BEING PREPARED – INCIDENT RESPONSE IN ENERGY

MIKA NORTUNEN

MANAGER, PRODUCT SECURITY INCIDENT RESPONSE

CYBER-AS-A-SERVICE

WÄRTSILÄ CORPORATION

FOUNDED IN 1834

GLOBAL LEADER

in sustainable solutions for the marine and energy markets

2018

Turnover
5 174 MEUR

Operating result
543 MEUR

Order intake
6 307 MEUR

Operations in
200 LOCATIONS

Our personnel
APPROX. 19 000

Nationalities
135

ENABLING SUSTAINABLE SOCIETIES WITH SMART TECHNOLOGY

INNOVATING SINCE 1834

TOGETHER

FOR A SUSTAINABLE FUTURE

ENERGY MARKET TRENDS & DRIVERS

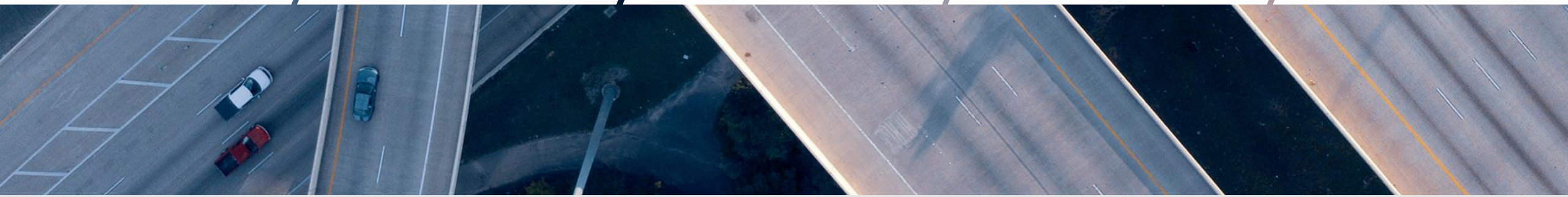
RAPIDLY INCREASING RENEWABLES

DECENTRALIZED ENERGY

INCREASING ROLE OF FLEXIBLE GAS

EMERGING STORAGE TECHNOLOGY

DATA & DIGITALIZATION



OTCSA AND WÄRTSILÄ

OT CSA

OT Cyber Security Alliance

ABB

BlackBerry CYLANCE

Check Point SOFTWARE TECHNOLOGIES LTD

FORESCOUT

FORTINET

Microsoft

MOCANA

nccgroup

Qualys

SCADAfence

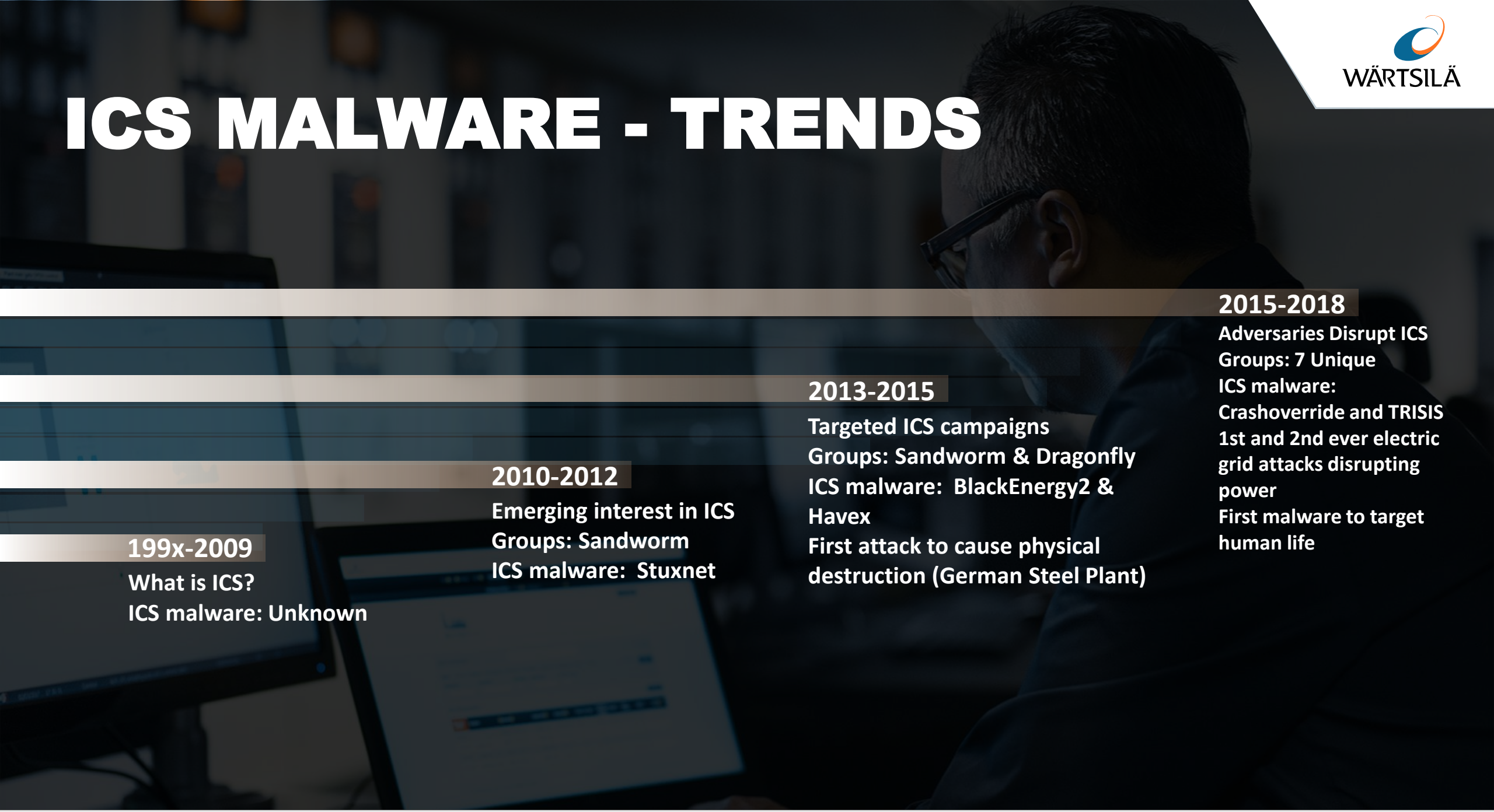
splunk>

WÄRTSILÄ

https://otcsalliance.org/

SECURITY MODEL: HOW PROACTIVE AND REACTIVE CYBER CONTROLS ENHANCE THE PRODUCT SECURITY

ICS MALWARE - TRENDS



199x-2009

What is ICS?
ICS malware: Unknown

2010-2012

Emerging interest in ICS
Groups: Sandworm
ICS malware: Stuxnet

2013-2015

Targeted ICS campaigns
Groups: Sandworm & Dragonfly
ICS malware: BlackEnergy2 & Havex
First attack to cause physical destruction (German Steel Plant)

2015-2018

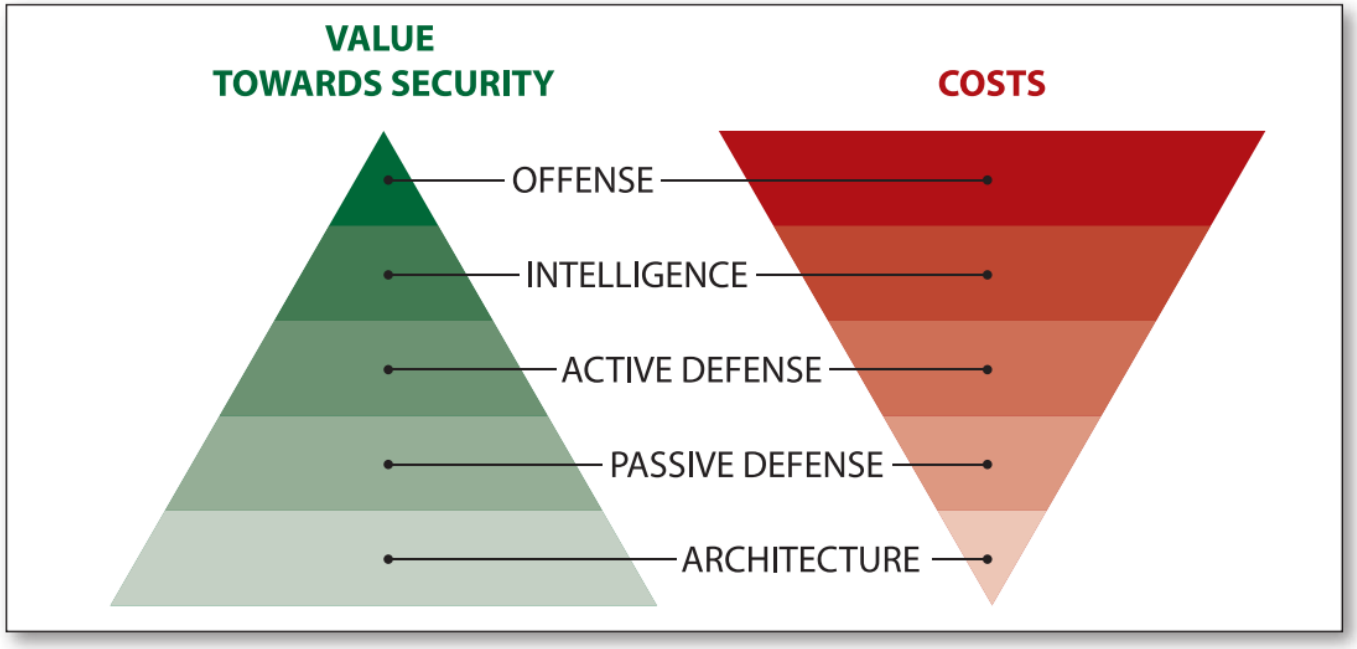
Adversaries Disrupt ICS
Groups: 7 Unique
ICS malware: Crashoverride and TRISIS
1st and 2nd ever electric grid attacks disrupting power
First malware to target human life

INCIDENT RESPONSE´S PURPOSE

- Safety as the number one priority
- Preserve operations while acquiring forensic quality evidence
- Evaluate the scope of the incident
- Support recovering actions

COSTS VS VALUE TOWARDS SECURITY

- Applying right controls in the right places
- Doing the basic stuff before jumping into more advanced measures



https://www.sans.org/reading-room/whitepapers/ActiveDefense/sliding-scale-cyber-security-36240

ESSENTIAL PREREQUISITIES

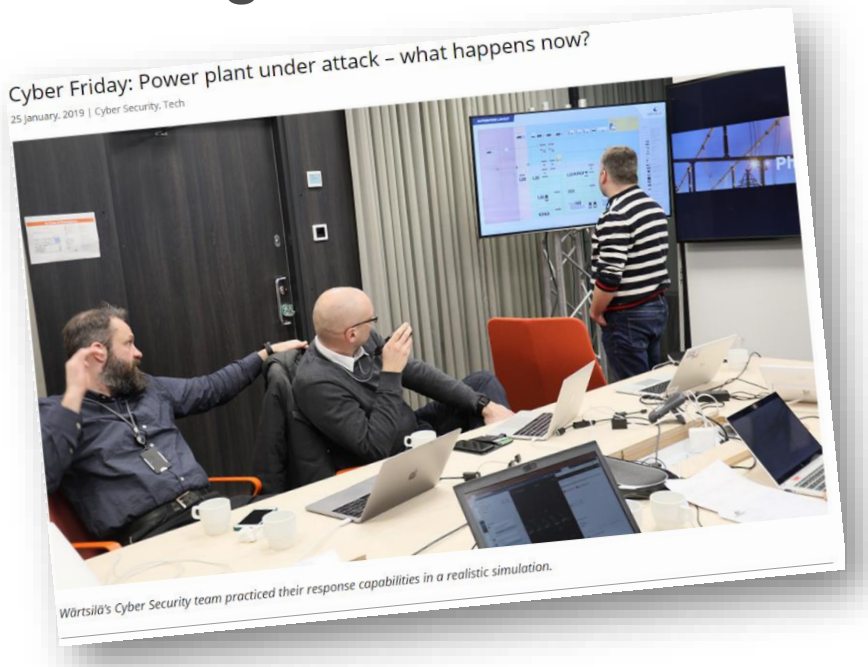
- Know your environment - *you can´t protect what you don´t know you have*
  - Up-to-date asset inventory, architectural documentation, purpose and criticality of assets etc.
- Playbooks, processes, roles and responsibilities

TECHNICAL PREPARATION

- Understanging your baseline
- Network data
  - Active monitoring or pre-configured/prepared port(s) for traffic captures
  - Pre-installed network taps
- Host data
  - Log data, event data
  - Memory images when needed
    - Possibly prepared collectors (e.g. Redline)
- Log data from the network devices
- (Log data from PLCs etc.)

TRAIN AS YOU FIGHT

- Training, exercises




WÄRTSILÄ