

Functional Exercises with the Crucible Framework

FUNCTIONAL EXERCISES ASSESS an organization's emergency preparedness by presenting participants with interactive scenarios that evaluate the response actions of key team members. An effective tool for assessing multi-agency coordination, functional exercises target policy, role, and responsibility coordination, integration, and interaction during simulated incidents. The planning process can be grueling when planners from multiple agencies rely on email and spreadsheets without change control to build a Master Scenario Event List (MSEL) and the associated inject data.

In addition to these challenges with the planning process, functional exercises often lack real-time adaptability. Functional exercises conducted without a dedicated simulation platform can also lack realism in inject presentation while the use of real-world communication channels can cause confusion. The Crucible Framework can address these drawbacks by providing a more flexible and cost-effective way to conduct exercises, ensuring efficient preparedness improvement.



Innovative Solution: Crucible Simulation Framework

The Crucible Framework provides dynamic virtual environments that boost exercise

simulation scalability and interoperability. With its open-source foundation and modular APIs, the Crucible Framework offers an immersive browser-based solution that can tailor each exercise to ensure success. Key Crucible applications for functional exercises include:

- **Player:** A centralized interface where participants interact with the exercise components
- **Blueprint:** An exercise planning tool where exercise planners collaboratively plan, develop, and deploy MSELs

- **CITE:** The Collaborative Incident Threat Evaluator, where participants can assess, score, and share insights on incident severity and their organization's roles and actions
- **Gallery:** A repository of exercise data where participants can analyze, collaborate, and share incident details with other participants
- **Open-Source Integrations:** Open discussions in chat, email, and video teleconferencing apps that foster real-time interaction within and across teams

Blueprint: Collaborative Exercise Planning

Blueprint empowers exercise planners by allowing centralized management of exercise and MSEL development. With team-based permissions and event lifecycle controls, Blueprint enables real-time collaboration of MSEL event creation, fine-tuning, and approval processes, eliminating confusion inherent to the use of spreadsheets edited by multiple people in tandem. The current version of the MSEL is immediately visible to allowed users. Storing MSELs and simulated organizations as templates in the system also enables scenario reuse for additional exercises, easing planning challenges down the road.

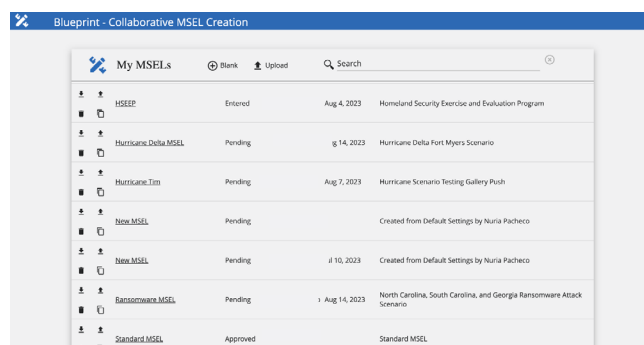


Figure 1: Blueprint Home Screen

Gallery: Interact with Exercise Data

Gallery serves as the comprehensive repository for exercise data crucial for participant response to the simulated event. This data can be a variety of types, such as simulated intelligence, reporting, orders, news articles, social media posts, telephone calls, and emails.

This sophisticated application empowers exercise planners to meticulously configure designated cards that group and display exercise data in categories on a virtual wall. This wall allows participants to effectively visualize the severity of the incident as it pertains to these categories, such as critical infrastructure sectors or key cyber terrains. The information provided in Blueprint equips participants with the knowledge required to navigate scenario evaluations.

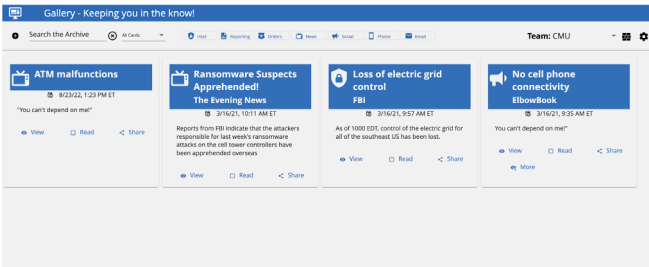


Figure 2: Gallery Dashboard

Collaborative Incident Threat Evaluator: Assess Incident Severity

Exercise participants can use CITE to record their analysis of the severity of simulated scenarios. With customizable scoring models, planners can use the National Cyber Incident Scoring System (NCISS) or add their own severity matrix to the platform. CITE also provides a situational awareness dashboard where participants can define actions and work roles that match their team's response plan, ensuring clarity and alignment of their resources.

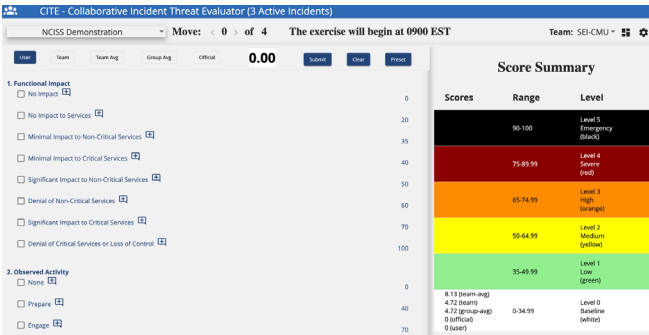


Figure 3: CITE Scoresheet

Third-Party Applications

Incorporating third-party applications into the Crucible Framework enhances collaboration and the efficiency of virtual exercises. It's essential to introduce applications that facilitate smooth information exchange throughout the exercise. With the integration of open-source tools for webmail, chat, and video teleconferencing, participants can replicate real-world communication scenarios, effortlessly sharing vital information.

Enabling Assessment

Post exercise reporting relies on quality data collected during the exercise's execution. When participants conduct the exercise remotely using real-world communications that cannot be monitored by the exercise controllers, the inability to observe the participants creates a barrier to effective assessment. When using the Crucible Framework for functional exercises, assessment opportunities exist through two primary means: observation and instrumentation. Both CITE and Gallery allow exercise controllers to observe a team's data in real time, helping them to assess whether each team is receiving information from and sharing information to other teams. These applications also use the Experience API (xAPI) to provide instrumentation for learning engineering. This instrumentation allows post-exercise reports to be generated that track when and how injects were received and shared by teams, thereby evaluating each team's response actions, and validating that exercise objectives were achieved.

Empower Your Organization

Unlike traditional exercises that require significant resources and costs, virtual exercises utilizing the Crucible Simulation Framework offer a more flexible and adaptable approach. Leave restrictions behind and embrace a dynamic, practical method that empowers participants and planners. Incorporate functional exercises and the Crucible Framework to revolutionize your emergency response preparedness. Experience dynamic virtual environments for enhanced scalability, collaboration, and real-world relevance. This integrated solution empowers your organization, streamlines communication, and navigates complexities seamlessly.

About the CERT Division

The CERT® Division of Carnegie Mellon University's Software Engineering Institute conducts valued, relevant, and trusted evidence-based research that fortifies the cyber ecosystem and protects national security and prosperity.

Contact Us

CARNEGIE MELLON UNIVERSITY
SOFTWARE ENGINEERING INSTITUTE
4500 FIFTH AVENUE; PITTSBURGH, PA 15213-2612
sei.cmu.edu
412.268.5800 | 888.201.4479
info@sei.cmu.edu