Security for smart Electricity GRIDs

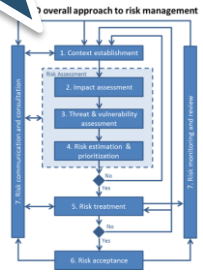
Operational Security Capability for DSOs

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no. 607109

Risk Management & SEGRID Innovations

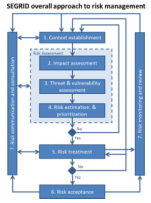
Risk management

Security officers
~ 1 year per cycle



Periodic update

Changes in:
- Threat landscape
- Infrastructure
- Business objectives
- Risk appetite



Power Grid Infrastructure

Power Grid Infrastructure

Power Grid Infrastructure

????
~ minutes to days per cycle

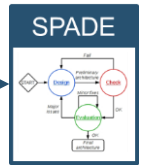
Security Operations

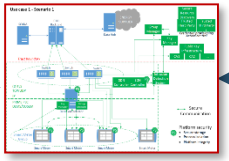
Vulnerability Management, Security Incident Monitoring & Incident Response

Operations

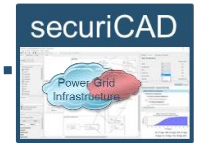
Development

Risk assessment





check



modelled

Security architects
~ 5 to 10 years per cycle

Development process

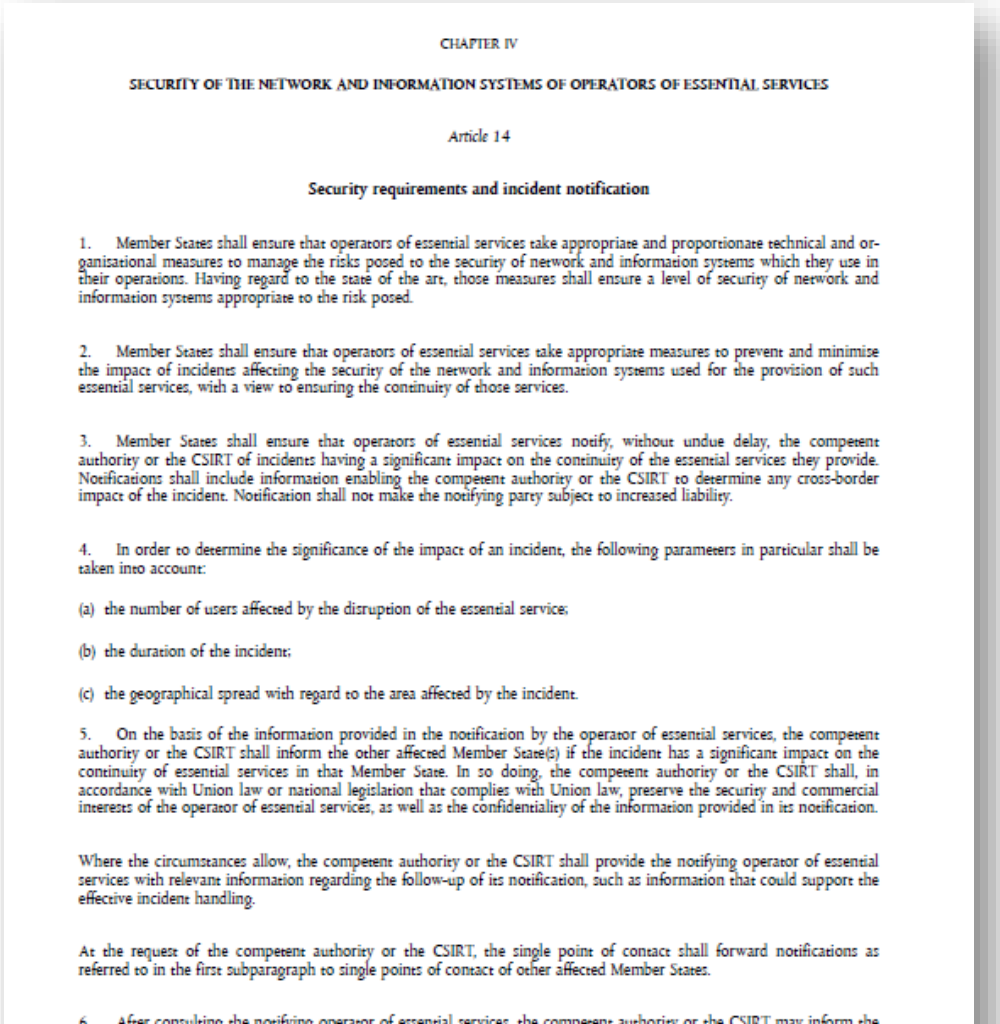
new system

Operational Security Capability Model

time

Regulatory Drive

NIS Directive



CHAPTER IV

SECURITY OF THE NETWORK AND INFORMATION SYSTEMS OF OPERATORS OF ESSENTIAL SERVICES

Article 14

Security requirements and incident notification

1. Member States shall ensure that operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed.

2. Member States shall ensure that operators of essential services take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, with a view to ensuring the continuity of those services.

3. Member States shall ensure that operators of essential services notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide. Notifications shall include information enabling the competent authority or the CSIRT to determine any cross-border impact of the incident. Notification shall not make the notifying party subject to increased liability.

4. In order to determine the significance of the impact of an incident, the following parameters in particular shall be taken into account:

(a) the number of users affected by the disruption of the essential service;

(b) the duration of the incident;

(c) the geographical spread with regard to the area affected by the incident.

5. On the basis of the information provided in the notification by the operator of essential services, the competent authority or the CSIRT shall inform the other affected Member State(s) if the incident has a significant impact on the continuity of essential services in that Member State. In so doing, the competent authority or the CSIRT shall, in accordance with Union law or national legislation that complies with Union law, preserve the security and commercial interests of the operator of essential services, as well as the confidentiality of the information provided in its notification.

Where the circumstances allow, the competent authority or the CSIRT shall provide the notifying operator of essential services with relevant information regarding the follow-up of its notification, such as information that could support the effective incident handling.

At the request of the competent authority or the CSIRT, the single point of contact shall forward notifications as referred to in the first subparagraph to single points of contact of other affected Member States.

6. After consulting the notifying operator of essential services, the competent authority or the CSIRT may inform the

1. Take appropriate measures to manage security risks
2. Take appropriate measures to prevent and minimize impact of incidents
3. Report incidents with significant impact to national CSIRT

Will need security operations to meet requirements 2 and 3

Why a Capability Model?

Traditional CSIRT Model

- Traditional model for security operations developed in early 2000s by CERT/CC
- **Reactive approach:** security operations team acts a service desk, reacting to calls and IDS alerts

List of Common CSIRT Services from CERT/CC, 2003

Why a Capability Model?

Modern Security Operations Centers (Telecom, Banking, …)

Modern SOC performs many activities to actively counter threats:

- Real-Time Analysis
- Incident Analysis and Response
- Scanning and Assessment
- Artifact Analysis
- Audit and Insider Threat
- SOC Tool Life-Cycle Support
- Intel and Trending

Table 1. SOC Capabilities

Name	Description
Real-Time Analysis	
Call Center	Tips, incident reports, and requests for CND services from constituents received via phone, email, SOC website postings, or other methods. This is roughly analogous to a traditional IT help desk, except that it is CND specific.
Real-Time Monitoring and Triage	Triage and short-turn analysis of real-time data feeds (such as system logs and alerts) for potential intrusions. After a specified time threshold, suspected incidents are escalated to an incident analysis and response team for further study. Usually synonymous with a SOC's Tier 1 analysts, focusing on real-time feeds of events and other data visualizations. Note: This is one of the most easily recognizable and visible capabilities offered by a SOC, but it is meaningless without a corresponding incident analysis and response capability, discussed below.
Intel and Trending	
Cyber Intel Collection and Analysis	Collection, consumption, and analysis of cyber intelligence reports, cyber intrusion reports, and news related to information security, covering new threats, vulnerabilities, products, and research. Materials are inspected for information requiring a response from the SOC or distribution to the constituency. Intel can be culled from coordinating SOCs, vendors, news media websites, online forums, and email distribution lists.
Cyber Intel Distribution	Synthesis, summarization, and redistribution of cyber intelligence reports, cyber intrusion reports, and news related to information security to members of the constituency on either a routine basis (such as a weekly or monthly cyber newsletter) or a non-routine basis (such as an emergency patch notice or phishing campaign alert).

Source: Carson Zimmerman, "*Ten Strategies of a World-Class Cybersecurity Operations Center*", MITRE, 2014

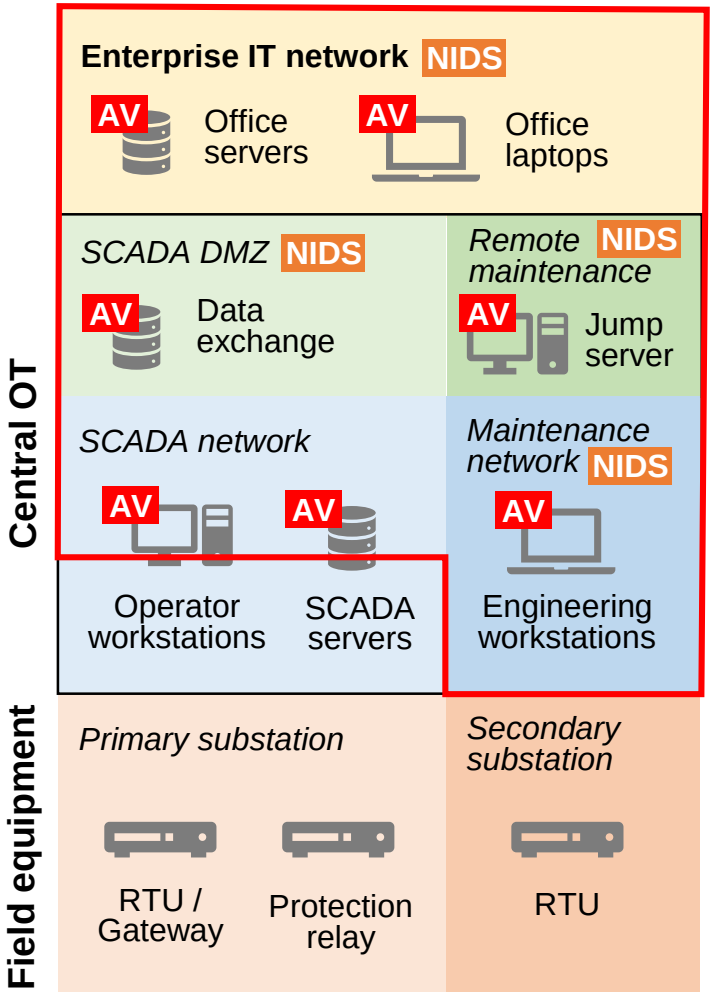
Activities are organized differently
But most SOCs develop similar capabilties

Challenges in Smart Grid Security Operations

1. New, anomaly-based detection technologies
2. Low alert and incident rates
3. Informal Operational Technology organizations

Challenges in Smart Grid Security Operations

New, anomaly-based detection technologies (1)



IT Detection techniques cover only part of Smart Grid systems

AV Signature- and host-based detection works on modern servers and workstations, but not on embedded devices

NIDS Signature- and network-based IDSs work for protocols used in IT, but not for SCADA protocols

Challenges in Smart Grid Security Operations

New, anomaly-based detection technologies (2)

Specialized intrusion detection systems have been developed for the OT domain. They are network- and anomaly-based, and usually offer two features:

1. **Flow-whitelisting:** the IDS can detect unusual network connections
2. **OT deep-packet inspection:** the IDS can parse OT communication protocols to detect malformed packets, and unusual commands and parameter

Challenges in Smart Grid Security Operations

New, anomaly-based detection technologies (3)

Typical **signature-based** alert: one possible cause, always malicious

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

Typical **anomaly-based** alert: many possible causes, most benign

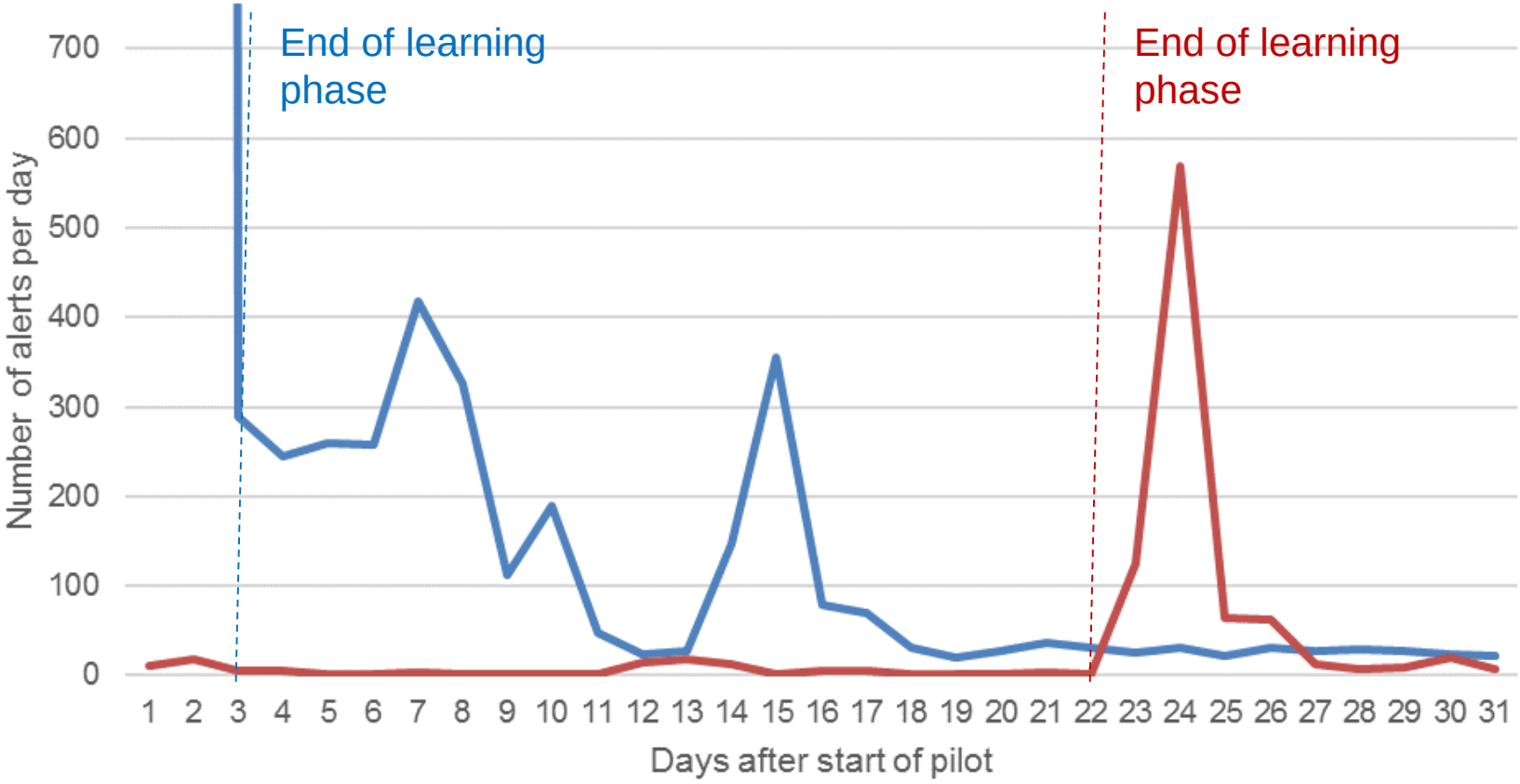
```
Communications host not whitelisted: the source host is not
whitelisted in any of the communication rules
```

Anomaly-based technology requires different capabilities to interpret alerts, and tweak the sensors

Challenges in Smart Grid Security Operations

Low alert and incident rates (1)

Alert rates for two anomaly-detection sensors in a pilot
Both stabilize at less than 20 alerts per day



Challenges in Smart Grid Security Operations

Low alert and incident rates (1)

Few real incidents should be expected in SCADA systems:

- SCADA systems only used by a few DSO employees
- Preventive measures should keep out non-targeted attacks
- Targeted attackers want to avoid incidents (until opportune)

Few false positives:

- Machine-to-machine interactions highly regular
- Sensors can be tweaked

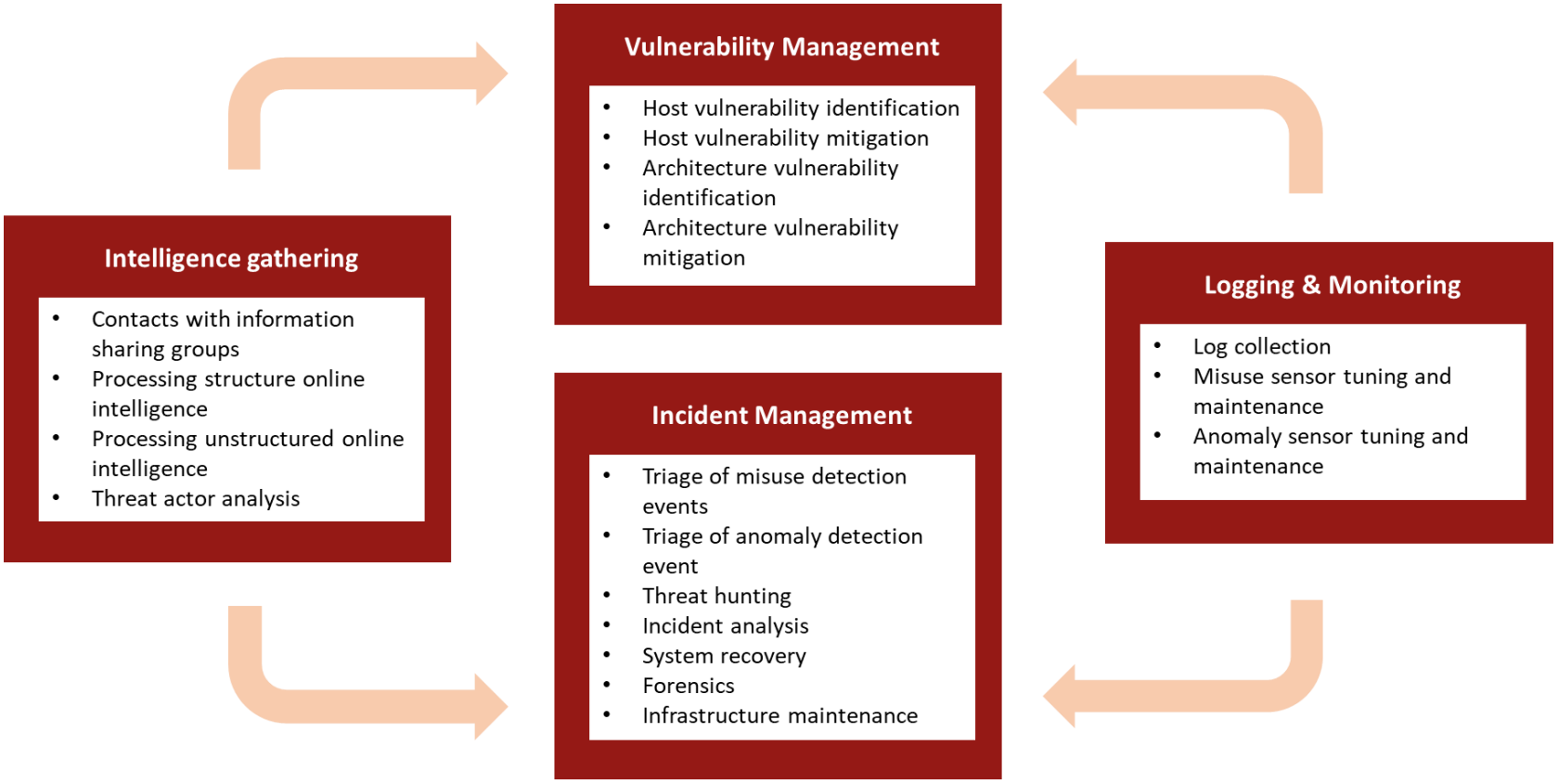
What should the SOC team do all day?

Challenges in Smart Grid Security Operations

Informal Operational Technology Organizations

- Lack of formal processes hinders security operations:
  - No up-to-date asset inventories
  - No up-to-date network maps
  - No formal change or configuration management
  - No tracking of maintenance schedules
- Security operations team needs to work closely with operational technology departments to:
  - Affect technical improvements in components and architecture
  - Affect organizational improvement

Capability Model



Roadmap

Split of Responsibilities

OT engineering:

- Engineers attached to SCADA and substation engineering departments
- Possibly organized in an operational monitoring center
- Responsible for vulnerability management
- Acts as buffer between security operations teams, and engineering

Security Operations Team:

- Security specialists
- May be part of IT or external for smaller grid operators
- Responsible for incident management

Roadmap

Capabilities to Develop

	Impact aware	Vulnerability aware	Threat agent-aware	Threat actor aware
OT engineering	System recovery Manual host vulnerability identification & mitigation Manual architecture vulnerability identification & mitigation			
Security operations team				

Impact aware phase:

- Aware of critical assets
- Security operations to protect and restore them

Roadmap

Capabilities to Develop

	Impact aware	Vulnerability aware	Threat agent-aware	Threat actor aware
OT engineering	System recovery Manual host vulnerability identification & mitigation Manual architecture vulnerability identification & mitigation	Automated host vulnerability identification & mitigation Automated architecture vulnerability identification & mitigation Basic anomaly sensor tuning and maintenance Basic triage of anomaly detection events		
Security operations team		Basic contacts with information sharing groups		

Vulnerability aware phase:

- Continuously aware of current vulnerabilities
- Security operations to actively mitigate high risk vulnerabilities

Roadmap

Capabilities to Develop

	Impact aware	Vulnerability aware	Threat agent-aware	Threat actor aware
OT engineering	System recovery Manual host vulnerability identification & mitigation Manual architecture vulnerability identification & mitigation	Automated host vulnerability identification & mitigation Automated architecture vulnerability identification & mitigation Basic anomaly sensor nce aly	Advanced anomaly sensor tuning and maintenance Advanced triage of anomaly detection events	
Security operations tear			Triage of misuse detection events & forensics Infrastructure maintenance & log collection Processing of online Intelligence	

Threat agent aware phase:

- Aware of local attacker actions
- Security operations react to them (risk-based)

Roadmap

Capabilities to Develop

	Impact aware	Vulnerability aware	Threat agent-aware	Threat actor aware
OT engineering	System recovery Manual host vulnerability identification & mitigation Manual architecture vulnerability identification & mitigation	Automated host vulnerability identification & mitigation Automated architecture	Advanced anomaly sensor tuning and maintenance Advanced triage of anomaly detection events	
Security operations team			n Processing of online Intelligence	Threat hunting Threat actor analysis Contacts with information sharing groups (advanced)

Threat actor aware phase:

- Aware of actors behind attacks
- Actively counter most dangerous actors

Roadmap

Capabilities to Develop

	Impact aware	Vulnerability aware	Threat agent-aware	Threat actor aware
OT engineering	System recovery Manual host vulnerability identification & mitigation Manual architecture vulnerability identification & mitigation	Automated host vulnerability identification & mitigation Automated architecture vulnerability identification & mitigation Basic anomaly sensor tuning and maintenance Basic triage of anomaly detection events	Advanced anomaly sensor tuning and maintenance Advanced triage of anomaly detection events	
Security operations team		Basic contacts with information sharing groups	Triage of misuse detection events & forensics Infrastructure maintenance & log collection Processing of online Intelligence	Threat hunting Threat actor analysis Contacts with information sharing groups (advanced)

Questions

Mail: info@segrid.eu
Website: www.segrid.eu
Telephone: +31 8886 67758

Project type: Collaborative project – small or medium scale focused research project
Grant agreement no: 607109
Thematic Priority: FP7-SEC-2013-1
Start date of project: October 1st, 2014
Duration: 36 months
Coordinator: TNO, The Netherlands