24 Tr Truman by 24 Sp Securepassage

Security ‘System of Systems’

Truman Brings It All Together

Cyber + Physical

Challenges in security present themselves daily, particularly considering that most organizations have a physical security operation as well as a cybersecurity team. While these functional security areas have grown into their respective and distinct roles, the simple fact that most all security ‘controls’ today are digital, the time is right for organizations to embrace a ‘cyber + physical system of systems’ to achieve greater visibility into security incidents and events.

Why a System of Systems? Each security control, whether software or hardware, comes with a platform, a user interface or other mechanism to operate and observe the control. Whether cameras, badge systems, or an endpoint tool, each control added is yet another control to be observed. Add together just a handful of controls, and the operator’s ability to keep up with incidents and events is quickly lost. By bringing in alert data from all security controls into the System of Systems, anomalies are prioritized by risk level and served up to security team members for action.

Introducing ‘Truman’ by Secure Passage

- Secure Passage knows no two security operations are alike, so Truman (System of Systems) is customizable to fit the unique requirements of your organization.
- Managing alerts is easy with Truman—and fast. We prioritize alert data and move it quickly from the control to the system where it’s highlighted for a security operator to act on, usually in mere seconds.
- Truman features an excellent analytics dashboard for overall visibility of incidents and events without having to visit/observe the control-native platform.
- A customizable rules engine and security orchestration and remediation is at the heart of Truman workflows, so you get the most out of your team and the System of Systems.
- Mobile companion for quick inspection of security on-the-fly will be available soon.

Case Management Friendly

□ Review and validate incoming concerns and incident reports.
□ Open a case.
□ Enter information on the asset and case relevant for people, places and things.
□ Eliminate information silos with team member and role designation.
□ Assign member tasks using preset templates or create custom tasks.
□ Upload files and integrate third-party control data for case management.
□ Evaluate the threat using commonly accepted assessment framework.
□ Determine response and intervention, if any.
□ Implement the chosen response.
□ Submit the case for review, and make further amendments, if necessary.
□ Close the case.
□ Analyze case records and submit reports to key stakeholders.