CYBER INCIDENT SIMULATIONS

GO

GAMIFIED
Simulations are interactive, engaging and imitate the unpredictability of an actual incident.

STEP 1

PLAN THE SIMULATION
We plan the simulation exercise in conjunction with your Cyber Security Management and Operations teams.

CUSTOMISED
Penetration testers design each scenario to ensure they are realistic to current attack types.

STEP 2

DEVELOP SCENARIO
Incident scenarios that are realistic, relevant and based on your organisation's unique threats and critical asset targets.

INCREASE AWARENESS
Simulations are effective in creating awareness of the response process and potential threats.

EVALUATE RESPONSE READINESS
Gauge how well prepared your procedures and security technologies are to respond and recover to an incident.

IMPROVE COLLABORATION
Key stakeholders work together to manage the incident across various business functions.

IDENTIFY GAPS
Exercises help you to assess your response and recovery processes, skill levels, roles/ responsibilities and security technologies.

STEP 4

POST-SIMULATION FEEDBACK
We deliver a report and presentation on how prepared you are, together with practical improvement recommendations.

STEP 3

RUN THE SIMULATION
Run simulations once, on an ongoing basis, or with different scenarios applicable to various business functions.

FACILITATED
Simulations are run by experienced consultants with skills across both the response management and technical levels.

VIRTUALISED
Key stakeholders can participate from wherever they are.

MOBIUS CONSULTING
Actualising change

Mobius provides Cyber Incident Simulations which enable organisations to run virtual, fun, interactive and realistic gamified exercises designed to help improve incident response readiness and Cyber Security capabilities.

Mauritius Office: +230 5297 0903 | Email: info@mobiusconsulting.mu | Website: mobiusconsulting.mu