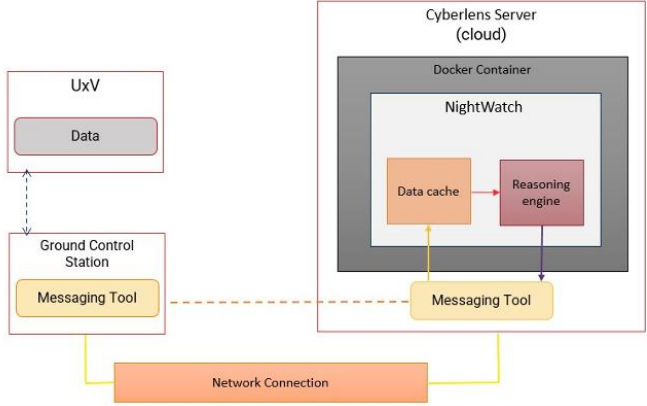


Nightwatch by CLS

<p>Picture</p>	
<p>Brief Description</p>	<p>A cyber-physical threat detection tool that enables the detection and classification of cyber-physical attacks targeting RESPOND-A's UAVs.</p>
<p>Main Functionality</p>	<p>Nightwatch is capable of detecting several types of cyber-physical threat attacks against autonomous systems (including UxVs, namely UAVs, UGVs, UUVs, etc.).</p> <p>CP_ATK1: Jamming Telemetry</p> <ul style="list-style-type: none"> • Communication lost between the UxV and the GCS <p>CP_ATK2: Jamming GPS</p> <ul style="list-style-type: none"> • Communication lost between the UxV and the satellites causing the immobilisation of the UxV. <p>CP_ATK3: Spoofing GPS</p> <ul style="list-style-type: none"> • All communications are alive but malicious GPS values injected cause the deviation of the UxV.
<p>Main Capabilities</p>	<p>Nightwatch is a fully owned, self-contained, and self-operated tool.</p> <p>It is highly extensible, cost efficient by design, and highly tailored to the drone industry.</p> <p>It comes with two modes of operation: cloud-based and host-based offering offloaded detection or onboard self-detection capabilities respectively to the monitored autonomous system.</p> <p>It generates threat alerts and analyst-friendly security logs.</p>

