Network Protection for Energy Control Systems

CSP004_C_E

PRESENTATION BY:

- **CRISTINA ALCARAZ**
  UNIVERSITY OF MALAGA, SPAIN

Acknowledgement

- *Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.*
- *Project Agreement no. 101083594*

Topic-4: Advanced Protection for Energy Control Networks

Overview

- Intrusion detection techniques and systems
- Advanced monitoring systems
- Final remarks
- References and sources

Topic-4: Advanced Protection for Energy Control Networks

Overview

- Intrusion detection techniques and systems
- Advanced monitoring systems
- **Final remarks**
- References and sources

Final remarks

- In this topic, we have **explored relevant intrusion detection techniques**, mechanisms and tools, providing a clear overview of:
  - Their configuration and deployment in real environments, such as energy control networks.
  - Precision characteristics and particular advantages of different techniques
  - Security threats and challenges
  - Response measures and relevance for the prevention of critical systems
- Likewise, we have explored other advanced monitoring techniques such as SIEMs !
- NOW we are ready to activate the necessary mechanisms to protect critical control networks and their key resources

Topic-4: Advanced Protection for Energy Control Networks

Overview

- Intrusion detection techniques and systems
- Advanced monitoring systems
- Final remarks
- **References and sources**

References and sources

1. Some figures are attributed from Vecteezy,
   URL: https://www.vecteezy.com/ - thanks !
2. DeepL Translator for proofreading.
   URL: https://www.deepl.com/translator
3. NIST, "Intrusion detection", Computer Security Resource Centre, 2024
   URL: https://csrc.nist.gov/glossary/term/intrusion_detection
4. NIST, "Guide Industrial Control Systems (ICS) Security", 2023
   URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
5. IETF, Internet Security Glossary, 2007
   URL: https://datatracker.ietf.org/doc/html/rfc4949
6. ENISA, "Appropriate security measures for smart grids.
   Guidelines to assess the sophistication of security measures implementation", 2012
   URL: https://www.enisa.europa.eu/publications/appropriate-security-measures-for-smart-grids
7. C. Davis, "Snorpy", 2024.
   URL: http://snorpy.cyb3rs3c.net
8. Buchanan, William J (2024). Snort Analyser. Asecuritysite.com.
   URL: https://asecuritysite.com/forensics/snort
9. Buchanan, William J (2024). Snort Analyser. Asecuritysite.com. https://asecuritysite.com/forensics/snort
   URL:https://asecuritysite.com/forensics/snort?fname=bit.pcap&rulesname=bit.rules

References and sources

10. Seguridad en Sistemas Informáticos Detección de intrusión
URL: https://www.tlm.unavarra.es/pluginfile.php/11611/mod_resource/content/0/clases/08_SSI-monitorizacion1.pdf
11. NIST, NIST 800-61r2, Computer Security Incident Handling Guide, 2012,
https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf
12. Ali A. Ghorbani, Wei Lu, Mahbod Tavallaee, Network Intrusion Detection and Prevention, Springer, ISBN 978-0-387-88770-8, 2010

Connect with CyberSecPro:
How to register and other practical information

1. Website: www.cybersecpro-project.eu
2. X (Twitter): https://twitter.com/CyberSecPro_eu
3. LinkedIn: https://www.linkedin.com/company/cybersecpro-euproject/

Thank you

If you have any questions, please do not hesitate to contact:

- Cristina Alcaraz
  Associate Professor
  University of Malaga
  alcaraz@uma.es