 Wind River VXWorks 6.9.4 and vx7 has CVSS: 6.8 STF.EC/ELV.3 CVE-2019-12265 Wind River VXWorks 6.9.4 and vx7 has CVSS: 5 STF.EC/ELV.3 CVE-2019-12265 Wind River VXWorks 6.5, 6.6, 6.7, 6.8, CVSS: 5 ST.EC/ELV.3 CVE-2021-27196 Improper Input Validation vulnerability CVSS: 5
VE ID X Search CVE ID Search CVE ID CVE-2003-0727 Suffer overflow in other ability in Oracle Babases 91 and 100 and 100 are 120.0 7.5 eywords X Search CVE ID CVE-2005-0721 Solution and 100 and 100 and 100 are 120.0 7.5 eywords X Search Keywords Search cVE ID CVE-2005-0721 Solution and 100 a	T.EC/ELV.18 cpe:2.3:h:moxa:nc Serial-Ethermet Cor MOXA T.EC/ELV.20 rpe:2.3:h:siemens Power Quality Anal Elspec T.EC/ELV.20 cpe:2.3:h:siemens Power Quality Anal Elspec T.EC/ELV.20 cpe:2.3:h:siemens Power Quality Anal Elspec T.EC/ELV.4 cpe:2.3:h:sibbrtus Rut ABB	PT-7728 Nport ser G4420 SICAM AF G4500 RTU560 asset Add select	ST.EC/ELV.3 CVE-2019-12261 Wind River VXWorks 6.7 though 6.9 an CVSS: 7.5 ST.EC/ELV.3 CVE-2019-12262 Wind River VXWorks 6.9.4 and vx7 has CVSS: 6.8 ST.EC/ELV.3 CVE-2019-12263 Wind River VXWorks 6.9.4 and vx7 has CVSS: 6.8 ST.EC/ELV.3 CVE-2019-12263 Wind River VXWorks 6.9.4 and vx7 has CVSS: 6.8 ST.EC/ELV.3 CVE-2019-12263 Wind River VXWorks 6.5, 6.6, 6.7, 6.8, 6.9 CVSS: 5 ST.EC/ELV.3 CVE-2019-12263 Wind River VXWorks 6.5, 6.6, 6.7, 6.8, CVSS: 5 S ST.EC/ELV.3 CVE-2021-27196 Improper Input Validation vulnerability CVSS: 5 ad CVEs from NVD Remove selected CVEs from asset Clear all
VE ID X Search CVE ID CVF-2005-0727 Multiple buffer overflows in the XML Database (XDB) fun V2.0 2.1 VE ID X Search CVE ID CVF-2005-0727 SQL injection vulnerability in Oracle Database 91 and 102 V2.0 7.5 ewwords X Search keywords Oracle Database Server 10g Release 2 allows local user V2.0 4.6 CVF-2005-0711 Absolute path traversal vulnerability in Oracle Database 91 and 102 0.0 CVF-2005-0714 VE description X Search keywords Oracle Database Server 10g Release 2 allows local user V2.0 4.6 CVF-2005-0711 Absolute path traversal vulnerability in Oracle Database V2.0 6.0 CVF-2007-5511 SQL injection vulnerability in Oracle Database 91 and 102.0 6.5 CVF-2007-5511 SQL injection vulnerability in Morkspace Manager for Or V2.0 6.5 CVF-2007-5591 Buffer overflow in MDSYS.SDO_CS in Oracle Database 5 V2.0 6.5 CVF-2007-5931 Buffer overflow in MDSYS.SDO_CS in Oracle Database 5 V2.0 6.8 CVF-2007-5931 Buffer overflow in MDSYS.SDO_CS in Oracle Database 5 V2.0 6.8 CVF-2007-5931 The instaliation procese for Oracle 103 and II guesas acc V2.0 <	T.EC/ELV.18 cpe:2.3:h:moxa:n; Serial-Ethernet Cor MOXA T.EC/ELV.19 power Quality Anal Elspec T.EC/ELV.20 cpe:2.3:h:siemens Power Quality Anal Elspec T.EC/ELV.20 cpe:2.3:h:abb:rtu5 RTU AB8 T.EC/ELV.4 Substation Substation	PT-7728 Nport ser G4420 SICAM AF G4500 RTUS60 asset Add select	ST.EC/ELV.3 CVE-2019-12261 Wind River VXWorks 6.7 though 6.9 an CVSS: 7.5 ST.EC/ELV.3 CVE-2019-12262 Wind River VXWorks 6.9.4 and voc has CVSS: 6.8 ST.EC/ELV.3 CVE-2019-12263 Wind River VXWorks 6.9.4 and voc has CVSS: 6.8 ST.EC/ELV.3 CVE-2019-12265 Wind River VXWorks 6.9.4 and voc has CVSS: 6.8 ST.EC/ELV.3 CVE-2019-12265 Wind River VXWorks 6.9.4 and voc has CVSS: 5 ST.EC/ELV.3 CVE-2019-12265 Improper Input Validation vulnerability CVSS: 5 ST.EC/ELV.3 CVE-2021-27196 Improper Input Validation vulnerability CVSS: 5 ad CVEs from NVD Remove selected CVEs from asset Clear all
viewords VCVE-2005-0701 Directory traversal vulnerability in Oracle Database Serv. V2.0 5.0 veywords X Search keywords Oracle Database Serv. V2.0 5.0 VE description X Search keywords Oracle Database Serv. V2.0 6.0 VE description VCVE-2005-7318 Multiple unspecified vulnerability in Oracle Database Serv. V2.0 6.0 VE description VCVE-2007-5511 SQL injection vulnerability in Vorkspace Manager for Or V2.0 6.5 VCVE-2007-5511 SQL injection vulnerability in Vorkspace Manager for Or V2.0 6.5 VE description CVE-2007-5511 SQL injection vulnerability in Vorkspace Manager for Or V2.0 6.5 VE-2007-5511 SQL injection vulnerability in Vorkspace Manager for Or V2.0 6.5 CVE-2007-5519 Orde Database endows remote attackers to obtain server memory V2.0 7.1 CVE-2007-5519 Buffer overflow in MDSYS.SOLO CS in Oracle Database V2.0 6.8 CVE-2007-5510 Unspecified vulnerability in the Logical Standby component in Oracle Database servers on affect V2.0 6.8 CVE-2001-1321 The kg accept krb5 function in krb3/scept.sec_conter V2.0 6.8 CVE-2014-6483 Unspecified vulnerability in the Application Express comp V2.0	T.EC/ELV.18 cpe:2.3:h:moxa:n; Serial-Ethernet Cor MOXA T.EC/ELV.20 cpe:2.3:h:siemens Power Quality Anal Elspec T.EC/ELV.20 cpe:2.3:h:siemens Power Quality Anal Elspec T.EC/ELV.4 cpe:2.3:h:abb:rtu5 RTU ABB T.EC/ELV.4 Substation	PT-7728 Nport ser G420 SICAM AC RTU560 RTU56	EST.EC/ELV.3 CVE-2019-12261 Wind River VXWorks 6.7 though 6.9 an CVSS: 7.5 EST.EC/ELV.3 CVE-2019-12262 Wind River VXWorks 6.9.4 and vxO has CVSS: 7.5 EST.EC/ELV.3 CVE-2019-12263 Wind River VXWorks 6.9.4 and vxO has CVSS: 6.8 EST.EC/ELV.3 CVE-2019-12263 Wind River VXWorks 6.9.4 and vxO has CVSS: 6.8 EST.EC/ELV.3 CVE-2019-12263 Wind River VXWorks 6.9.6 and vxO has CVSS: 5 EST.EC/ELV.3 CVE-2019-12263 Wind River VXWorks 6.9.6 and vxO has CVSS: 5 ST.EC/ELV.3 CVE-2019-12263 Wind River VXWorks 6.9.6 and vxO has CVSS: 5 ed CVEs from NVD Remove selected CVEs from asset Clear all VES 2001-0832 Vulnerability in Oracle 8.0.x through 9.0.1 on Unix allow: V2.0 2.1
vewords X Search keywords Search keywords Search keywords VE 2005-701 Directory traversal vulnerability in oracle Databases Serve V2.0 5.0 vewords X Search keywords Oracle Databases Server 10g Release 2 allows local user V2.0 6.0 VE description CVE-2005-7551 Multiple unspecified vulnerability in oracle Databases V2.0 6.0 VE description CVE-2007-5511 SQL injection vulnerability in Oracle Databases V2.0 6.5 CVE-2007-5511 SQL injection vulnerability in Workspace Manager for Or V2.0 6.5 CVE-2007-5514 Oracle allows remote attackers to obtain server memory V2.0 7.1 Unspecified vulnerability in the Logical Standby component in integrity via unknown vectors. VE-2001-1906 Unspecified vulnerability in the Logical Standby component V2.0 6.8 CVE-2001-1921 The installation process for Oracle 10g and Ilg uses accel, kr56 function in kr53/vecept, kee compt. V2.0 6.8 CVE-2011-1321 The installation process comp. V2.0 6.0 CVE-2011-6483 Unspecified vulnerability in the Application Express comp. V2.0 6.8 CVE-2011-1321 The key of avail value avail	T.EC/EUV.18 cpe:2.3:h::moxa::n; Serial-Ethernet Cor MOXA T.EC/EUV.20 cpe:2.3:h::siemens Power Quality Anal Elspec T.EC/EUV.20 cpe:2.3:h::abb:rtu5 RT AB8 T.EC/EUV.20 cpe:2.3:h::abb:rtu5 Rt AB8 T.EC/EUV.4 Substation Substation	PT-7728 Nport ser G420 SICAM AC G4500 RTU550 asset Add select	ST.F.C/ELV.3 CVE-2019-12261 Wind River VXWorks 6.7 though 6.9 an CVSS: 7.5 ST.F.C/ELV.3 CVE-2019-12262 Wind River VXWorks 6.6, 6.7, 6.8, 6.9 CVSS: 7.5 ST.F.C/ELV.3 CVE-2019-12263 Wind River VXWorks 6.9, 4 and vz/ has CVSS: 6.8 CVSS: 6.8 ST.F.C/ELV.3 CVE-2019-12263 Wind River VXWorks 6.9, 4 and vz/ has CVSS: 6.8 CVSS: 5 ST.F.C/ELV.3 CVE-2019-12263 Wind River VXWorks 6.5, 6.6, 6.7, 6.8, CVSS: 5 ST.F.C/ELV.3 CVE-2021-27196 Improper Input Validation vulnerability CVSS: 5 ed CVEs from NVD Remove selected CVEs from asset Clear all VEs 2001-0832 Vulnerability in Oracle 8.0.x through 9.0.1 on Unix allow: V2.0 2.1 Autor overflow in dvcrep in Oracle 8.0.x through 9.0.1 in Unix allow: V2.0 2.1 Vulnerability in Oracle 8.0.x through 9.0.1 in Unix allow: V2.0 7.2 2001-0833 Buffer overflow in dvcrep in Oracle 8.0.x through 9.0.1 in V2.0 7.2
eywords X Search keywords OVE-2006-7081 Oracle Database Server 10g Release 2 allows local user V2.0 4.6 OVE-2006-7141 Absolute path traversal undurerability for Oracle Database V2.0 6.5 OVE-2006-7141 Absolute path traversal undurerability for Workspace Marger for Or V2.0 6.5 VE description CVE-2007-5511 SQL injection vulnerability in Workspace Marger for Or V2.0 6.5 Unspecified vulnerability in the Logical Standby component in Oracle Database allows remote authenticated users to affect integrity via unknown vectors. Oracle Database allows remote authenticated users to affect integrity via unknown vectors. 6.8	T.EC/EUV.18 cpe:2.3:h:moxa:nc Serial-Ethernet Cor MOXA T.EC/EUV.19 Power Quality Anal Elspec T.EC/EUV.20 cpe:2.3:h:siemens Power Quality Anal Elspec T.EC/EUV.20 cpe:2.3:h:abbrtus RTU Siemens T.EC/EUV.20 cpe:2.3:h:abbrtus RTU ABB T.EC/EUV.4 Substation	PT-7728 Nport ser G420 SICAM AC G4500 RTUS60 RTUS60 CVE cve cve cve cve cve cve cve cve cve cve	ST. EC/ELV.3 CVE-2019-12261 Wind River VXWorks 6.7 though 6.9 an CVSS: 7.5 ST. EC/ELV.3 CVE-2019-12262 Wind River VXWorks 6.9 though 6.9 an CVSS: 6.8 ST. EC/ELV.3 CVE-2019-12263 Wind River VXWorks 6.9 though 7.5 ST. EC/ELV.3 CVE-2019-12263 Wind River VXWorks 6.9 though 7.5 ST. EC/ELV.3 CVE-2019-12263 Wind River VXWorks 6.9 though 7.5 ST. EC/ELV.3 CVE-2019-12263 Wind River VXWorks 6.9 though 7.5 ST. EC/ELV.3 CVE-2021-27196 Improper Input Validation vulnerability Multiple total for though 7.5 CVE-2021-27196 Improper Input Validation vulnerability VES E2001-0832 Vulnerability in Oracle 8.0.x through 9.0.1 on Unix allows: V2.0 2.1 Suffer overflow in otrcrep in Oracle 8.0.x through 9.0.1 i V2.0 7.2 1 2001-0832 Vulnerability in Oracle 8.0.x through 9.0.1 i V2.0 7.2 Suffer overflow win other torep in Oracle 8.0.x through 9.0.1 i V2.0 7.2 2001-0837 SQL injection vulnerability for Oracle 8.0.x through 9.0.1 i V2.0 7.2 Suffer overflow win other torep in Oracle 8.0.2 Wind 9.0.1 i V2.0 7.2 SQL injection vulnerability for Oracle 8.0.2 Wind 9.0.1 i V2.0 7.2 SQL injection vulnerabili
eywords X Search keywords CVE-2007-7510 Absolute path traversal vulnerability in Oracle Database V2.0 6.0 CVE-2007-5510 Multiple unspecified vulnerability in Vorkspace Manager for Or V2.0 6.5 VE description CVE-2007-5510 SQL injection vulnerability in Vorkspace Manager for Or V2.0 6.5 Unspecified vulnerability in the Logical Standby component in Oracle Database allows remote attackers to obtain server memory V2.0 6.8 CVE-2007-5510 SUE injection vulnerability in the Logical Standby component in Oracle Database allows remote attackers to obtain server memory V2.0 6.8 CVE-2007-1321 The installation process for Oracle 10g and IIg uses accc V2.0 6.8 CVE-2017-1321 The kg.accept krb5 function in krb3/sccpt.sec_conter V2.0 6.8 CVE-2017-1321 The kg.accept.krb5 function in krb3/sccpt.sec_conter V2.0 6.0 CVE-2017-5510 Unspecified vulnerability in the Application Express comp V2.0 6.8 CVE-2017-6433 Unspecified vulnerability in the Application Express comp V2.0 6.0 CVE-2014-6433 Unspecified vulnerability in the Application Express comp V2.0 6.0	T.EC/EUV.18 cpe:2.3:h:moxa:nc Serial-Ethernet Cor MOXA T.EC/EUV.19 Power Quality Anal Elspec T.EC/EUV.20 cpe:2.3:h:siemens Power Quality Anal Elspec T.EC/EUV.20 cpe:2.3:h:abbrtus RTU Siemens T.EC/EUV.20 cpe:2.3:h:abbrtus RTU ABB T.EC/EUV.4 Substation	PT-7728 Nport ser G420 SICAM AI G4500 RTU550 asset Add select	ST. F.C/ELV.3 CVE-2019-12261 Wind River VXWorks 6.7 though 6.9 an CVSS: 7.5 ST. F.C/ELV.3 CVE-2019-12262 Wind River VXWorks 6.9.4 and vx7 has CVSS: 6.8 ST. F.C/ELV.3 CVE-2019-12263 Wind River VXWorks 6.9.4 and vx7 has CVSS: 6.8 ST. F.C/ELV.3 CVE-2019-12263 Wind River VXWorks 6.9.4 and vx7 has CVSS: 6.8 ST. F.C/ELV.3 CVE-2019-12263 Wind River VXWorks 6.5, 6.6, 6.7, 6.8, 6.9 CVSS: 5 ST. F.C/ELV.3 CVE-2021-27196 Improper Input Validation vulnerability CVSS: 5 ed CVEs from NVD Remove selected CVEs from asset Clear all VEs 2001-0832 Vulnerability in Oracle 8.0.x through 9.0.1 on Unix allow: V2.0 2.1 2001-0832 Vulnerability in Oracle 8.0.x through 9.0.1 in Unix allow: V2.0 2.1 2001-0233 Buffer overflow in dtrorep in Oracle 8.0.x through 9.0.1 in Unix allow: V2.0 2.1 2001-0237 SQL injection vulnerability in Oracle B.0.x through 9.0.1 or Unix allow: V2.0 2.1 2003-0277 SQL injection vulnerability in Oracle Babase Server V2.0 5.0
VE description CVE-2007-5511 SQL injection vulnerability in Workspace Manager for Or V2.0 6.5 VE description CVE-2007-5554 Oracle allows remote attackers to obtain server memory V2.0 6.5 Unspecified vulnerability in the Logical Standby component in Oracle Database allows remote authenticated users to affect integrity via unknown vectors. 0.6.8 CVE-2007-6260 The installation process for Oracle 10g and IIg uses accc V2.0 6.8 CVE-2007-1321 The kg_accept_krb5 function in krb5/accept_sec_conter V2.0 6.8 CVE-2017-6255 Unspecified vulnerability in the Logical Standby componer V2.0 6.8 CVE-2019-1996 Unspecified vulnerability in the Logical Standby componer V2.0 6.8 CVE-2019-1995 Unspecified vulnerability in the Logical Standby componer V2.0 6.8 CVE-2019-1995 Unspecified vulnerability in the Application Express comp V2.0 6.8 CVE-2019-1995 Unspecified vulnerability in the Application Express comp V2.0 6.8	T.EC/EUV.18 cpe:2.3:h:moxa:nc Serial-Ethernet Cor MOXA T.EC/EUV.19 Power Quality Anal Elspec T.EC/EUV.20 cpe:2.3:h:siemens Power Quality Anal Elspec T.EC/EUV.20 cpe:2.3:h:abbrtus RTU Siemens T.EC/EUV.20 cpe:2.3:h:abbrtus RTU ABB T.EC/EUV.4 Substation	PT-7728 Nport ser G420 SICAM AL G4500 RTU550 asset Add select	STF.EC/ELV.3 CVE-2019-12261 Wind River VXWorks 6.7, though 6.9 an CVSS: 7.5 STF.EC/ELV.3 CVE-2019-12262 Wind River VXWorks 6.6, 6.7, 6.8, 6.9 CVSS: 7.5 STF.EC/ELV.3 CVE-2019-12263 Wind River VXWorks 6.6, 4.and vxO has CVSS: 6.8 STF.EC/ELV.3 CVE-2019-12263 Wind River VXWorks 6.5, 6.6, 6.7, 6.8, CVSS: 5 ST.EC/ELV.3 STF.EC/ELV.3 CVE-2019-12263 Wind River VXWorks 6.5, 6.6, 6.7, 6.8, CVSS: 5 ST.EC/ELV.3 ST.EC/ELV.3 CVE-2021-27196 Improper Input Validation vulnerability CVSS: 5 ST.EC/ELV.3 CVE-2021-27196 Improper Input Validation vulnerability CVSS: 5 ed CVEs from NVD Remove selected CVEs from asset Clear all VES 2001-0832 Vulnerability in Oracle 8.0.x through 9.0.1 on Unix allow: V2.0 2.1 2001-0833 Buffer overflow in attracting in Oracle B.0.x through 9.0.1 in V2.0 7.2 200-2027 SQL injection vulnerability in Oracle Database (XDB) fun V2.0 2.1 2.1 2005-0327 SQL injection vulnerability in Oracle Database Ser V2.0 1.0.0 Wittple unspecified vulnerability in Oracle Database Ser V2.0 1.0.0
VE description CVE-2007-5554 Oracle allows remote attackers to obtain server memory V2.0 7.1 Unspecified vulnerability in the Logical Standby component in Oracle Database allows remote attackers to obtain server memory V2.0 8.5 Oracle Database allows remote attackers to obtain server memory V2.0 8.5 Oracle Database allows remote attackers to obtain server memory V2.0 6.8 CVE-2007-6260 The installation process for Oracle 10g and IIg uses acc V2.0 6.8 CVE-2007-6261 The installation process for Oracle 10g and IIg uses acc V2.0 4.0 Oracle Database allows remote authenticated users to affect CVE-2010-1995 The kg_accept_kb5 function in kb5/xscept_sec_onter V2.0 6.8 CVE-2010-1995 Unspecified vulnerability in the Application Express comp V2.0 6.8 CVE-2010-1995 Unspecified vulnerability in the Application Express comp V2.0 6.0 CVE-2010-1955 Unspecified vulnerability in the Application Express comp V2.0 6.0 CVE-2010-1955 Unspecified vulnerability in the Application Express comp V2.0 6.0	T.EC/EU.V.18 cpe:2.3:h:moxa:nc Serial-Ethernet Cor MOXA T.EC/EU.V.2 cpe:2.3:h:shemens Power Quality Anal Elspec T.EC/EU.V.2 cpe:2.3:h:abbrtus RTU Siemens T.EC/EU.V.2 cpe:2.3:h:abbrtus RTU ABB T.EC/EU.V.3 cpe:2.3:h:abbrtus Retrieve current CVEs of selected Opy selected CPE to NVD search Retrieve current CVEs of selected D search PE name pe:2.3:a:oracle:database_server:-:*:*:*:*:*:* X VE ID X Search	PT-7728 Nport ser G420 SICAM AC RTU560 RTU56	STF.EC/ELV.3 CVE-2019-12261 Wind River VXWorks 6.7 though 6.9 an CVSS: 7.5 STF.EC/ELV.3 CVE-2019-12262 Wind River VXWorks 6.9.4 and v2/ has CVSS: 5 STF.EC/ELV.3 CVE-2019-12263 Wind River VXWorks 6.9.4 and v2/ has CVSS: 6.8 STF.EC/ELV.3 CVE-2019-12263 Wind River VXWorks 6.9.4 and v2/ has CVSS: 6.8 STF.EC/ELV.3 CVE-2019-12263 Wind River VXWorks 6.9.4 and v2/ has CVSS: 5 STF.EC/ELV.3 CVE-2019-12263 Wind River VXWorks 6.9.4 and v2/ has CVSS: 5 STF.EC/ELV.3 CVE-2019-12261 Improper Input Validation vulnerability CVSS: 5 ed CVEs from NVD Remove selected CVEs from asset Clear all VES Vulnerability in Oracle 8.0.x through 9.0.1 on Unix allow: V2.0 2.1 2001-0832 Vulnerability in Oracle 8.0.x through 9.0.1 in Unix allow: V2.0 7.1 2001-0822 Vulnerability in Oracle 8.0.x through 9.0.1 in Unix allow: V2.0 7.1 2001-0823 Vulnerability in Oracle 8.0.x through 9.0.1 in Unix allow: V2.0 7.2 2001-07207 SQL injection vulnerability in Oracle Database 91 and 10; V2.0 7.2 2003-0727 Multiple Unrepe
Ver description CVE-2007-5897 Buffer overflow in MDSYS.SDO_CS in Oracle Database S V2.0 8.5 Unspecified vulnerability in the Logical Standby component in Oracle Database allows remote authenticated users to affect integrity via unknown vectors. CVE-2007-5897 Buffer overflow in MDSYS.SDO_CS in Oracle Database S V2.0 8.5 CVE-2007-5897 Buffer overflow in MDSYS.SDO_CS in Oracle 10g and lig uses acc V2.0 6.8 CVE-2007-1000 Unspecified vulnerability in the Logical Standby component in CVE-2019-121 The kg_accept_krb5 function in krb5Vaccept_sec_conter V2.0 6.8 CVE-2019-1221 The kg_accept_krb5 function in krb5Vaccept_sec_conter V2.0 6.8 CVE-2019-1325 Unspecified vulnerability in the Application Express comp V2.0 6.0 CVE-2019-1325 Unspecified vulnerability in the Application Express comp V2.0 6.0 CVE-2019-1325 Unspecified vulnerability in the Application Express comp V2.0 6.0	T.EC/EU.V.18 cpe:2.3:h:moxa:nc Serial-Ethernet Cor MOXA T.EC/EU.V.20 cpe:2.3:h:shemens Power Quality Anal Elspec T.EC/EU.V.20 cpe:2.3:h:abbrtus RTU Siemens T.EC/EU.V.20 cpe:2.3:h:abbrtus Rtrieve quality Anal Elspec T.EC/EU.V.20 cpe:2.3:h:abbrtus Rtrieve quality Anal Elspec T.EC/EU.V.20 cpe:2.3:h:abbrtus Retrieve current CVEs of selected	PT-7728 Nport ser G4420 SICAM AL G4500 RTU56	ST. EC/ELV.3 CVE-2019-12261 Wind River VXWorks 6.7 though 6.9 an CVSS: 7.5 ST. EC/ELV.3 CVE-2019-12262 Wind River VXWorks 6.9.4 and vx7 has CVSS: 6.8 ST. EC/ELV.3 CVE-2019-12263 Wind River VXWorks 6.9.4 and vx7 has CVSS: 6.8 ST. EC/ELV.3 CVE-2019-12263 Wind River VXWorks 6.9.4 and vx7 has CVSS: 6.8 ST. EC/ELV.3 CVE-2019-12263 Wind River VXWorks 6.9.4 and vx7 has CVSS: 5 ST. EC/ELV.3 CVE-2019-12263 Wind River VXWorks 6.9.4 and vx7 has CVSS: 5 ST. EC/ELV.3 CVE-2021-27196 Improper Input Validation vulnerability CVSS: 5 ad CVEs from NVD Remove selected CVEs from asset Clear all VEs 2001-0832 Vulnerability in Oracle 8.0.x through 9.0.1 in Unix allows: V2.0 7.2 2001-0832 S0Lingeton winetrability in Oracle 0.0.x through 9.0.1 i V2.0 7.2 2001-0832 S0Lingeton winetrability in Oracle 0.0.x through 9.0.1 i V2.0 7.2 2001-0832 S0Lingeton winetrability in Oracle Database St v2.0 5.0 5.0 2001-0832 S0Lingeton winetrability in Oracle Database St v2.0 5.0 5.0 2001-0832 S0Lingeton winetrability in Oracle Da
Unspecified vulnerability in the Logical Standby component in Oracle Database allows remote authenticated users to affect Integrity via unknown vectors.	T.EC/EUV.18 cpe:2.3:h:moxa:nc Serial-Ethernet Cor MOXA T.EC/EUV.12 cpe:2.3:h:siemens Power Quality Anal Elspec T.EC/EUV.20 cpe:2.3:h:abbrtus RTU Siemens T.EC/EUV.20 cpe:2.3:h:abbrtus RTU ABB T.EC/EUV.4 Substation	PT-7728 Nport ser G4420 SICAM AC RTU550 RTU5	ST.F.C/ELV.3 CVE-2019-12261 Wind River VXWorks 6.7 though 6.9 an CVSS: 7.5 ST.F.C/ELV.3 CVE-2019-12262 Wind River VXWorks 6.6, 6.7, 6.8, 6.9 CVSS: 7.5 ST.F.C/ELV.3 CVE-2019-12263 Wind River VXWorks 6.9, 4 and v2/ has CVSS: 6.8 ST.F.C/ELV.3 CVE-2019-12263 Wind River VXWorks 6.9, 4 and v2/ has CVSS: 6.8 ST.F.C/ELV.3 CVE-2019-12263 Wind River VXWorks 6.5, 6.6, 6.7, 6.8, CVSS: 5 ST.F.C/ELV.3 CVE-2019-12263 Wind River VXWorks 6.5, 6.6, 6.7, 6.8, CVSS: 5 ST.F.C/ELV.3 CVE-2021-27196 Improper Input Validation vulnerability CVSS: 5 ed CVEs from NVD Remove selected CVEs from asset Clear all VEs Vulnerability in Oracle 8.0.x through 9.0.1 on Unix allow: V2.0 2.1 2001-0832 Vulnerability in Oracle 8.0.x through 9.0.1 in ULV 2.0 7.2 2.1 2001-0833 Buffer overflow in dtrorep in Oracle 8.0.x through 9.0.1 in ULV 2.0 7.2 2.1 2003-027 SQL injection vulnerability in Oracle Database Set V2.0 7.5 7.5 2003-027 SQL injection vulnerability in Oracle Database Set V2.0 5.0 10.0 2005-9313 Multiple buf
Oracle Database allows remote authenticated users to affect integrity via unknown vectors. CVE-2010-1320 The kg_accept_krbs function in krbs/vaccept_sec_conte V2.0 6.8 CVE-2010-1325 Unspecified vulnerability in the Application Express comp V2.0 6.0 CVE-2010-1355 Unspecified vulnerability in the Application Express comp V2.0 6.0	T.EC/EUV.18 cpe:2.3:h:moxa:nc Serial-Ethernet Cor MOXA T.EC/EUV.12 cpe:2.3:h:siemens Power Quality Anal Elspec T.EC/EUV.20 cpe:2.3:h:abbrtus RTU Siemens T.EC/EUV.20 cpe:2.3:h:abbrtus RTU ABB T.EC/EUV.4 Substation	PT-7728 Nport ser G4420 SICAM AF G4500 RTUS6	ST. F.C/ELV.3 CVE-2019-12261 Wind River VXWorks 6.7 though 6.9 an CVS: 7.5 ST. F.C/ELV.3 CVE-2019-12262 Wind River VXWorks 6.9.4 and vo2 has CVS: 6.8 ST. F.C/ELV.3 CVE-2019-12263 Wind River VXWorks 6.9.4 and vo2 has CVS: 5.6 ST. F.C/ELV.3 CVE-2019-12263 Wind River VXWorks 6.9.4 and vo2 has CVS: 5.6 ST. F.C/ELV.3 CVE-2019-12263 Wind River VXWorks 6.9.4 and vo2 has CVS: 5 ST. F.C/ELV.3 CVE-2019-12263 Wind River VXWorks 6.9.4 and vo2 has CVS: 5 ST. F.C/ELV.3 CVE-2011-27196 Improper Input Validation vulnerability CVS: 5 ad CVEs from NVD Remove selected CVEs from asset Clear all VES Suffer overflow in otrcrep in Oracle 8.0.x through 9.0.1 in Unix allows: Y2.0 7.2 2001-0832 Vulnerability in Oracle 0.0.x through 9.0.1 i Y2.0 7.2 2001-0832 SQL ingection vulnerability in Oracle Databases (YDB) fun Y2.0 7.2 2001-0832 Vulnerability in Oracle Databases 9 and 10 Y2.0 7.2 2001-0832 Nultiple unspecified vulnerability in Oracle Databases 9 and 10 Y2.0 7.1 2005-0701 Directory traversal vuln
integrity via unknown vectors. CVE-2014-5481 Unspecified vulnerability in the Application Express comp V2.0 6.0 (VE-2014-5483 Unspecified vulnerability in the Application Express comp V2.0 6.0 (VE-2014-5255 Unspecified vulnerability in the Application Express comp V2.0 2.1	T.EC/EU.V18 cpe:2.3:h:moxa:nc Serial-Ethernet Cor MOXA T.EC/EU.V2 cpe:2.3:h:shemens Power Quality Anal Elspec T.EC/EU.V2 cpe:2.3:h:abbrtos RTU Siemens T.EC/EU.V2 cpe:2.3:h:abbrtos RU ABB opy selected CPE to NVD search Retrieve current CVEs of selected PS ever quality Anal Elspec T.EC/EU.V3 cpe:2.3:a:oracle:database_server:::":":":":":":":":":":":":":":":":":"	PT-7728 Nport ser G420 SICAM AL Add selector RTUS60	ST. F.C/ELV.3 CVE-2019-12261 Wind River VXWorks 6.7 though 6.9 an CVS: 7.5 ST. F.C/ELV.3 CVE-2019-12262 Wind River VXWorks 6.9.4 and v2/ has CVS: 7.5 ST. F.C/ELV.3 CVE-2019-12263 Wind River VXWorks 6.9.4 and v2/ has CVS: 6.8 ST. F.C/ELV.3 CVE-2019-12263 Wind River VXWorks 6.9.4 and v2/ has CVS: 5 ST. F.C/ELV.3 CVE-2019-12263 Wind River VXWorks 6.9.4 and v2/ has CVS: 5 ST. F.C/ELV.3 CVE-2019-12263 Wind River VXWorks 6.5, 6.6, 6.7, 6.8, CVS: 5 ST. F.C/ELV.3 CVE-2011-27196 Improper Input Validation vulnerability CVS: 5 ed CVEs from NVD Remove selected CVEs from asset Clear all VES Suffer overflow in otrcrep in Oracle 8.0.x through 9.0.1 i V2.0 7.2 2001-0832 SQL injection vulnerability in Oracle Databases (XDB) fun V2.0 7.2 2001-0832 SQL injection vulnerability in Oracle Databases (YADB fun V2.0 7.2 2001-0832 SQL injection vulnerability in Oracle Databases (YADB fun V2.0 7.5 2001-0833 Buffer overflow win the XML Database (YADB fun V2.0 7.5 2001-0824 Nultrable unspecified vulner
CVE-2015-2585 Unspecified vulnerability in the Application Express comp. V2.0. 2.1.	T.EC/ELV.18 cpe:2.3:h:moxa:n; FC/ELV.19 Serial-Ethernet Core Power Quality Anal Elspec Siemens FLC/ELV.20 Siemens Power Quality Anal Elspec T.EC/ELV.3 T.EC/ELV.3 cpe:2.3:h:abbrtus FLC/ELV.4 ABB T.EC/ELV.4 Substation	PT-7728 Nport ser G420 SICAM AI G4500 RTU550 asset Add select rch CPE name CVE cve cve cve cve cve cve cve cve cve cve	ST. E.C/ELV.3 CVE-2019-12261 Wind River VXWorks 6.7. though 6.9 an CVSS: 7.5 ST. E.C/ELV.3 CVE-2019-12263 Wind River VXWorks 6.6, 6.7, 6.8, 6.9 CVSS: 7.5 ST. E.C/ELV.3 CVE-2019-12263 Wind River VXWorks 6.9, 4.6, 6.9 CVSS: 6.8 ST. E.C/ELV.3 CVE-2019-12263 Wind River VXWorks 6.5, 6.6, 6.7, 6.8, CVSS: 5 Encode State Stat
	T.EC/EU.18 cpe:2.3:h:moxa:nc Serial-Ethernet Cor MOXA T.EC/EU.20 cpe:2.3:h:siemens Power Quality Anal Elspec T.EC/EU.20 cpe:2.3:h:siemens RTU Siemens T.EC/EU.20 cpe:2.3:h:abbrtos RTU ABB T.EC/EU.2 cpe:2.3:h:abbrtos Retrieve current CVEs of selected T.EC/EU.4 Substation Substation	PT-7728 Nport ser G420 SICAM AL Add select asset Add select rch CPE name crch keywords CVE CVE CVE CVE CVE CVE CVE CVE CVE CVE	ST.E.C/ELV.3 CVE-2019-12261 Wind River VXWorks 6.7 though 6.9 an CVSS: 7.5 ST.E.C/ELV.3 CVE-2019-12262 Wind River VXWorks 6.9.4 and v27 has CVSS: 6.8 ST.E.C/ELV.3 CVE-2019-12263 Wind River VXWorks 6.9.4 and v27 has CVSS: 6.8 ST.E.C/ELV.3 CVE-2019-12263 Wind River VXWorks 6.9.4 and v27 has CVSS: 6.8 ST.E.C/ELV.3 CVE-2019-12263 Wind River VXWorks 6.9.4 and v27 has CVSS: 5 ST.E.C/ELV.3 CVE-2019-12263 Wind River VXWorks 6.9.4 and v27 has CVSS: 5 ST.E.C/ELV.3 CVE-2011-27196 Improper Input Validation vulnerability CVSS: 5 St.E.C/ELV.3 CVE-2021-27196 Improper Input Validation vulnerability CVSS: 5 St.E.C/ELV.3 CVE-2021-27196 Improper Input Validation vulnerability CVSS: 5 St.E.C/ELV.3 Vulnerability in Oracle 8.0.x through 9.0.1 on Unix allow: V2.0 2.1 St.E.C/ELV.3 Vulnerability in Oracle 8.0.x through 9.0.1 i V2.0 7.2 St.E.C/ELV.3 Wulnerability in Oracle Database 9 and 10g V2.0 7.2 St.E.C/ELV.3 Vulnerability in Oracle Database 9 and 10g V2.0 7.5 St.E.C/ELV.3 Oracle Database Server 10g Release 2 allows locababase V2.0 6.0 St.E.C/ELV.3 </td

o-----

INFORMATIKA

Remediation of cascading effects



Discussion

INFORMATIKA d.o.o. Vetrinjska ulica 2 | 2000 Maribor | Slovenija T: +386 2 707 10 00 E-mail: info@informatika.si www.informatika.si

Andrej Bregar

andrej.bregar@informatika.si