Addressing Cyber Threats in Power Generation and Distribution

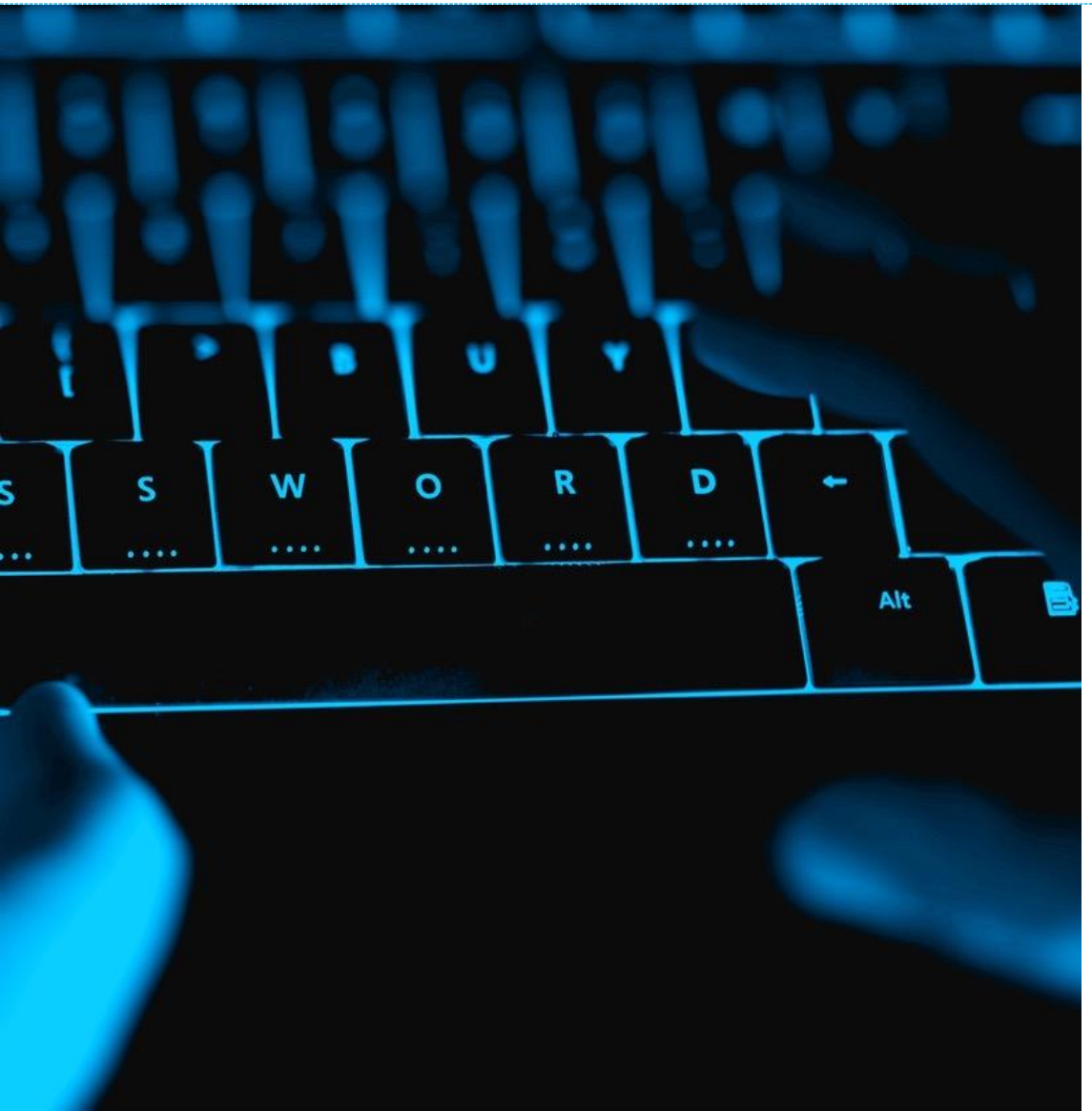
VEO, Asko Tuomela

- Bachelor of Science in Electrical Power Engineering
- Over 6 years experience in power projects, PLCs and supervision systems
- 16 years in several positions in local teleoperator’s IT management
- Development Manager, Cyber Security at VEO Oy

Cyber security

- In general
- In the energy sector

Cyber security trends



- Cyber threats are evolving and becoming more difficult to prevent and detect
- Attack surface increases: Amount of systems is increasing, and they are getting more complex and interconnected

- ***Probability to get breached increases***

Impacts of cyber attacks

- Companies, consumers and society are more and more dependent on different types of network-connected systems and services
- ***Impact of acts in cyber space is increasing***

EU and national legislation

- EU NIS directive
  - Network and systems security requirements for EU member states
  - Directive concerns:
    - EU member states' information security cooperation with EU and member states
    - Key services providers from different industry sectors including electric power generation and distribution
- Finnish act on electricity market, add-on 29 a §
  - Derived from the EU NIS directive
  - Electricity grid operator has obligation:
    - To have risk management in place for its systems and communication networks
    - To inform energy authorities about information security-related incidents

Cyber security standards

- Several standards address cyber security
  - Most known and widest adopted are standard series of IEC 27000 and 62443, where IEC 27000 is mainly targeted to company's internal information security, and IEC 62443 to industrial production and it's supply chain.

- Investments and efforts in cyber security development should be suitably scaled to the protected asset.

Cyber security in Finland’s critical infrastructure

- Finland has a geopolitically strategic location
  - Key players have most likely already mapped Finland’s strategic targets in critical infrastructure, and cyber warfare methods against them

- Finland’s national emergency supply agency has ordered from VTT a group of cyber security development projects

VEO will participate in a pilot project focusing on energy sector’s cyber threats

Cyber security in the energy sector

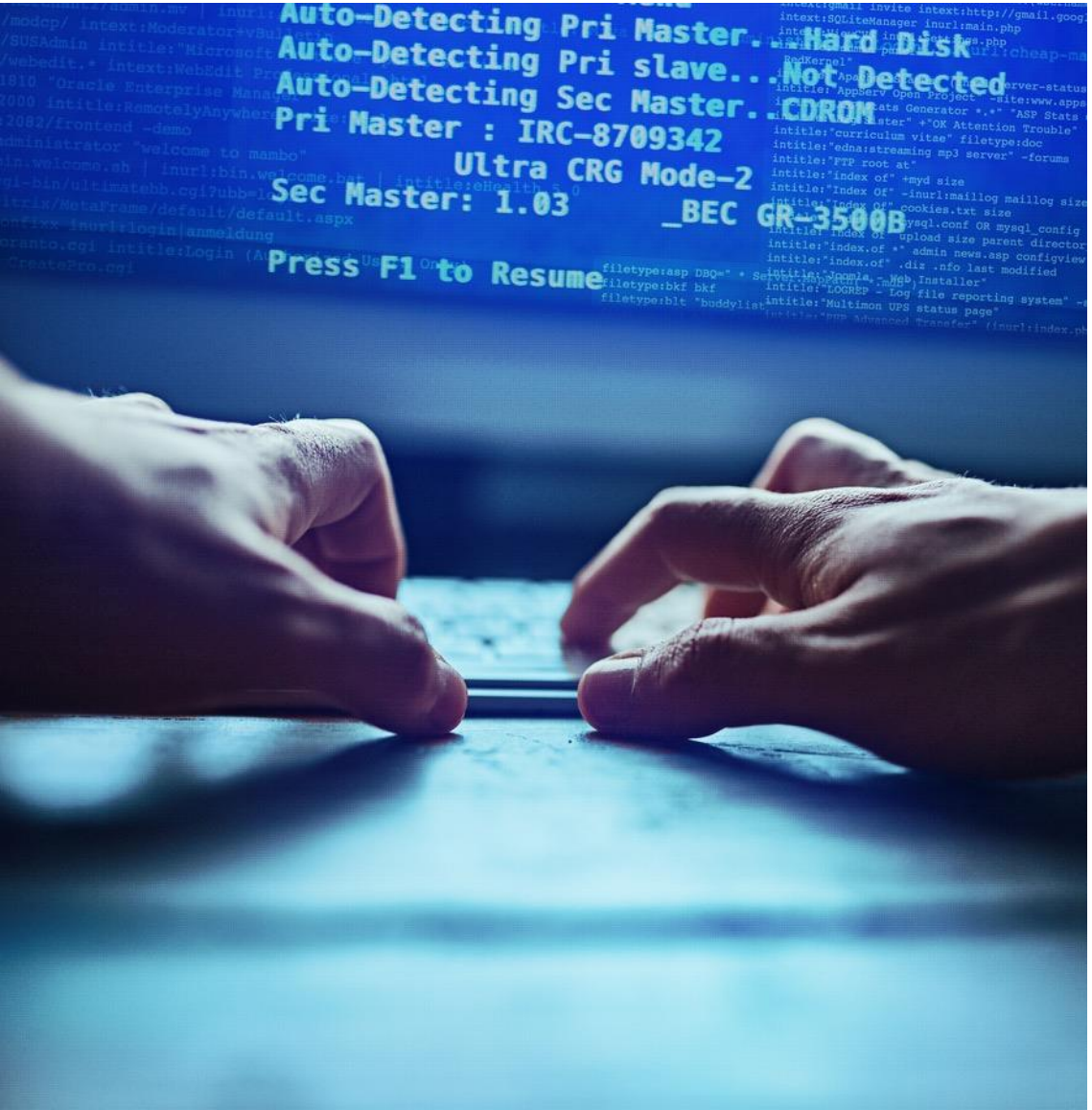
- General cyber threats also have an impact on industrial control systems used in the energy sector
- Power plants and electricity grids form the most important part of society's critical infrastructure
- ***The energy sector's supply chain is an attractive target to cyber attacks***

ICS Cyber Security

- **Attack process**
- **Defending**
  - From the big picture to the details
  - What VEO can offer

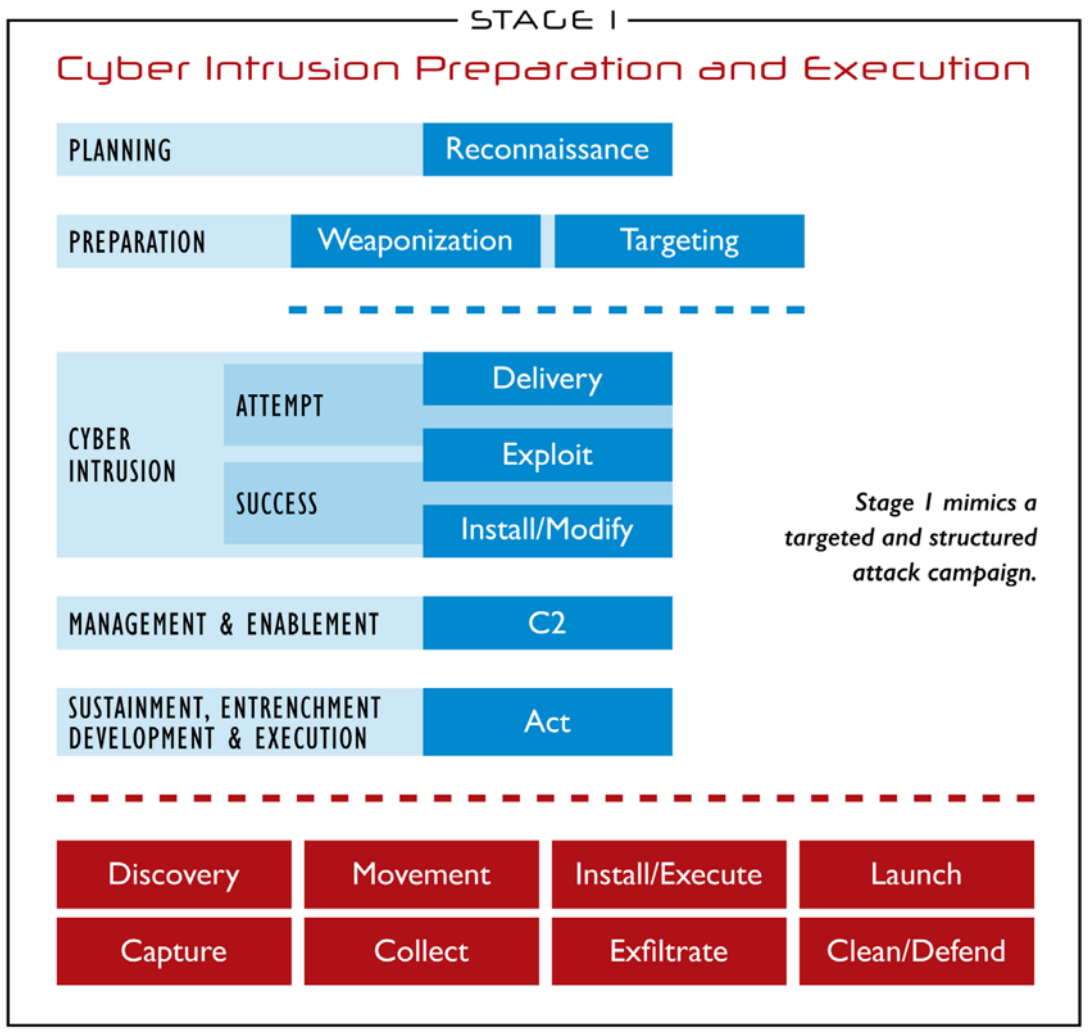
VEO

ICS Cyber Kill Chain

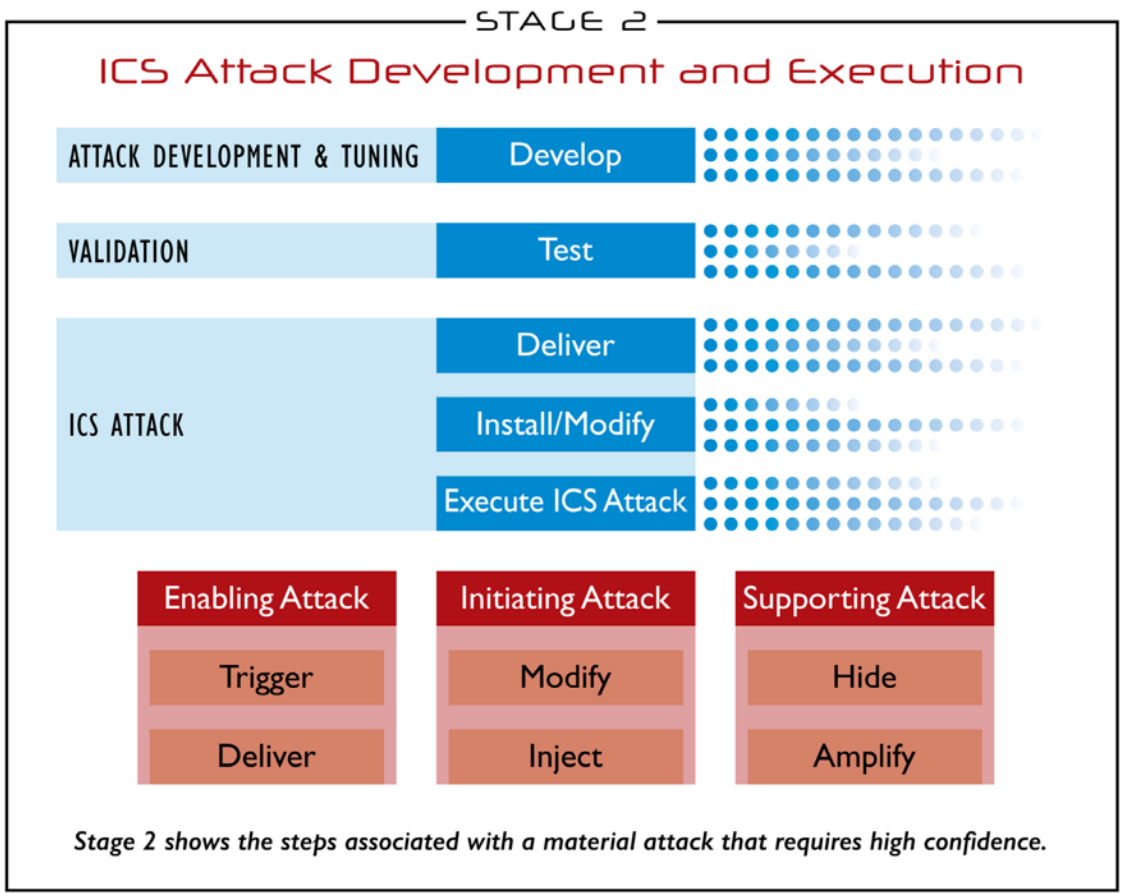


- Kill Chain is a warfare method meaning the process that attackers takes to achieve their final goals
- Cyber Kill Chain was originally developed by Lockheed Martin
- SANS Institute added stage 2 on top of the original concept
- Stage 1 and 2 forms together the **ICS Cyber Kill Chain**

VEO



Based on the Cyber Kill Chain® model from Lockheed Martin



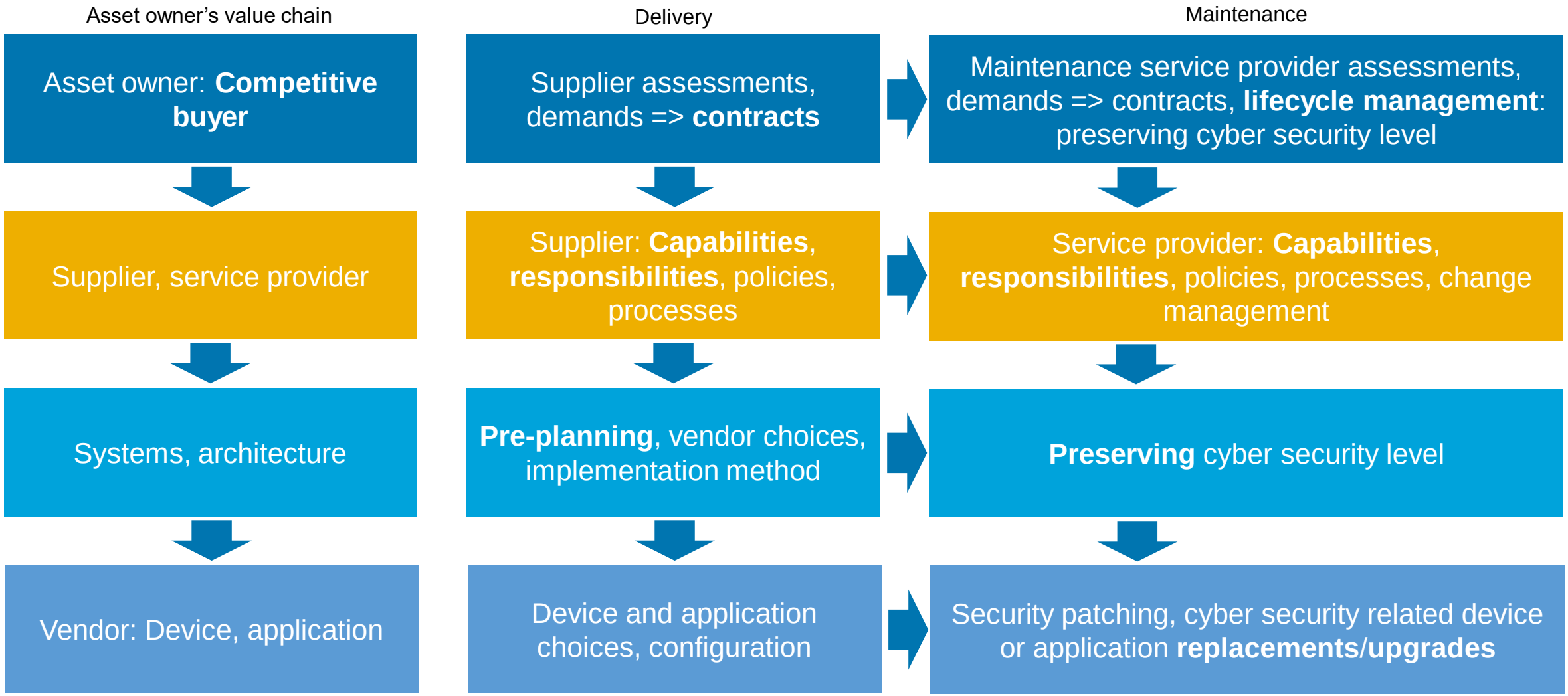
VEO

*) Graphics from SANS Institute's document, "The Industrial Control System Cyber Kill Chain"

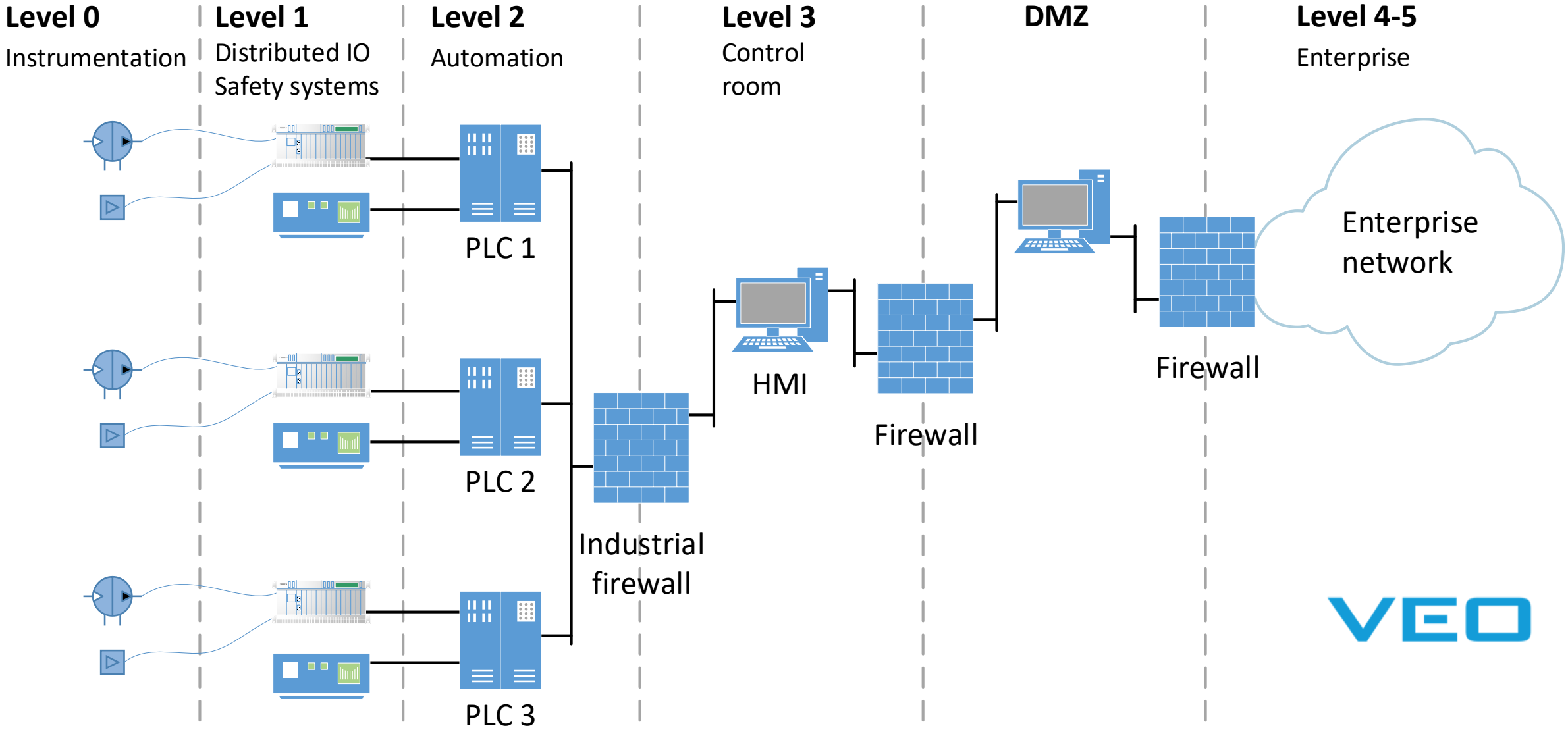
Malware targeted at the energy sector

- In the past there have been industrial control system-targeted malware, like **Stuxnet** and **BlackEnergy**
- In the end of 2016, Ukraine faced large blackouts in Kiova electrical grids, caused by cyber attack
  - It turned out that it was specifically energy sector-targeted malware (Industroyer/ Crashoverride), which abused automation protocols IEC 101, 104, 61850 and OPC DA to open breakers and disconnectors in substations

Cyber security management



ICS, defense in depth architecture



ICS cyber defenses, key elements

- ✓ **Defense in depth / zones:** instrumentation, safety, PLC, HMI, DMZ (broker), enterprise, internet
- ✓ **Air gap to internet:** Both inbound and outbound traffic to internet blocked
- ✓ **ICS production and management separated at network level:** PLCs, safety relays, safety logic, RTUs
- ✓ Only necessary automation protocol traffic enabled
- ✓ Remote maintenance connections default off
- ✓ Strong authentication in remote connections
- ✓ **Physical methods against cyber acts**, like local/remote switches
- ✓ Application whitelisting on HMIs
- ✓ Malware screening on transient media

VEO

ICS cyber defenses, notes

- ✓ **In the end, it's all about details!**
- ✓ Don't forget continuity management, like HMI disaster recovery backups and restore tests
- ✓ **Put focus on the 1st line of defense:** Educate personnel against initial intrusion attempts
- ✓ Windows and Linux PCs are hot spots, embedded devices also!
- ✓ Internet-facing devices are hot spots
- ✓ **Detection is as important as prevention is**
- ✓ Take care of those USB sticks!
- ✓ You have to know normal, to better detect abnormal
- ✓ Network traffic visibility at **application layer**
- ✓ In the edge, **traditional firewall is not enough anymore**

VEO

VEO’s cyber security services

- **Cyber security assessments** for existing power plants
- **Named cyber security officer**
- Cyber security taken into account in **delivery projects**
  - Different types of power plants
  - Substations
  - Industry
  - New installations and refurbishing projects

VEO is ready to help with cyber security

- We can help your company in cyber security-related matters and development
- We offer cyber security services especially to power plants and substations, and also to other industrial environments

We want to utilize our expertise by participating in our customers' cyber security development processes!

VEO

Ready for new challenges!