Tabletop 2.0

CLOUD RANGE

Cloud Range Tabletop 2.0™

NEXT GENERATION TABLETOP EXERCISES

Cloud Range has taken traditional tabletop exercises to a new level in order to provide customers with a holistic, comprehensive, and cross-disciplinary approach to detection, response, and remediation.

SO, WHAT HAPPENED BEFORE THE BREACH?

THE TRADITIONAL TABLETOP EXERCISE

- Assumes a breach has already happened
- Theoretical
- Decision-making
- Soft-skills focused
- Static scenarios

TAKING IT TO THE NEXT LEVEL WITH TABLETOP 2.0

- Experience what happens as early as when the threat is detected
- The addition of a live cyber range creates a comprehensive approach
- Analysts practice following their own playbook on a live attack
- Practice the entire playbook, from detection through remediation
- Integrate processes for analysts, technical staff, and executive leadership

SEE THE WHOLE PICTURE.

CLOUD RANGE TABLETOP 2.0

CYBER RANGE EXERCISE/TECHNICAL SIMULATION

COORDINATED COMMUNICATION

TRADITIONAL TABLETOP

DETECT / INVESTIGATE

✕

THREAT DETECTED

RESPOND / REMEDIATE

- Executive leadership
- Legal
- Communications

CLOUD RANGE

Cloud Range Tabletop 2.0™

SUCCESS STORY

A GLOBAL BANK'S STRATEGY

One of the 10 largest banks in the world sought out Cloud Range to simulate the entire attack process for their global cybersecurity teams. The organization had been conducting traditional tabletop exercises, but they knew there was an inherent limitation in what they were doing because they were missing the component of the cyber attack actually transpiring. In addition, they needed a way for the SOC analysts to be able to experience a live attack transpiring in a contained, safe, custom environment.

> *By 2022, 15% of large enterprises will be using cyber ranges to develop the skills of their security teams, up from less than 1% today.*
>
> GARTNER, INC.

THE SOLUTION IN DETAIL: A HOLISTIC APPROACH

To fill the gap in their cyber training strategy, the bank implemented Cloud Range's cyber range simulation exercises in a continuum paired with a more traditional tabletop exercise. This allowed for all participants to experience a holistic, dynamic, experience of what would happen in an actual cyber attack from detection to response to remediation.

PART 1- TECHNICAL SIMULATION
on the Cloud Range cyber range:

- **24 participants** logged onto the **Cloud Range virtual cyber range platform**
- Live **SQL Injection cyber attack** simulation occurs
- Participants **practice** the following steps:
  - Threat detection
  - Analysis
  - Technical response
  - Remediation

- **Debrief session** after the attack that ensures participants understood all aspects of the attack:
  - Attack flow
  - Decision-making
  - Review of non-technical steps in the playbook involving communication with leadership and non-technical stakeholders

PART 2- NON-TECHNICAL SIMULATION
(traditional tabletop exercise conducted by IR firm):

- **Technical response** happening in background
- Communication of technical findings to the **executive track** and **non-technical stakeholders,** including:
  - Executive leadership
  - Legal
  - Communications

- **Cohesive approach** of technical and non-technical stakeholders, accounting for the entire timeline of the attack, role definitions, playbook alignment, and decision process

FUTURE MONTHLY EXERCISES

The global bank will continue to conduct 12 technical simulations throughout the year, where each one will be a different type of attack, giving security analysts the ability to hone their skills on an unlimited number of threat types. A comprehensive cyber attack simulation involving both technical and non-technical participants will be conducted in person twice per year.

GLOBAL STRATEGY

A comprehensive approach to incident response has become a global strategy for the company in order to test all processes and playbooks, upskill and retain staff, which ultimately reduces risk.

Contact us for more information at info@cloudrangecyber.com