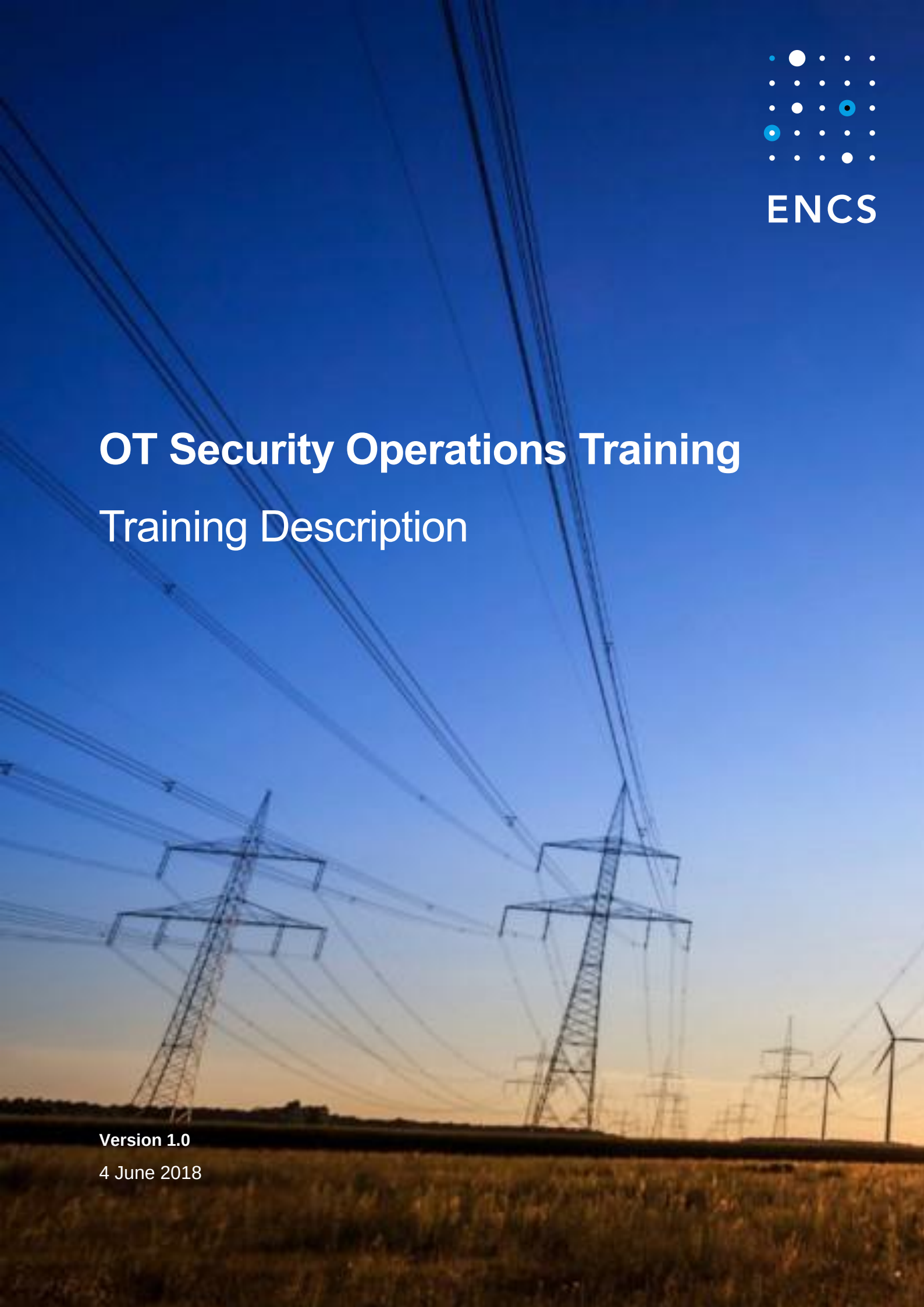

ENCS

OT Security Operations Training

Training Description

Version 1.0

4 June 2018

ENCS Security Operations Training

Are you seeing all security vulnerabilities and incidents in your OT systems? Only a few years ago, many grid operators were completely blind. They would only notice an incident if it would disrupt normal operations.

Since then, a lot has improved in gathering security data. Network-based sensors are being deployed in OT, and SIEM systems are used to gather logs. The risk now is rather data overload. One badly configured sensor can give thousands of false alarms today, burying the rare relevant events.

The solution needs to come from smarter analysts. You need people that can tune sensors to monitor for the biggest risks. Who can spot the one event that could come from an advanced threat, and can analyze this event to find out what happened.

In 2017, ENCS ran a highly valued member project on OT security monitoring. Security experts at ENCS and its member together defined use cases to cover the biggest security risks. New security sensors for OT were evaluated in a lab. And best practices were shared and written down in whitepapers.

ENCS has now made all this information available in a two days training, so that anyone can quickly get the latest knowledge on OT security monitoring for use in their daily work

Who Should Attend This Training?

The training is designed for staff responsible for finding vulnerabilities and detecting incidents in operational technology (OT) systems. This includes engineers and system administrators of OT systems who are specializing in security, as well as analysts of IT security operations centers and CSIRTs who are moving into OT.

Training Objectives

Participants learn how to:

- choose monitoring use cases to counter the biggest security risks
- choose the right sensors and data sensors to cover the whole OT domain
- identify vulnerabilities and mitigations
- analyze alerts and possible incidents
- configure and use the new security sensors developed for OT

Program

The training consists of the following modules:

1. Risk-based detection strategy	• Learn what use cases can be applied in OT systems • Learn how to select use cases based on risks • Apply the risk-based selection to a SCADA system

2. Vulnerability management	• Learn how to structurally manage vulnerabilities to make sure they are really fixed • Learn how to find vulnerabilities on individual hosts • Learn how to find vulnerabilities in network architectures • Learn how to prioritize vulnerabilities based on real-world examples • Learn how to find fixes and mitigations that work in OT systems (including legacy systems)
3. Misuse detection	• Learn how to use IT intrusion detection sensors in OT • Learn how to analyze deep-packet inspection alerts on malformed packets
4. Access monitoring	• Learn how to analyze logs for unusual access • Learn how to set up flow whitelisting • Learn how to analyze alerts for new hosts and connections
5. Reviewing action logs	• Learn how to analyze logs for unusual maintenance actions (e.g. someone installing backdoors) • Learn how to configure and use deep-packet inspection to detect unusual actions in SCADA systems
6. Bringing it all together	• Analyze how the different use cases would have detected the attacks in Ukraine in 2015 and 2016, and the Industroyer malware • Practice hands-on with detecting a similar attack • Learn how to correlate information from the different use cases learned in earlier modules

The training emphasizes hands-on practice. Participants practice how to analyze incidents in exercises with realistic traffic captures or log files.

Practical information

Location: The training is held at Schiphol airport to allow easier travelling.

Training times: the training consists of two days:

- Day 1: 10:00 – 17:00
- Day 2: 9:00 – 15:00

Dinner: on the evening of Day 1 there is a dinner to allow for networking between the training participants. The dinner is included in the training price.

Prerequisites: participants are expected to have knowledge about:

- TCP/IP networking
- Wireshark

Some Linux knowledge, and knowledge about the IEC 104 and IEC 61850 protocols is useful, but not mandatory.

Laptop required: participants are expected to bring their own laptop with Wireshark installed.

Price: 1,500 euros per participant