CoAction

Tabletop Exercises (TTX)

Continuously Improve your organization's Cybersecurity resiliency

Tabletop Exercises (TTX)

By augmenting traditional Tabletop Exercises with CoAction's live-fire range, technical teams gain invaluable experience working through a cyber compromise in realistic conditions.

This includes adapting to higher operational tempos, making course of action decisions under attack, while also facing communications challenges during a cyber fight.

Through the TTX-Enhanced range, your unified command can gain an advanced level of insight into the exercises - empowering decisive decisions.

TTX Enhanced Runbook:

- Observe operational choreography
- Examine tactical response skill sets
- Improve tactical response skill sets
- Unify intention to contain, eradicate, and recover
- Rehearse common real-world threat scenarios
- Maintain tactical response muscle memory
- Strengthen overall cyber readiness posture
- Examine and Improve tactical response skill sets
- Unify Identification, containment, eradication and recovery

CoActionTech.com
Sales@CoActionTech.com

CoAction

Re-Wire For Speed and Embed Long-Term DNA

CoAction

Many organizations witness organizational dysfunction during a cyber attack. The tactical aspects of response may be top shelf, but any concept of execution under fire is nonexistent, and the collective reaction of the enterprise is in disarray. Activities performed during a TTX, led by CoAction Incident response teams, help transform dysfunction into functional containment, eradication, and recovery.

CoAction Tabletop Excercise (TTX) helps answer questions like:

- Who responds in the event of an attack?
- Which responders are trained and qualified to handle the attack?
- Which courses of action (COA) will contain the enemy's advance?
- Who defines and prioritizes, communicates, and executes the COA?
- How do we prevent broader asset compromise?
- How do we communicate information to the C-Level during the response?
- How do we communicate information to employees during the response?
- Which external organizations must be involved in neutralizing the threat?
- Which external organizations will be involved after the threat is put down?
- How, when, and what information is provided to the C-Level, legal, employees and 3rd party parties?
- When do you get Law enforcement involved?
- Which External organizations need to be notified after the threat is mitigated?

The answer to the above questions are essential when readying your cybersecurity posture but the risk of a cybersecurity attack is never eliminated. It's what you do when it happens that matters most.

CoAction

CoActionTech.com
Sales@CoActionTech.com