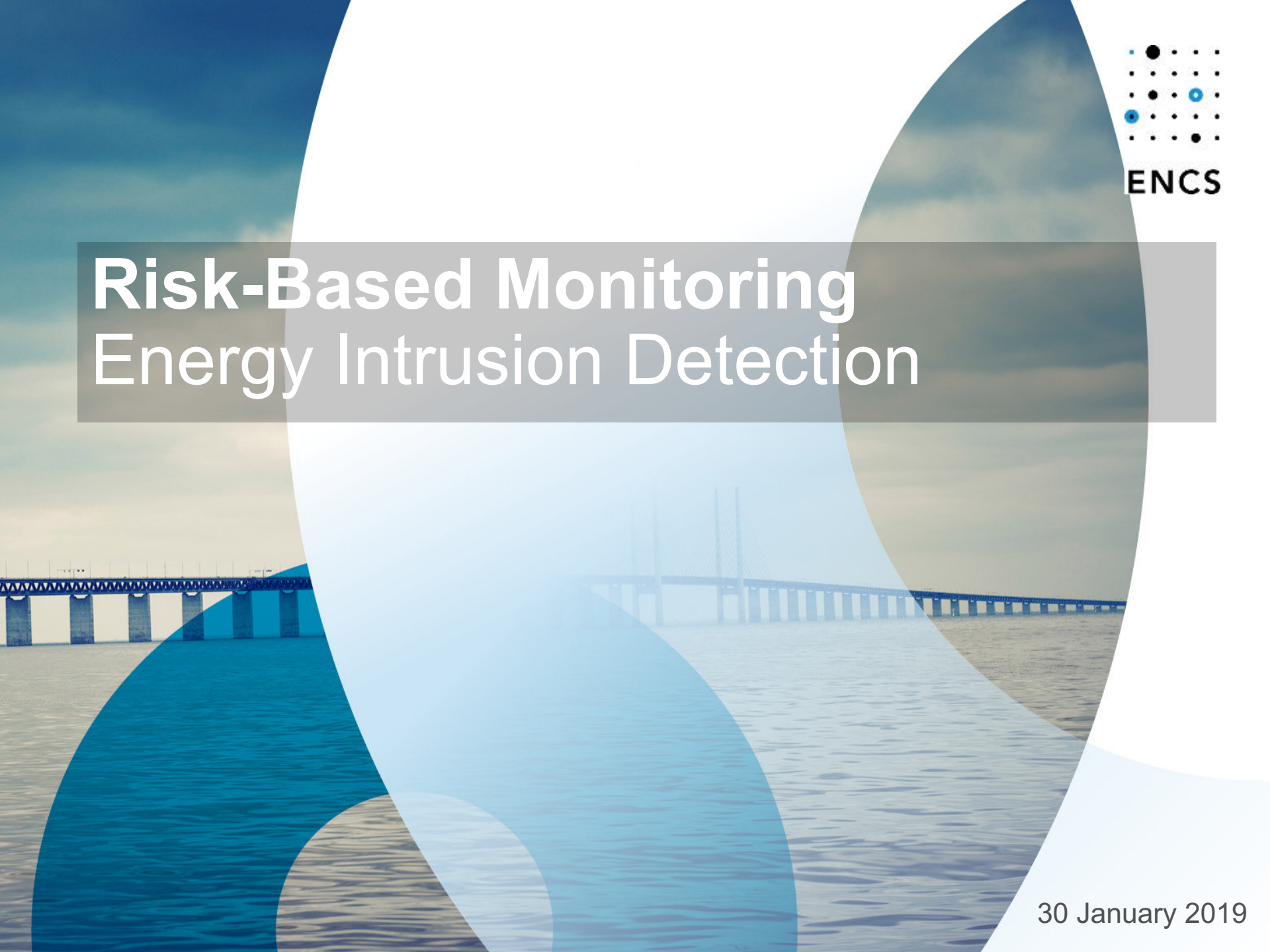


ENCS

Risk-Based Monitoring
Energy Intrusion Detection

30 January 2019

Security Monitoring in Operation

ENCS

- Energy companies are making large investments in security monitoring
  - Intrusion Detection Systems
  - SIEM systems
  - Security Operations Centers
- Often the investments are not used to their full potential once they are operational

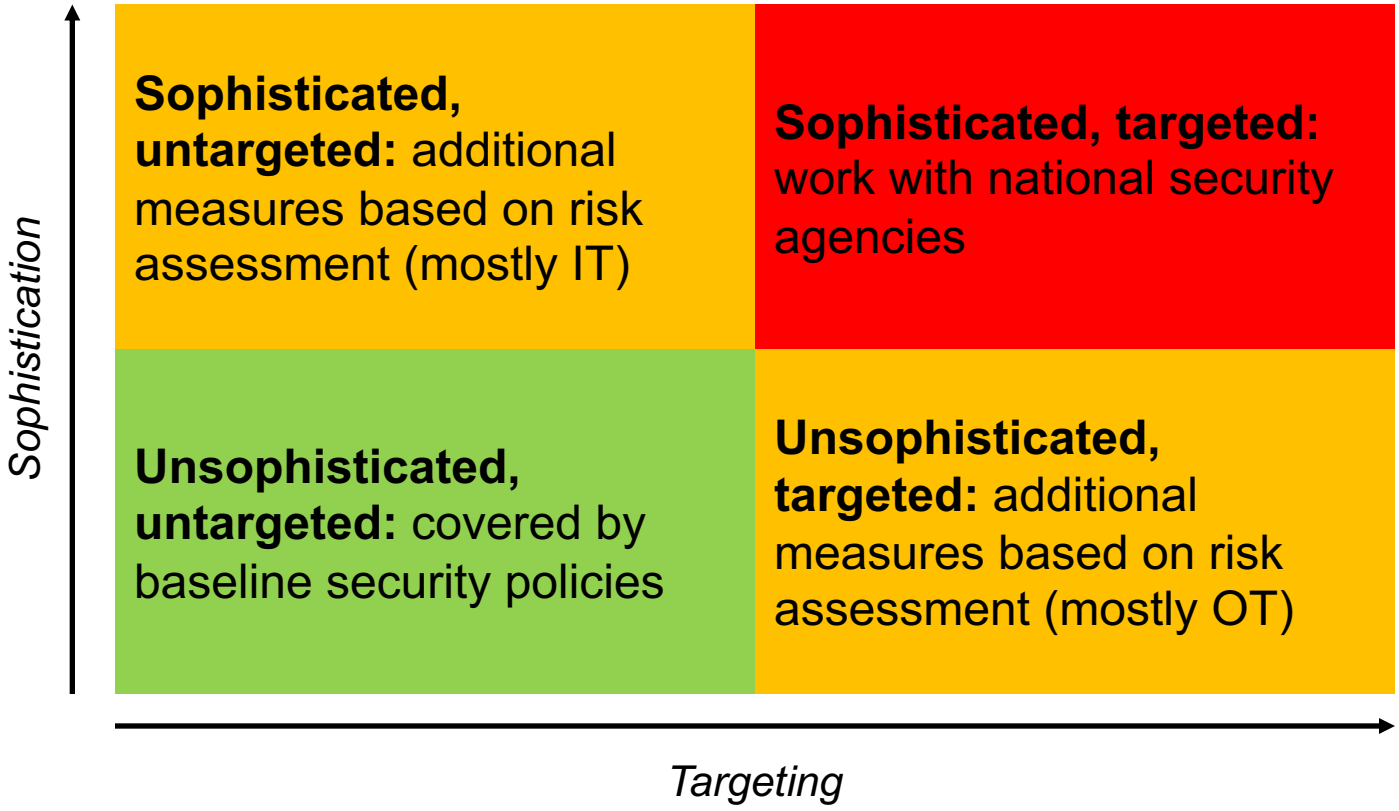
Why Do You Need to Understand the Risks?

- To monitor effectively, everyone involved needs to understand the risks:
  - **Management** to provide continuing budget and support
  - **Business owners** to support response
  - **Architects** to select the right use cases and tools
  - **Analysts** to prioritize alerts and stay motivated
- Each group will understand risks in their own way

Management

Risks for Management

Top management needs to understand the strategic risks to ensure continuing funding and support



Operational Costs Often Underestimated

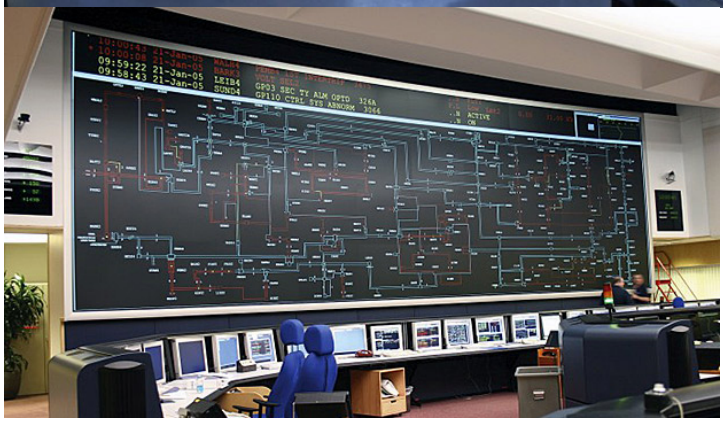
- Management often underestimates the effort needed after the setup project:
  - To handle the alerts
  - To maintain data sources and detection rules
  - To keep pace with new threats
  - To keep analyst skills and knowledge up to date

For OT, Managers Need to Look Outside of Their Department

ENCS

Need collaboration between IT and OT to have effective monitoring:

- OT too small to sustain specialized team
- Need IT security expertise
- Need OT knowledge
- Analysts need network in OT departments



Dividing Responsibilities Between IT and OT

ENCS

IT Analysts	OT Security Specialists
• Run IT detection systems • Detect and analyze incidents • Coordinate response (below crisis level)	• Support analyzing incidents • Support response • Run OT security sensors • Correlate access with maintenance activities

Business Owners

Risks for Business Owners

ENCS

Business owners need to understand the risks in terms of business impact to properly support response actions

Category	Reliability	Safety	Compliance	Affordability	Customer satisfaction	Sustainability
Disastrous	>20,000,000 cml (HV/MV station >16 hrs interruption)	Accident with one or multiple fatalities	Silent curator; Criminal case against board member; Fine by regulator >0.1% of turnover	Damage beyond 10M euro	International commotion; >20,000 complaints	Emission >250 kton CO_2
Serious	2,000,000 - 20,000,000 cml (HV/MV station 4 hrs interruption)	Accident with severe, permanent injury	Direction or warning by competent authorities; Fine 6th category	Damage between 1M and 10M euro	National commotion; 2,000 - 20,000 complaints; Conflict >10 municipalities or multiple provinces	Emission 25 - 250 kton CO_2

Need for Business Support

ENCS

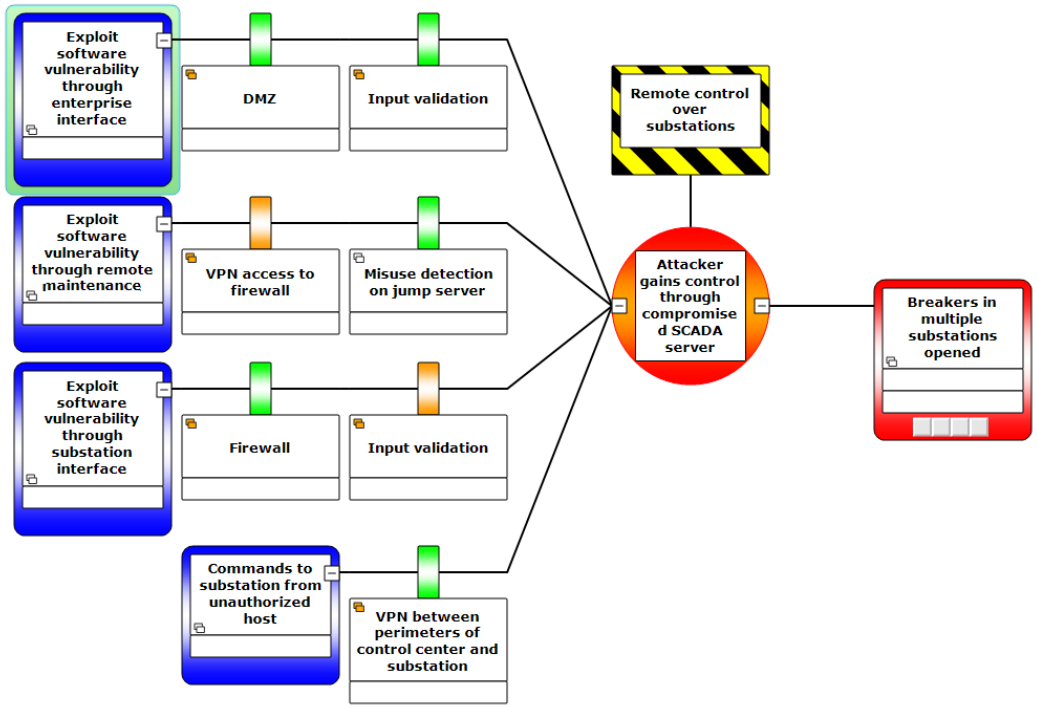
Monitoring finding	Business Response
Technical vulnerabilities	• Patch software • Improve password strength
Policy violations	• Train employees on security • Enforce security policies from management • Enforce policies with vendors
Security incidents	• Support forensics on critical systems • Disconnect OT from IT • Shut down critical systems such as SCADA

Architects

Risks for Architects

ENCS

Architects designing the monitoring system need to understand the risks on a technical level to select the right use cases and tools



Monitor IT/OT Boundary Often Most Effective

ENCS

For most grid operators, focusing on IT technology on OT boundary has the best business case:

- Can use IT tools (and analyst knowledge) on:
  - Data exchange servers in DMZ
  - Jump servers or stepping stones
  - Engineering laptops
  - Network equipment
- Can detect attacker before they are in the core OT

We Need Better Maintenance Access Monitoring

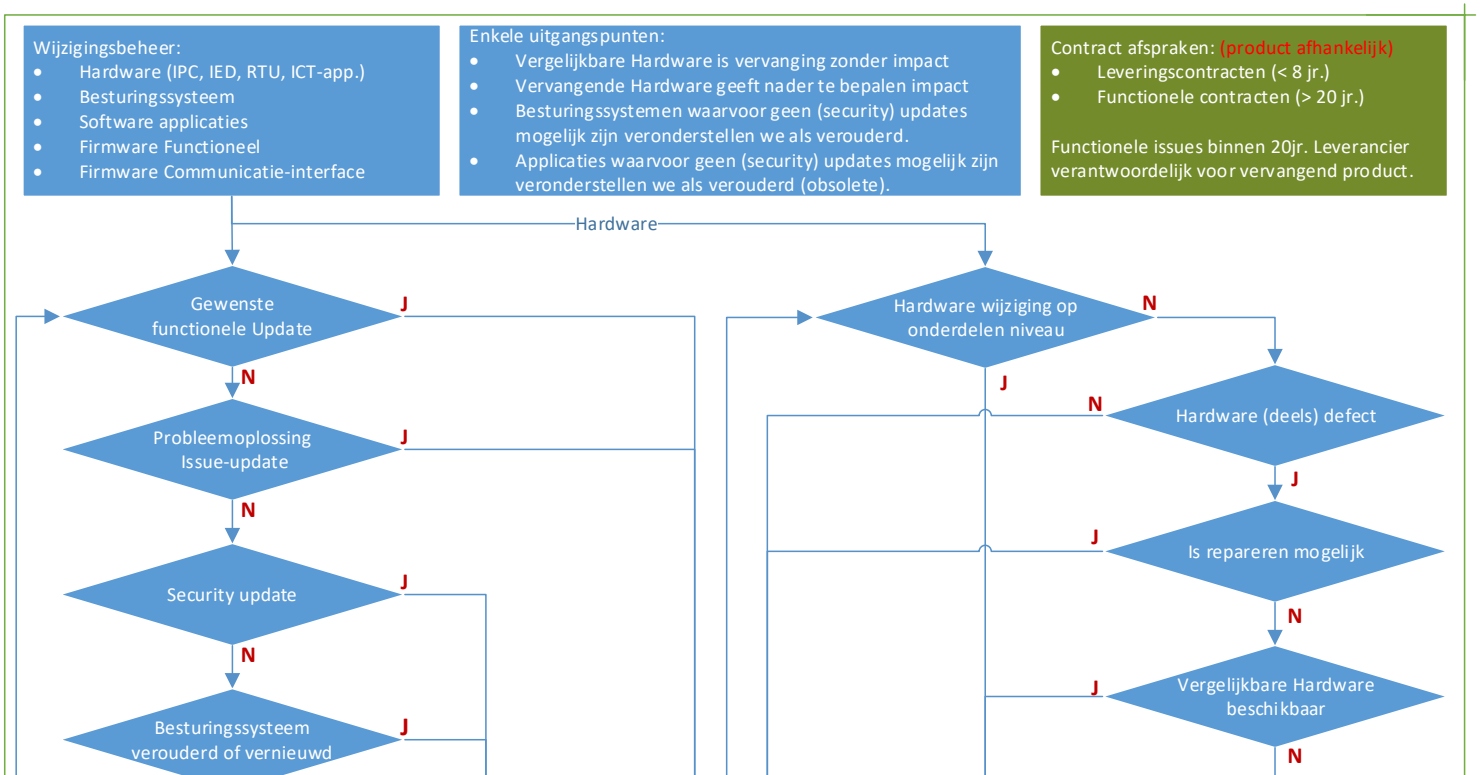
ENCS

	Type of access	Reaction
	Known bad access	Treat as security incident
	Normal user access	Correlate with maintenance schedules
	Normal M2M access	Whitelist (ignore)
	Unknown access	Threat hunting

Analysts

Risks for Analysts

Analysts that handle alerts and maintain the monitoring systems need to understand the risks to prioritize alerts and stay motivated



Interpreting Anomalies

Signature-based alert from Snort

```
OS-WINDOWS DCERPC NCACN-IP-TCP srvsvc NetrpPathCanonicalize
path canonicalization stack overflow attempt; cve 2008-4250
```

Anomaly-based alert from OT security sensor

```
Communications host not whitelisted: the source host is not
whitelisted in any of the communication rules
```

Analysts Need to Be Able to Link Alerts to Risks

Function	Risks Detected (Examples)
New hosts and connections	• Commands or configuration from unauthorized host • Access to control center servers from substations • Malware command and control traffic
Unusual commands and parameters	• Address range scanning • Large numbers of switching operations • Zero-day attacks on SCADA front-end