Partner Use Case

IBM

Principle 1 "Ownership for cyber and IT security"

Starting point

As cybersecurity has become a growing topic among companies, IBM acknowledged that most organizations use to place emphasis on having their technical IR/IT teams go through tabletop exercises to prepare them to respond at the tactical level. However, in accordance with Principle 1, which notably aims at "anchoring responsibility for cybersecurity at the highest governmental and business levels", IBM noticed that few companies have their Executive Leadership Teams (C-Suite) go through an exercise that focuses on the whole-of-business response to enterprise-wide cyber-attacks (ransomware, destructive, etc.) that threaten the operations, brand, reputation, and data of an organization. This observation led the company to establish the IBM Security Command Center.

Objectives

The IBM Security Command Center aims to ramp up cybersecurity capacities both in the private and public sectors globally, at the highest level – C-Suite, HR, Legal and Communications. More specifically, the main objective is to upgrade skills to better face cyber incidents and provide a swift, agile, and confident response to incidents.

Description

More concretely, the IBM Security Command Center consists of immersive simulations, exercises, and workshops:

- The Business Response Challenge enables participants to test a complete business response to a cyber incident, identify gaps in incident response teams and plans, and shows how quick, practiced decisions can help mitigate risk and cost.
- The Cyber Wargame enhances technical skills and the integration of SIEM and incident response platforms. Participants can practice how technical and business teams should work together during an incident.
- In the Mind of a Hacker webinar, participants learn to understand WiFi attacks, malicious USBs, phishing, and Open Source Intelligence.

Lessons learned/results

More than 13,000 IBM customers have trained at IBM's Security Command Centres globally to be proactive responders. In has become clear that training in an authentic, but controlled, virtual environment – with experiences that authentically simulate a cyber incident – can help security teams learn to deal with the pressure of crisis situations. IBM has been leveraging the lessons learned to identify industry best practices in developing fool-proof incident responses and a proactive cyber leadership.