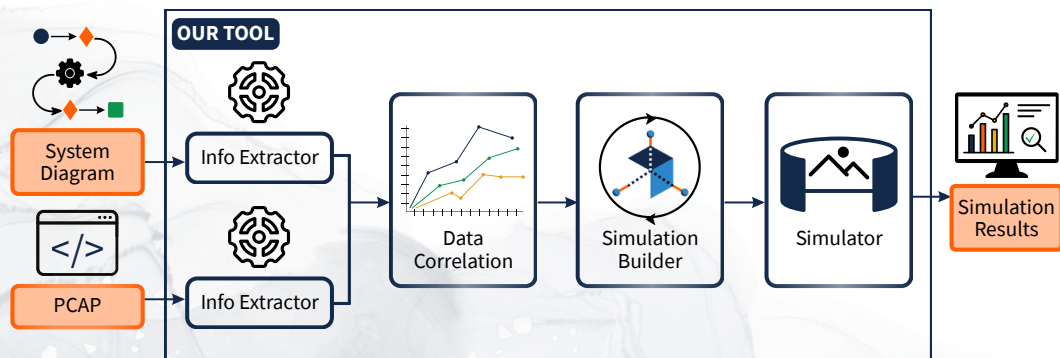


THRUST 4: EVALUATION

SECURITY MONITORING PLATFORM

Smart communities consist of heterogeneous devices networked together in a system-of-systems manner, which creates a complex operational environment. While introducing security technologies to a system is critical, doing so can result in performance degradation and increased attack surfaces. Analyzing the introduction of technologies using existing digital twins or testbed deployments can be risky, costly, and unscalable. This creates an essential need to design a framework that is capable of automated system artifact ingestion to generate a model that can then be simulated with existing network data. This framework facilitates scalable assessments of system performance that:

- Enables stakeholders to easily create a system model with little effort.
- Models the system with the integration of varied information sources across multi-resolution levels.
- Analyzes and evaluates the performance of large systems under different what-if scenarios.



After successful verification, the framework automatically generates a machine-readable simulator model. The primary model artifact describes the network system model and is the primary data source for subsequent simulations.

Network packets and parameterized background flows are then layered over each other using a discrete event simulation framework. The resulting simulator represents a stress-testing environment that determines the boundaries of system performance in relation to the deployment of security solutions within the system. The framework provides a basis for optimizing operational stability and security, thereby enabling stakeholders to evaluate the impact of making changes to their systems.