CYBELLUM

# Mapping WP.29 CSMS Requirements to the ISO/SAE 21434 Standard and Cybellum

| UNECE – WP.29 CSMS Requirements | ISO/SAE-21434 Processes Requirements | Cybellum Product Security Solution |
|---|---|---|
| (A) The processes used within the manufacturer's organization to manage<br>cybersecurit | Chapters 5 and 6 define the process required for managing cybersecurity in the manufacturer's organization. For example:<br>- 5.4.1 Cybersecurity Governance<br>- 5.4.2 Cybersecurity Culture<br>- 6.4.2 Cybersecurity Plan<br>- 6.4.7 Cybersecurity Case | As part of each of the activities a Vulnerability Management system should be discussed and in place, including the relevant roles in the organization, risk communication channels, playbooks and plans for risk treatment and implementation |
| (B) The processes used for the identification of risks to vehicle types; and<br>(C) the processes used for the assessment, categorization and treatment of the risks identified; | Chapter 8 defines the Risk Assessment methods, including:<br>- 8.3 Asset Identification<br>- 8.4 Threat Scenario Identification<br>- 8.5 Impact Rating<br>- 8.6 Attack Path Analysis<br>- 8.7 Attack Feasibility<br>- 8.8 Risk Determination<br>- 8.9 Risk Treatment Decision | -TARA can be stored in the Cybellum system as part of the Cyber Digital Twin asset.<br>- Correlation and updating the TARA scenarios can be done in Cybellum platform to achieve traceability throughout the life-cycle |
| (D) The processes in place to verify that the risks identified are appropriately managed; and<br>(E) the processes used for testing the security of the system throughout its | Chapter 10 in ISO/SAE-21434 suggests various verification activities to be performed to confirm the implementation of the cybersecurity design:<br>- 10.4.2. Integration and validation | - Cybellum Product Security Assessment automates the security requirements validation and helps in gap analysis and resolutions<br>- Secure coding standards such as MISRA C and others are also automatically tested and checked as |

| | | |
|---|---|---|
| development and production phases; | - 10.4.3. Specific Requirements for Software Development | part of Cybellum Product Security Assessment |
| (F) The processes used for ensuring that the risk assessment is kept current; | | Central Cybellum Cyber Digital Twin platform stores all assets and organization policies to constantly reassess the risk and match it with new information |
| (G) The processes used to monitor, detect and respond to cyber-attacks on vehicle types; | Chapter 7 defines the need for continuous cybersecurity activities, such as:<br>- 7.3 Cybersecurity Monitoring<br>- 7.4 Cybersecurity Event Assessment | Cybellum Product Operations constantly tracks new vulnerabilities, threats, exploits, etc. and monitors your assets to trigger the relevant events in case they are affected.<br>(without being installed on the vehicle, from the back-end only) |
| (H) The processes used to identify new and evolving cyber threats and vulnerabilities to vehicle types; | Chapter 7 defines the need for continuous cybersecurity activities, such as:<br>- 7.5 Vulnerability Analysis<br>- 7.6 Vulnerability Management | Cybellum includes a full Vulnerability Management System, to perform all vulnerability related activities from data collection, to triaging, event triggering and remediation.<br>All activities are documented and ready to be exported for auditing and reporting |
| (I) The processes used to appropriately react to new and evolving cyber threats and vulnerabilities | Chapter 13 defines the operations and maintenance processes, such as:<br>- 13.3 Cybersecurity incident response | Cybellum Product Security Operations performs an on-going analysis of new events. Once a relevant event is detected, a playbook of actions can be automatically triggered to respond to the event |

Done reading? Schedule a free consultation with one of our experts.