INCIDENT **RESPONSE SIMULATION SERVICES**

MOBIUS CONSULTING

Actualising change

Organisations are increasingly required to conduct incident simulations on an ongoing basis in order to test incident response readiness and comply with regulatory requirements.

Incident simulations should be planned and run across the organisation and include both Business Management and IT. Additionally, stakeholders across the company should have the necessary awareness and training of the incident response process in order to be better prepared to respond effectively to an incident.

However, most organisations face resourcing constraints related to the time and people needed to plan and run the simulations. Mobius is perfectly positioned to help your organisation conduct ongoing simulations and provide recommendations to enable you to constantly improve your incident response capabilities.

WHY MOBIUS?

Mobius provides various types of Incident Simulation Services at both a business and technical level, which includes tabletop simulations and real-world simulations. Our attack based simulations are technical in nature and are run in collaboration with our penetration testing team. We conduct incident simulations that are applicable to your organisation and customised to your specific requirements.

Our service includes training and awareness sessions to all stakeholders so that they are better prepared, and can contribute more meaningfully during the incident simulation. Our ongoing simulations consider and review previously identified shortcomings in order to continuously improve the organisation's readiness.

BENEFITS

- Customised training and awareness
- Tabletop and attack based simulations
- Improved organisational-wide incident response readiness
- Increased confidence and resilience

APPROACH TO **INCIDENT RESPONSE SIMULATIONS**

MOBIUS CONSULTING
Actualising change

The diagram below details our approach to incident simulations as well as the activities and outcomes included in the service:

PHASE 1
PLANNING AND PREPARATION

- Review existing processes, documentation, and any previous incident simulation shortcomings.
- Develop detailed incident scenario/s applicable to the organisation.
- Develop simulation documentation required for the simulation exercises.
- Conduct technical preparation for technical simulation attacks.

OUTCOME
A plan to test incident response capabilities using incident simulation scenario/s.

PHASE 2
TRAINING AND AWARENESS

- Develop content for the training session.
- Provide training and awareness sessions prior to the actual simulation.
- Facilitate awareness session.

OUTCOME
Familiarise stakeholders with your incident response process to be better prepared for the actual simulation.

PHASE 3
FACILITATED INCIDENT SIMULATION

- Facilitate the simulation exercise.
- Perform incident simulation attack scenarios using appropriate tools and techniques (for technical incident simulations).
- Observe the simulation exercise to identify shortcomings.

OUTCOME
Completed incident simulation exercise together with a report on organisational readiness and recommended improvements.

PHASE 4
POST-SIMULATION ANALYSIS, FEEDBACK, AND REPORTING

- Perform post-simulation analysis.
- Identify improvement areas and other recommendations.
- Report and feedback on incident simulation successes, shortcomings, improvement areas, and recommendations.

OUTCOME
Feedback of the incident simulation with recommendations for improvements.

DID YOU KNOW?
Mobius offers a range of Incident Simulation Services, including business-level tabletop simulations, Cyber Security Incident Response Team (CSIRT) simulations, and technical adversarial simulations utilising our expert penetration testing team.

MOBIUS
CONSULTING

CONTACT US

South Africa
info@mobiusconsulting.co.za
www.mobiusconsulting.co.za

Mauritius
info@mobiusconsulting.mu
www.mobiusconsulting.mu

United Kingdom
info@mobiusconsulting.co.uk
www.mobiusconsulting.co.uk