Smart Grid Security Symposium

DSO-oriented Operational Security Capability Model

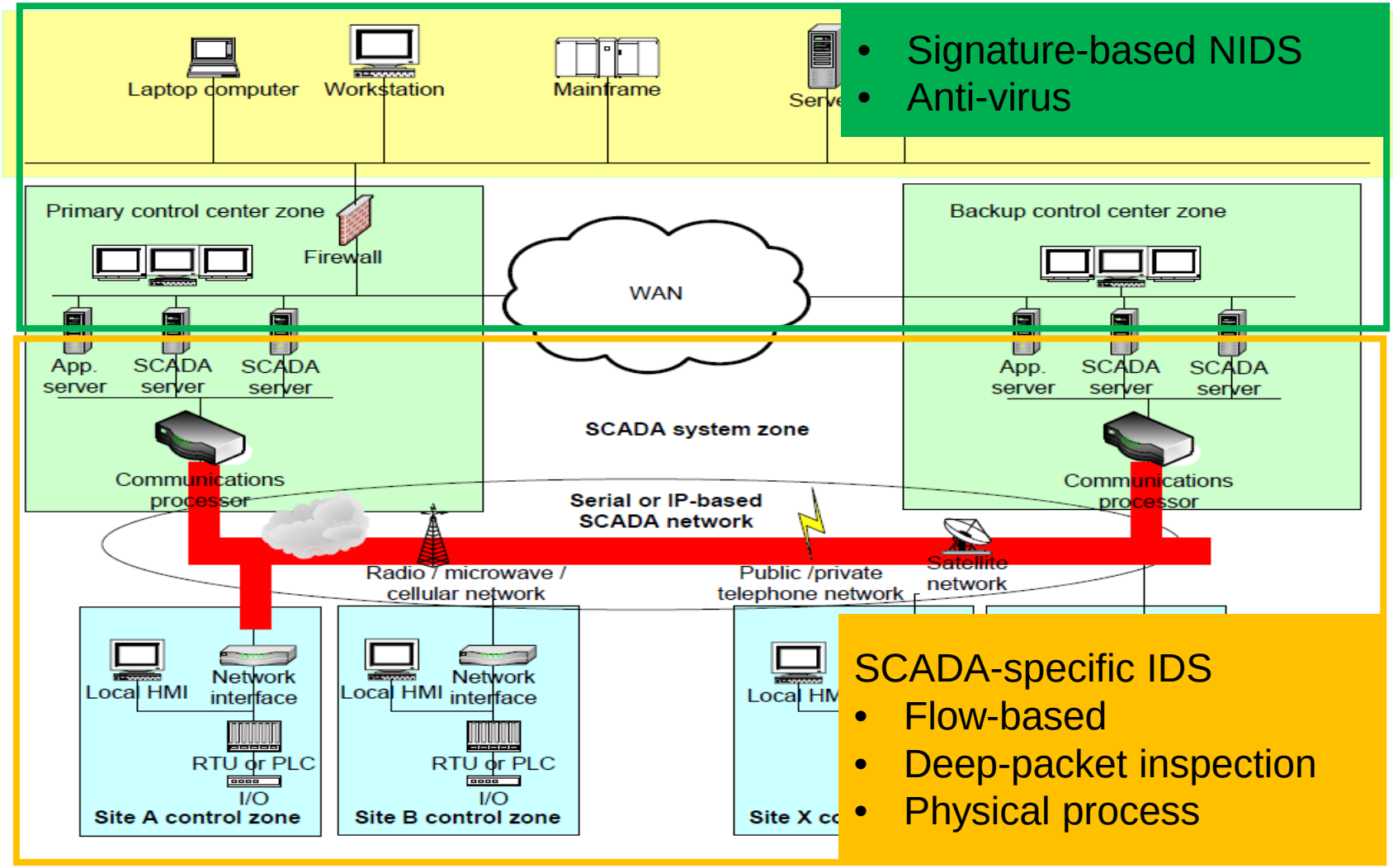
Vienna, 13 March 2017

DSO-oriented Operational Security Capability Model

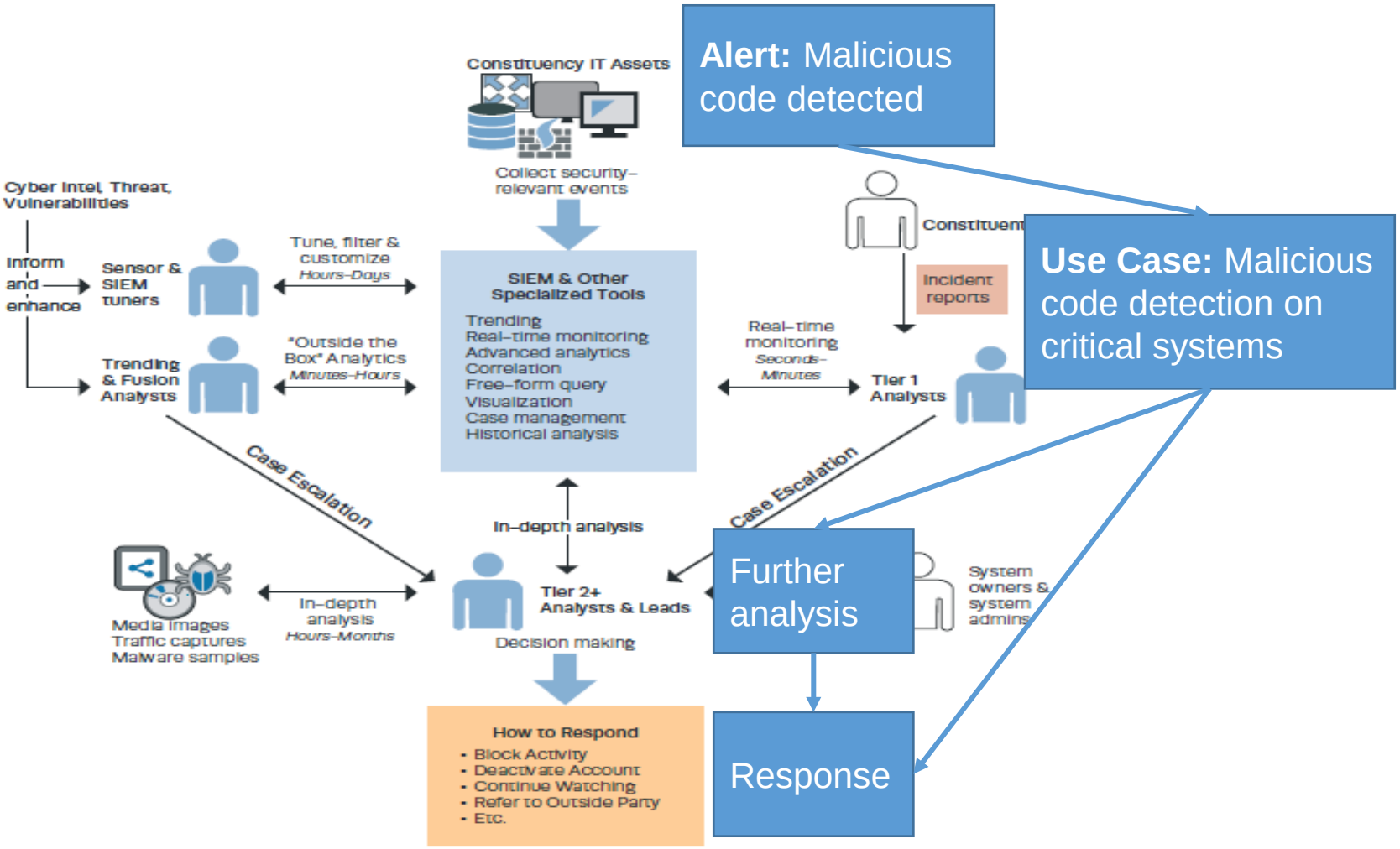
Abstract – Many DSOs are setting up operational security teams to monitor their networks for vulnerabilities and attacks. This talk presents a model for the capabilities they need to develop to make such teams effective.

Intrusion Detection in SCADA Systems

ENCS



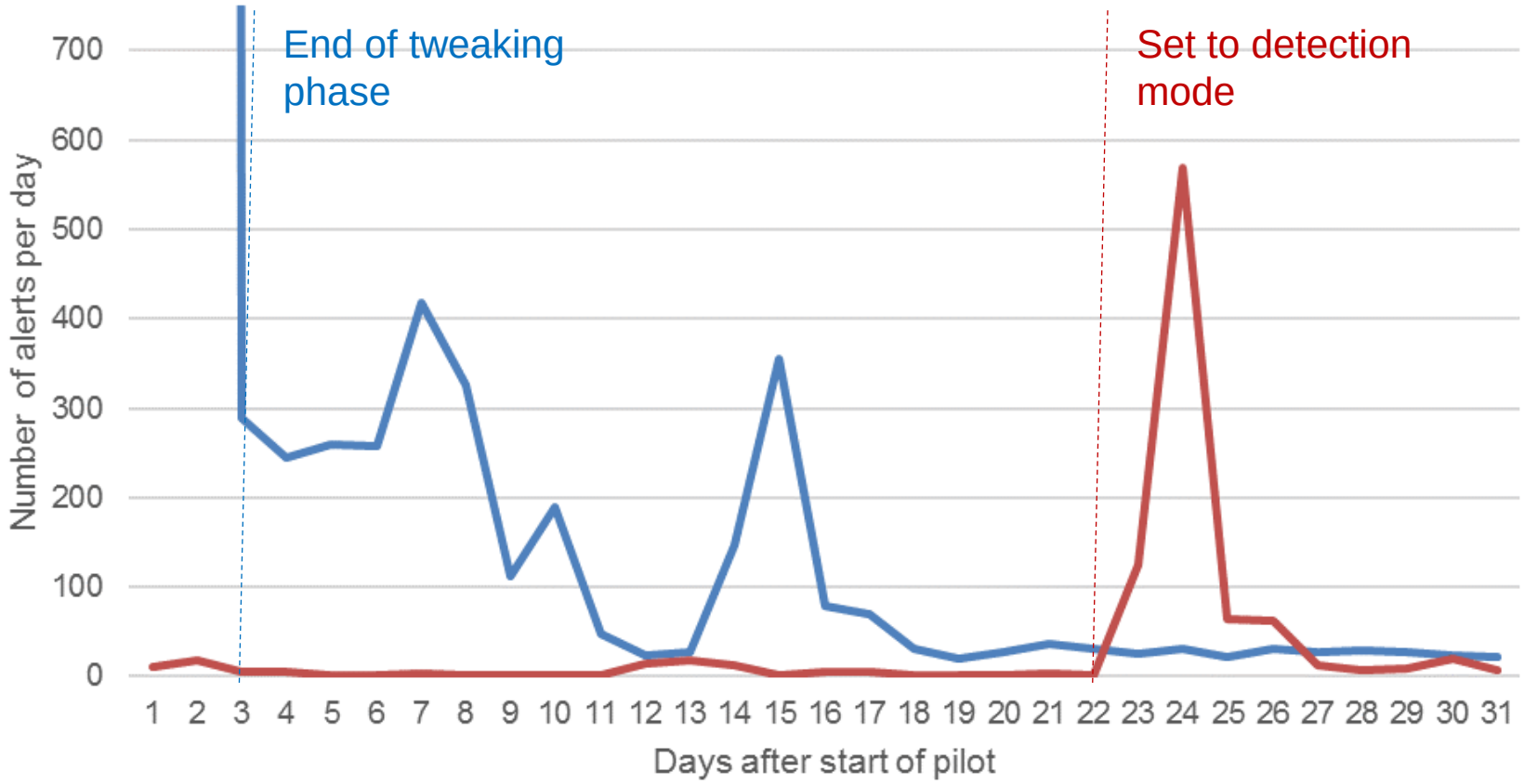
IT Processes: Triage



Fewer Alerts in OT Domain

ENCS

Number of alerts for two SCADA-specific IDS systems



Different Type of Alerts

ENCS

Examples of alerts from SCADA IDS pilots:

- New communication protocol detected (e.g. DNS)
- New host in the network
- Unexpected restart(s) of IEC104 field device
- Unpermitted usage of ASDU types

How do you react to this?

Goal for OT Security Operations

Preventing APTs from reaching their goal is beyond reach

More productive goals:

- Understanding system leads to better preventive measures
- Monitoring helps in preparing for a major incident
- Business case can be based on quicker recovery

Choose Detection Activities to Counter Risks

ENCS

Threats	Detection Activities
Exploitation of software vulnerabilities in SCADA servers through IT data exchange interface	• Misuse detection in DMZ • Monitoring the network access policy • Misuse detection in SCADA zone • Anomaly detection on session data
Exploitation of software vulnerabilities in SCADA servers from a substation	• Monitoring the network access policy • Misuse detection in SCADA zone • Anomaly detection on session data • Detection of malformed SCADA packets
Commands to RTUs from unauthorized hosts	• Monitoring the network access policy • Monitoring system assets • Anomaly detection on session data • Detection of unusual SCADA commands

Initial Capabilities for OT Security Monitoring

ENCS

Initially focus on small number of capabilities:

Situational Awareness	**Sensor Tuning**
	Network Mapping
	Vulnerability Scanning
	Situational Awareness
Handling Major Incidents	Cyber Intel Collection and Analysis
	Incident Analysis
	Incident Response

Capabilities needed in the future will be investigated in SEGRID

SEGRID

Thank You

Maarten Hoeve
Maarten.Hoeve@encs.eu