TechData

CYBER RANGE

Zero Trust Experience

Objective:

Zero Trust is a security concept centered on the belief that organizations should not automatically trust anything inside or outside its network perimeter. It is crucial that any business – big or small – verify anything and everything trying to connect to its networks/systems before granting access.

Participants will become skilled on the core principles of Zero Trust, be able to evaluate and plan for implementing or converting to a Zero Trust framework and most importantly, be able to monitor and deliver analytics of network/system disturbances.

Participant Experience:

Through this invaluable exercise, participants will not only learn to recognize potential intrusion risks but adapt the philosophy behind a Zero Trust network which assumes that there are attackers both within and outside of the network, so no users or machines should be automatically trusted. Additionally, Zero Trust methodologies limit the risk to any one system/network during intrusions. Each participant will come away with an understanding of:

- The principle steps necessary to protect applications, systems and controls
- The importance of privileges in extending access for users, systems, and applications
- How to define and implement governance and policies for your Zero Trust framework
- Design and implement monitors to sustain your Zero Trust

Participant Roles:

- Executive / top management groups (C-level)
- Strategic management groups (mid-management)
- Technical groups

Exercise Outcomes:

- Ability to implement Zero Trust methodology
- Understand whether a Zero Trust strategy is a good fit for business objectives
- Build awareness and base knowledge of different vendors that support a Zero Trust framework

Schedule your Zero Trust Experience today!

Call (800) 237-8931 x 5540508 or email us at **securityservices@techdata.com** for pricing and availability.