



Cyber threats and attacks in ICS

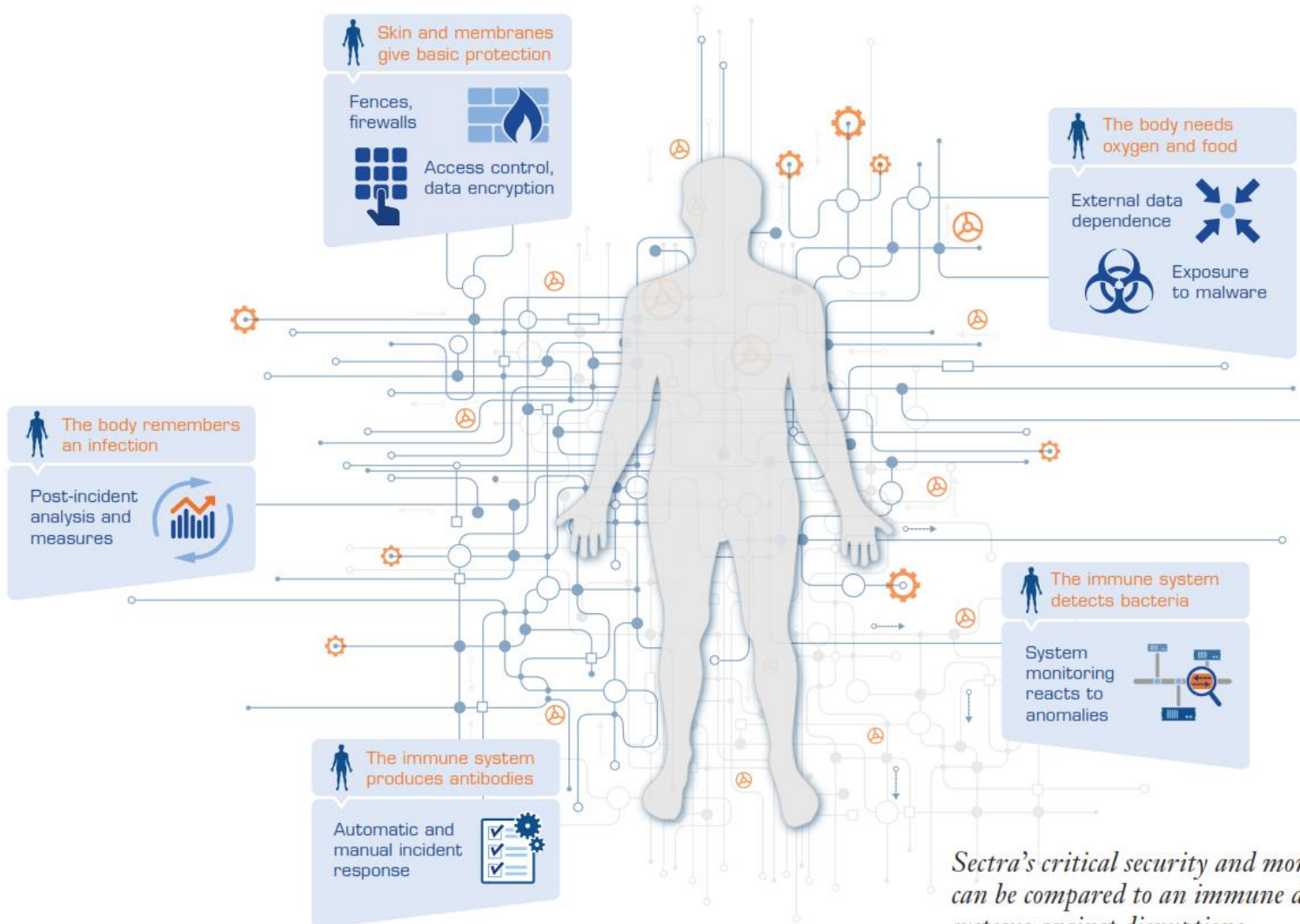
Geode Springseminar 29.5.2018

Lauri Haapamäki
Sectra Communications Oy
lauri.haapamaki@sectra.com
+358 400 254059

SECTRA

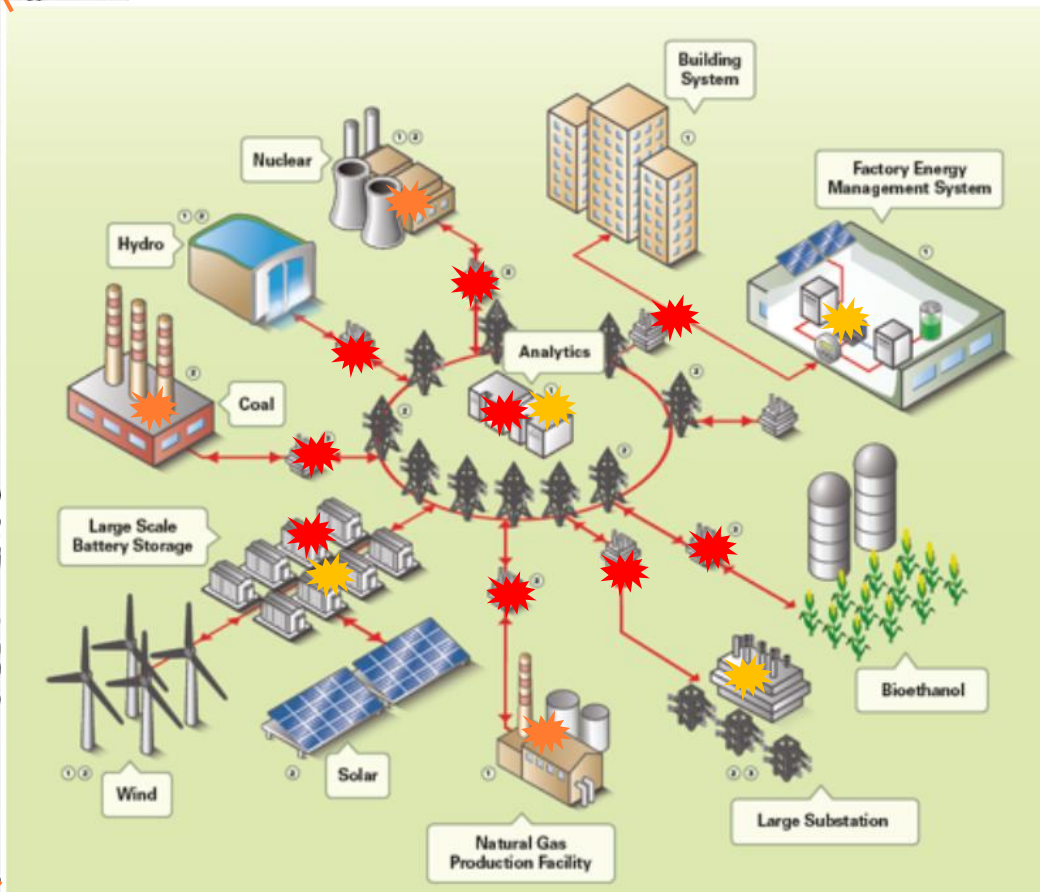
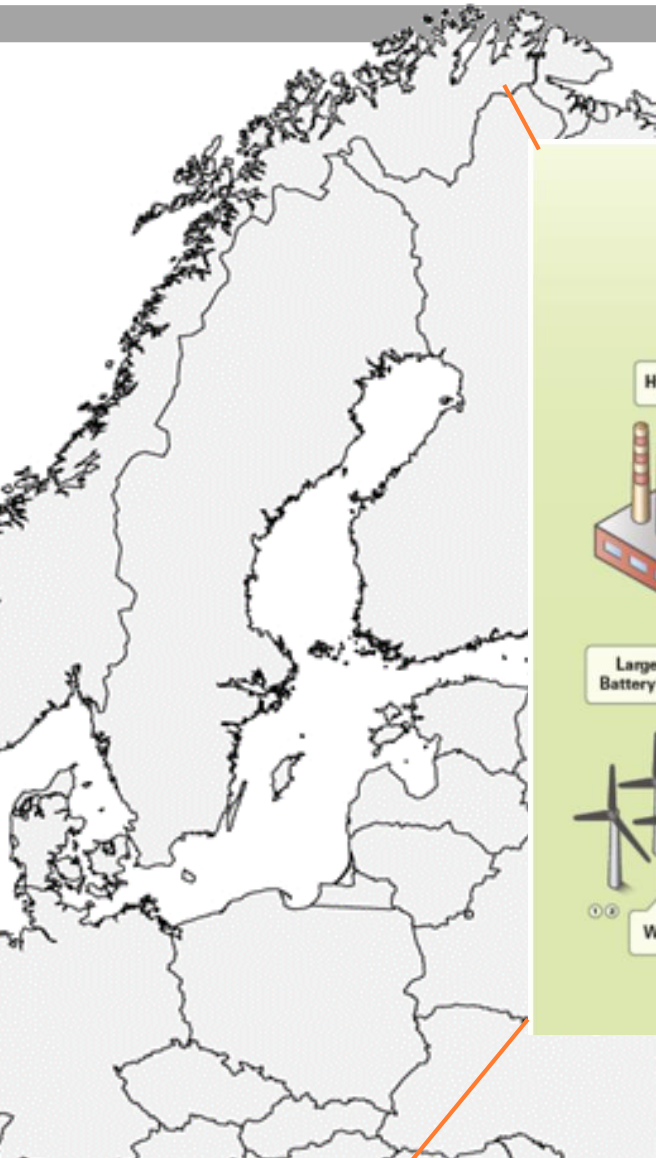
Knowledge and passion





What is cyber risk



Secra's critical security and monitoring services can be compared to an immune defense that protects systems against disruptions

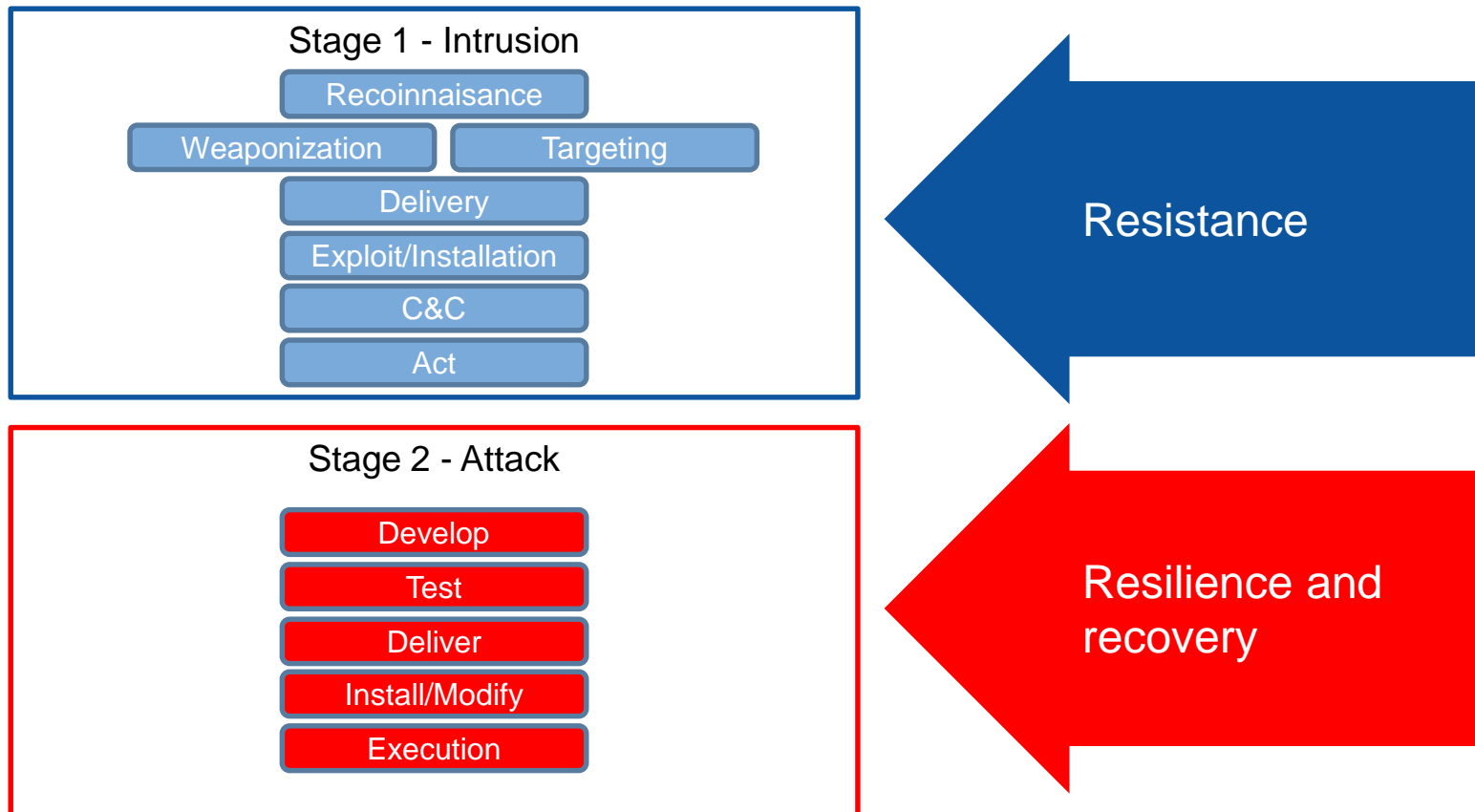
Total security of the society is at stake



-  Black energy
-  WannaCry
-  Dragonfly
-  Indicative



ICS Cyber kill chain



Source: SANS Institute

Resistance and Resilience are different things and capabilities!

Black energy

- Well documented and studied attack into Ukrainian distribution network with service loss to 225000 end users
- December 2015 but new variants emerging even today
- Specifically targeting ICS and energy companies
- Trojan based hack which enables access to ICS control
- How to protect
 - Strong authentication
 - Patching
 - Strong administrative policies
 - User training



Petya / NotPetya

- 2017 series of attacks with Ukraine as the main target but infections widely also elsewhere in Europe
- First version needed user to download and approve. The evolved and got in from “MeDoc” accounting widely in use in Ukraine, when its update was compromised
- Ransomware attack
- Targeting business and industrial infrastructures – shows wannacry was only the beginning
- Maersk hit with tens of millions of damages (up to billion) 45000 PCs and 4000 servers reinstalled
- How to protect
 - Strong authentication
 - Patching
 - Strong administrative policies
 - Network monitoring and separation
 - User training



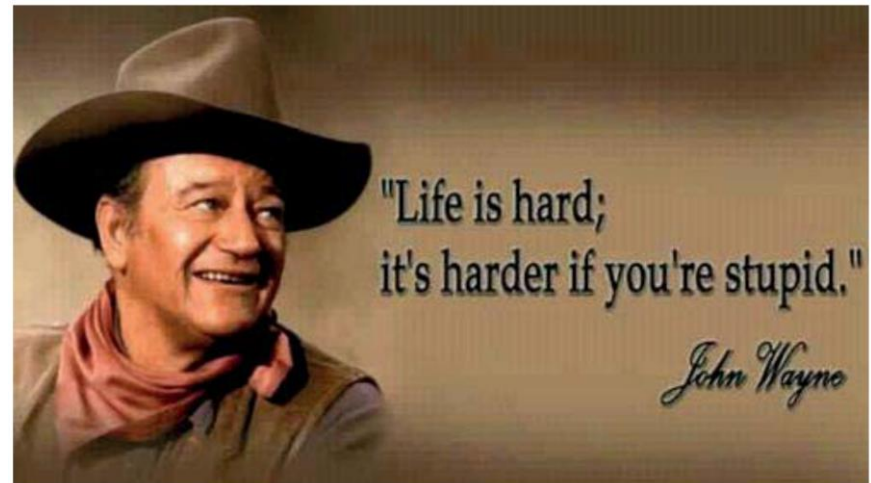
VPNFilter

- Very recent – reported by FBI in past week publicly and revealed by Cisco Talos
- More than half million routers compromised creating botnet in several countries
- Can intercept, monitor and impact passing data. Evolves in steps and enables Modbus SCADA features...
- Targets ICS
- How to protect
 - Strong authentication
 - Patching
 - Network monitoring and separation
 - Strong administrative policies
 - User training



In conclusion

- Threats are real!
 - Even nation state based
- Cyber security is a continuous process
 - Security assessments
 - Monitoring
 - Cyber insurance
- Response is a joint effort
 1. Victim
 2. Cyber security service companies
 3. ICS vendors
 4. Police and government i.e. NCSA







Thanks!

Geode spring seminar 29.5.2018

Lauri Haapamäki
Sectra Communications Oy
lauri.haapamaki@sectra.com
+358 400 254059

SECTRA

Knowledge and passion