Gergő GYEBNÁR

Black Cell Magyarország Kft.

Black Cell Magyarország Kft.

-

Tactics, Techniques, and Procedures of Attacks in Control Systems

During the presentation, the MITRE ATT&CK framework will be introduced in both its ICS (Industrial Control Systems) and Enterprise domains. By utilizing this framework, I aim to showcase how sector-specific attack heatmaps can be developed, aiding in identifying cybersecurity development areas in a prioritized manner. The topic covers various aspects of threat intelligence in a pragmatic and easily adoptable format.

Following the identification of cybersecurity incidents affecting the given sector, the technical interpretation of the attacks ensues, facilitated by the aforementioned framework. Each campaign, adversary group, or specific malware is mapped to a separate layer using a fundamental mathematical model. After consolidating these layers, the result is the attack heatmap, which we delve further into in the second part of the presentation.

Detection of the most exploited attacks and attack procedures is the primary focus, with numerous solutions being presented explicitly tailored to control systems. These solutions and workarounds create the visibility required for ensuring the security of cyber-physical systems.

The final part of the presentation emphasizes testing and the power of community collaboration. I would like to conclude by showcasing our opportunities through a platform adopted even by NATO.

The key takeaway throughout the presentation revolves around the utilization of industrial Cyber Threat Intelligence (CTI).