Overview

IMPORTANT: It is strongly recommended that you complete the following checklists to ensure that you are prepared to be effective in the upcoming event. These activities are critical to your success during the event and all players need to be proficient in these tasks PRIOR to the event. Not all tasks may be relevant to your role or job function.

Please complete this checklist prior to the end of the Portal Familiarization Period.
If you have any questions, please contact the support team at support@simspace.com.

Account Access and Range Familiarization

❏ Verify you can log into the SimSpace Portal and access the appropriate Live Action Event
❏ Review how to access and interact with the helpdesk (for range and account issues)
❏ Review how to access and interact with your event, VM consoles, defender logs, and Mattermost chat:
    ❏ What goes in chat vs the defender logs?
    ❏ How will your team manage console access to operator designated VMs?
❏ Verify and review the file management capability, capacity, and use
❏ Review all documents uploaded to the *Event Documents* section of your event's lobby.
Pay particular attention to the rules of engagement (ROE)

In-Range Preparation

❏ Review the network diagram
❏ Confirm the expected defender team toolset is present
❏ Confirm the ability to log into specific tools
❏ Adjust, configure, create operator-specific tool accounts as needed. Document all changes.

If you experience account access or login/password issues, contact your team lead for resolution at least the day prior to the event and/or support@simspace.com.

Defender Team Reconnaissance Plan

After completing the above, begin assessing and building knowledge of your network. The following are a few suggestions to get you started, but you are free to develop your own internal list. Running through these pre-event practical tasks will build familiarity and help the team identify any issues interacting with the range. These tasks can be accomplished prior to event execution and will provide the team with a firm foundation for operations. This list is not exhaustive, and the team can add any passive tasks that do not violate ROE or change the configuration of the range itself.

- ❏ Conduct tool checks (i.e., proper configuration, dashboards, logging, etc.)
- ❏ Examine configuration of passive network monitoring tools, including:
    - ❏ Rulesets
    - ❏ Tap placement
    - ❏ Ability to access PCAP, NetFlow, and log data
- ❏ Conduct initial network scans:
    - ❏ Confirm hosts and topology
    - ❏ Discover network services
    - ❏ Discover vulnerabilities (**NOTE**: The range is set to a recent, but not real-time-current patch level. Patches that you recommend for remediation will not be exploited, though they may not be applied.)
- ❏ Conduct initial tool validation:
    - ❏ Enumerate all sources of log and security data
    - ❏ Determine how security data is aggregated and processed:
        - ❏ Will operators work at the point-of-collection or off aggregated data?
        - ❏ Do all operators have access they need to aggregated data?
        - ❏ How will operators share and collaborate?
- ❏ Conduct a policy audit:
    - ❏ Examine existing security policies to understand current network state and recommend changes:
        - ❏ Domain group policies
        - ❏ Host intrusion prevention system policies

NOTE: Within the range, these policies will initially focus on *detection* rather than *prevention,* to facilitate successful simulation of various forms of attack so that teams can confirm their ability to detect. Refer to the ROE documentation for an out-of-bounds list and other relevant information.

- ❏ Enumerate services and hosts:
    - ❏ Examine running services in terms of the event scenario
    - ❏ Baseline network traffic
    - ❏ Baseline installed software and configurations
    - ❏ Examine user permissions and group memberships
- ❏ Understand network map and critical assets and services relationship
    - ❏ Understand dataflow based on business requirements
- ❏ **Hunt for the active beacon in the range**