THE UTILITIES FORGOTTEN DATA STREAM

Webinar on
DATA PROTECTION FOR POWER UTILITIES

Yosi Shneck
YSICONS CEO, Former SVP,
CIO& CISO, Israel Electric
yosi.shneck@iec.co.il

IEC and the Israeli Electricity System

"Electricity Island" - no backup or interconnection to neighboring country	Fast growth rate: 2%- 3% demand growth rate is expected during the next decade	Structural changes- De-regulation and opening the market to competition.	Majority of electricity generated by natural gas	All IEC power stations are dual fueled

Established in 1923, the Israel Electric Corporation Limited ("IEC") is a dominant player in the Israeli electricity sector and is an essential service provider of electricity in Israel, and the sole vertically integrated provider in the electricity chain.

IEC is appx. 99.85% owned by the State of Israel, operates ~60% of the national total installed capacity, and serves 2.9 million customers.

Introduction

Data in utilities was always
CRITICAL!
and

it is more & more & more

CRITICAL!

Management, Operations, Safety, Business, Customers, Digitization, Automation, Autonomous, Smart

Context

The three pitfalls

- Know your self – where are all my data STREAMS & More?
- The forgotten UNCONNECTED data stream still so popular in utilities.
- Who is TOUCHING my systems?

Presentation

Where are my **DATA STREAMS & MORE?**

UNCONNECTED data stream

Who is **TOUCHING?**

Case examples

Where: A connection to ADMS control system was left after SAT procedure to unsecured lab - **COMPROMIZED**

Forgotten: 350Mw coal power station cooling water control system contaminated by laptop during a threshold value change in a PLC - **COMPROMIZED**

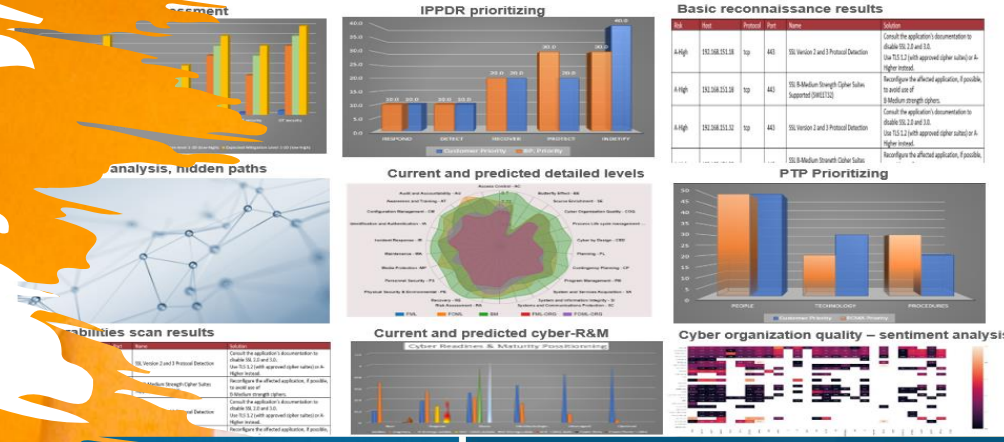
Touching: A critical operational data stolen in a man in the middle attack issued in vendors office during remote support process - **COMPROMIZED**

Recommendations – IEC's Sophic™ Solutions

RC*RR*MA™ - Comprehensive assessment & scan

Access™ - Secure Remote Access for highly sensitive OT environment

Info™ - Securing the most sensitive file transfers is a key challenge when dealing with critical infrastructure operators



Israel Electric

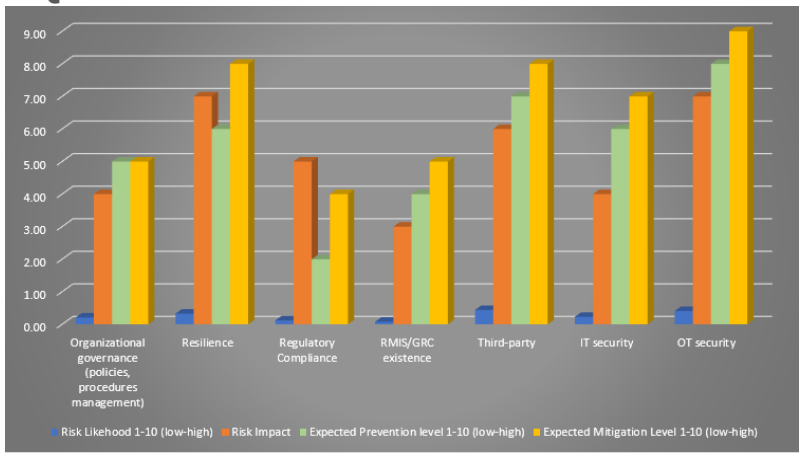
OGSGF Global Smart Energy Federation

Israel Electric

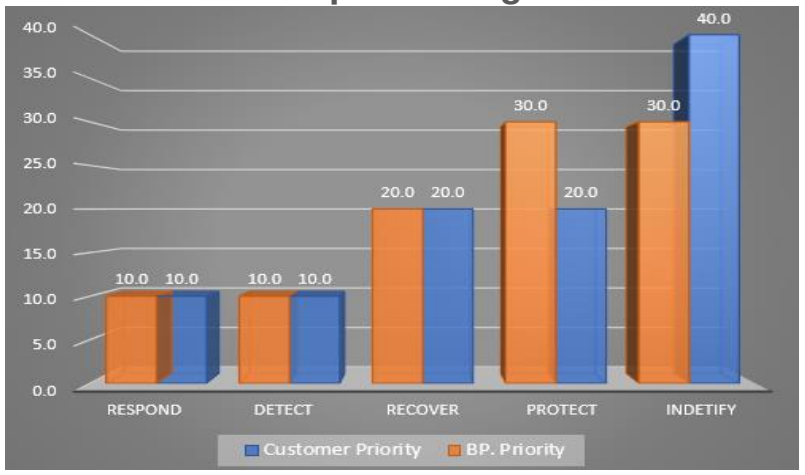
Thank you.

www.iec.co.il/international

Quantitative risk assessment



IPPDR prioritizing

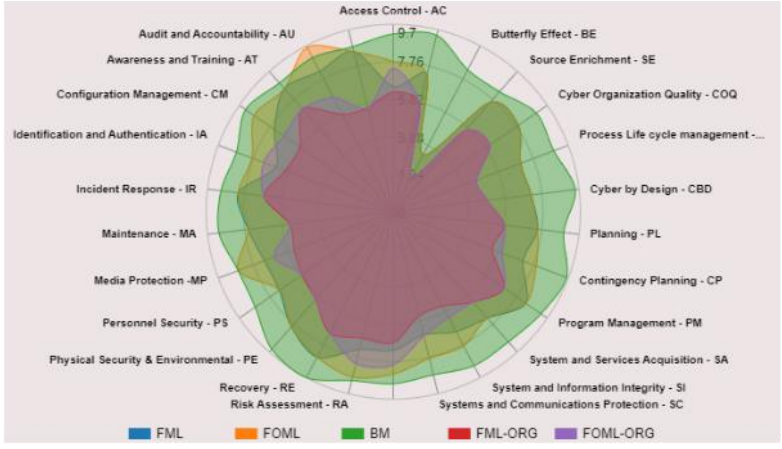


Basic reconnaissance results

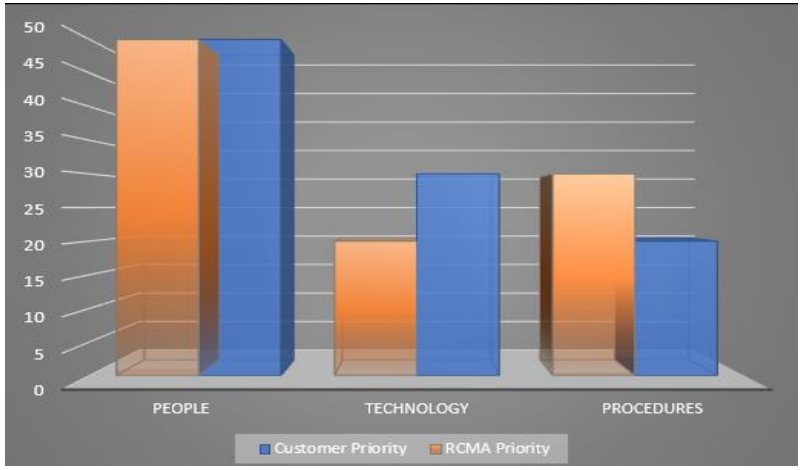
Risk	Host	Protocol	Port	Name	Solution
A-High	192.168.151.18	tcp	443	SSL Version 2 and 3 Protocol Detection	Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or A-Higher instead.
A-High	192.168.151.18	tcp	443	SSL B-Medium Strength Cipher Suites Supported (SWEET32)	Reconfigure the affected application, if possible, to avoid use of B-Medium strength ciphers.
A-High	192.168.151.32	tcp	443	SSL Version 2 and 3 Protocol Detection	Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or A-Higher instead.
				SSL B-Medium Strength Cipher Suites	Reconfigure the affected application, if possible,

Weak signal analysis, hidden paths

Current and predicted detailed levels



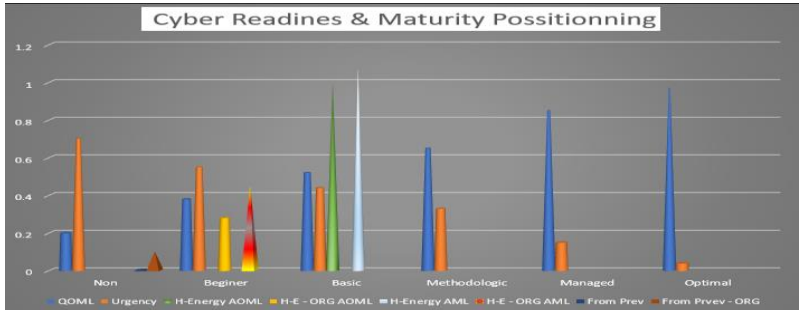
PTP Prioritizing



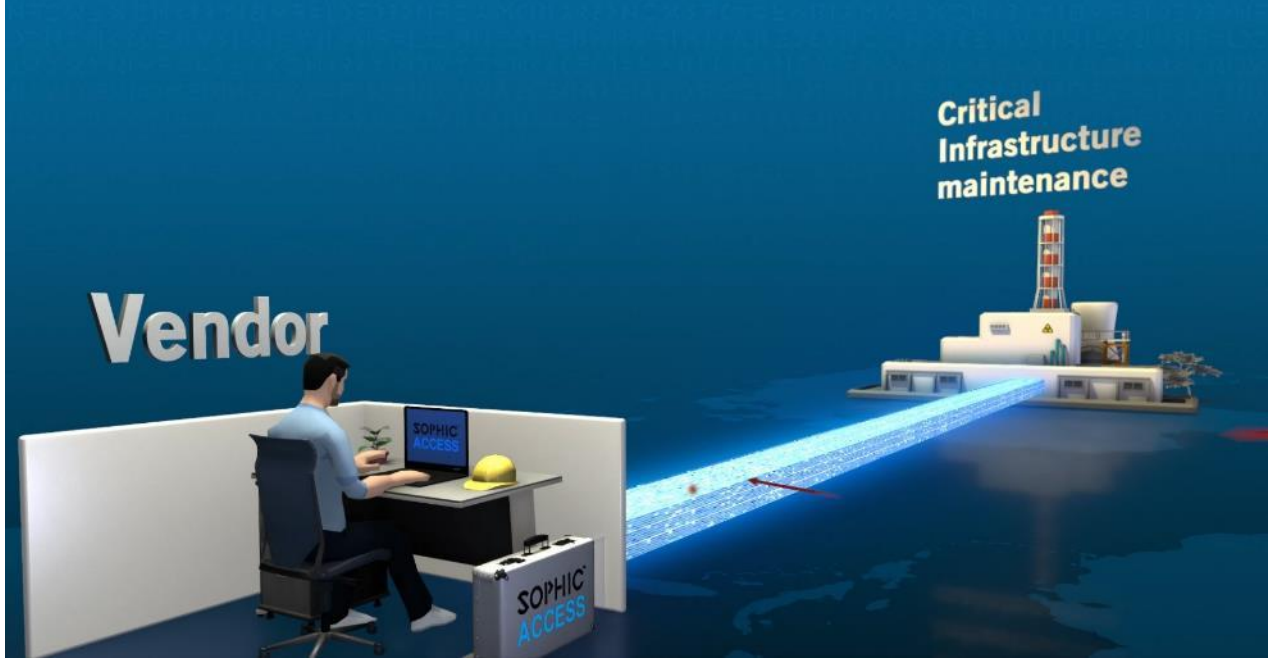
Vulnerabilities scan results

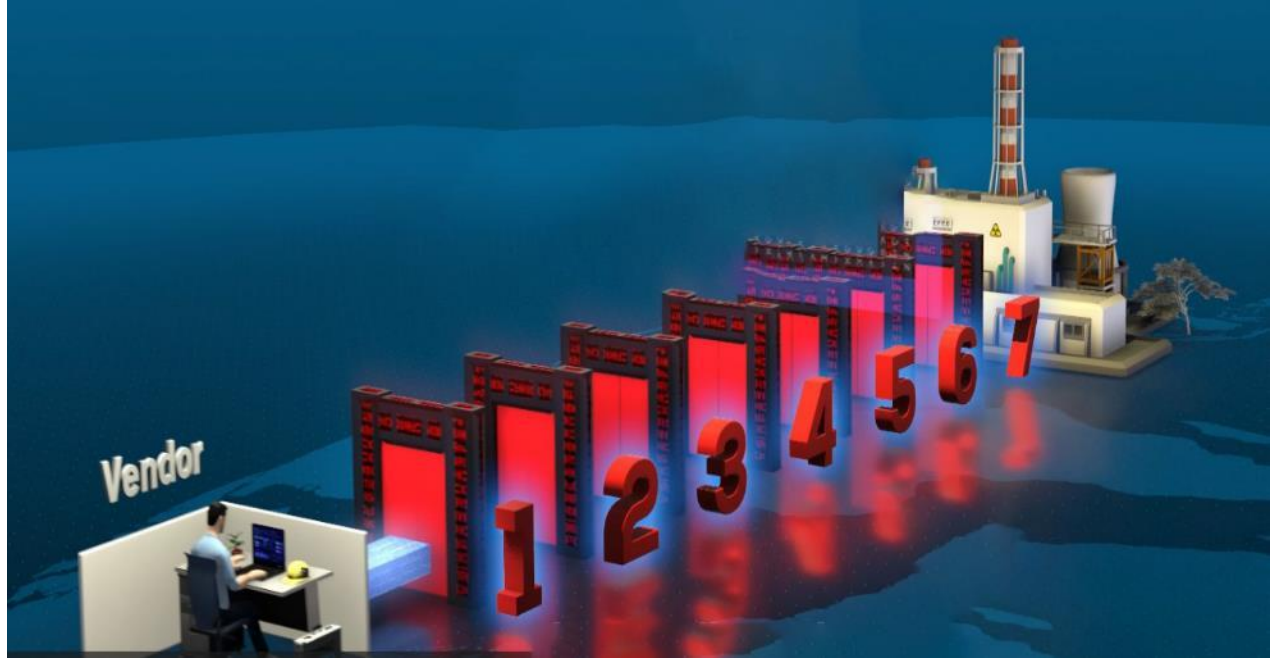
Risk	Host	Protocol	Port	Name	Solution
A-High	[redacted]	tcp	443	SSL Version 2 and 3 Protocol Detection	Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or A-Higher instead.
A-High	[redacted]	tcp	443	SSL B-Medium Strength Cipher Suites Supported (SWEET32)	Reconfigure the affected application, if possible, to avoid use of B-Medium strength ciphers.
A-High	[redacted]	tcp	443	SSL Version 2 and 3 Protocol Detection	Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or A-Higher instead.
	[redacted]			SSL B-Medium Strength Cipher Suites	Reconfigure the affected application, if possible,

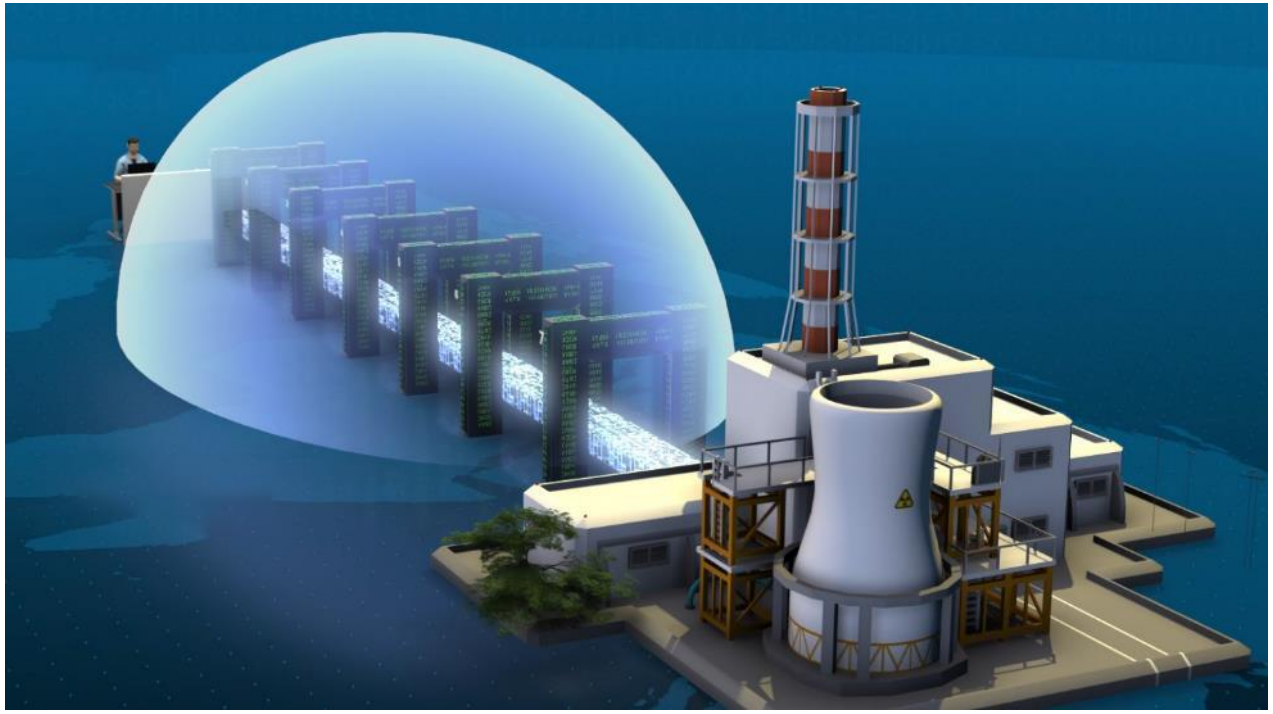
Current and predicted cyber-R&M



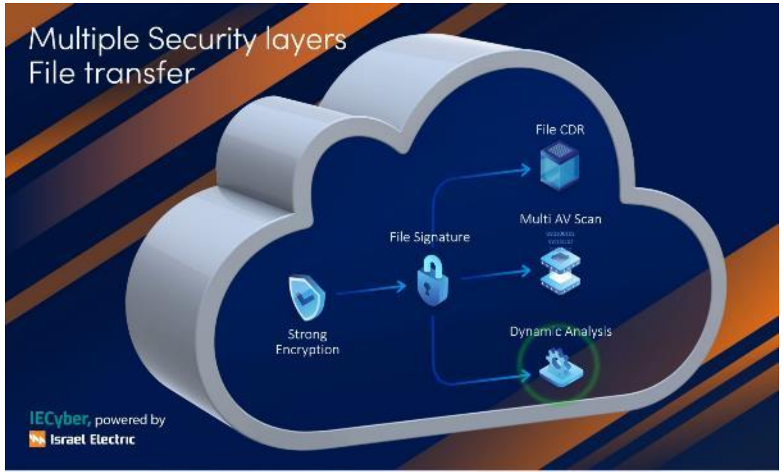
Cyber organization quality – sentiment analysis

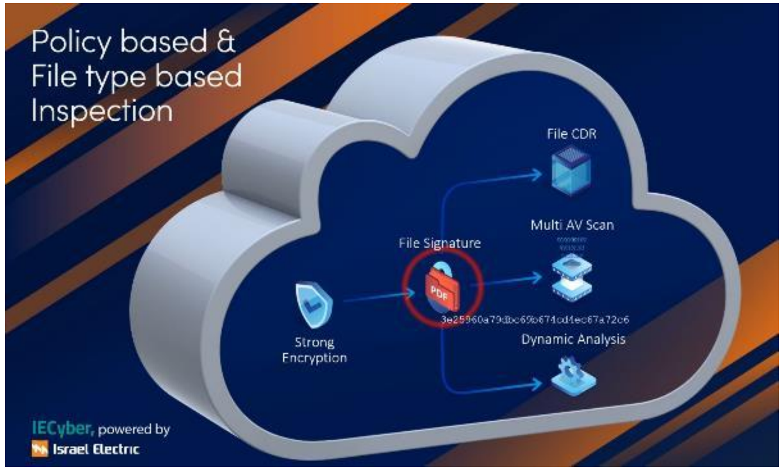






- Zero-Trust Architecture
- Pre-configured and dedicate hardened hardware
- Remote suppliers will receive limited privileges, only as needed to complete their task
- Central security monitoring and analytics
- Data Vaulting technology
- Unique Secure Cloud with Flexible deployment options
- Secure File transfer model for support access
- Advanced MAG (Multi Air Gap) Cloud Security
- Full control over sessions and activities


Multiple Security layers
File transfer
File CDR
Multi AV Scan
File Signature
Strong Encryption
Dynamic Analysis
IECyber, powered by
Israel Electric


Policy based &
File type based
Inspection
File CDR
Multi AV Scan
File Signature
PDF
Strong Encryption
Dynamic Analysis
IECyber, powered by
Israel Electric


Policy based &
File type based
Inspection
File CDR
PDF
File Signature
Multi AV Scan
Strong Encryption
Dynamic Analysis
IECyber, powered by
Israel Electric


Policy based &
File type based
Inspection
File CDR
Multi AV Scan
File Signature
Strong Encryption
Dynamic Analysis
IECyber, powered by
Israel Electric


Policy based &
File type based
Inspection
File CDR
Multi AV Scan
File Signature
Strong Encryption
Dynamic Analysis
EXE
IECyber, powered by
Israel Electric


3-Dimensional
File Inspection
File CDR
Multi AV Scan
File Signature
Strong Encryption
Dynamic Analysis
IECyber, powered by
Israel Electric


3-Dimensional
File Inspection
File CDR
Multi AV Scan
File Signature
Strong Encryption
Dynamic Analysis
IECyber, powered by
Israel Electric


Sophic Info™
IECyber, powered by
Israel Electric
IECyber, powered by
Israel Electric


Sophic Info™
IECyber, powered by
Israel Electric
IECyber, powered by
Israel Electric