Singtel Business

Product Brochure
Cyber Range

Gear Up for Cyber Combat: Be Prepared For the Real Thing.

The cyber threat avalanche does not wait. Every business is a prime target and no one is spared. It is no longer about whether it will happen, but when it will happen or worse – if it has already happened without your knowledge.

A Cyber Range offers a real-world environment for the realistic simulation of possible cyber-attack scenarios, bringing you inside a cyber attacker's mind. It elevates cyber security as a top-of-mind focus to deepen C-Suite and Board awareness on cyber risk, crisis management and communication. It also heightens your enterprise-wide security resilience by testing, checking or verifying on your cyber readiness.

Singtel

Cyber Range

Race Against Time: Critical Importance of Effective Incident Response

In today's climate, a security breach is inevitable. Attacks can come in many forms and from different entry points into one's Information Technology (IT) or Operation Technology (OT) systems, including: online threats, data breaches, e-crime/malware, social media/scams, mobile applications and more. It is time businesses know, and not guess, if they are operationally ready to tackle today's highly sophisticated and fast-mutating cyber-attacks.

There are many reasons for ineffective security incident responses, such as:

- Incident response processes are not properly documented or tested for effectiveness
- Crisis management and communication strategies are untested
- Existing security solutions are not adequate for detecting or blocking malicious traffic optimally
- Weakened security operational effectiveness when there are too many false positives, manual processes or lack of security analytical skills.

Spotlight: Incident Response

Recent survey by the Ponemon Institute of IT and IT security professionals revealed:

68% reported that their organisation experienced a security breach or incident in the past 24 months[1].

57% expected to experience a security breach within the next year[2].

81% said right investments in people, process and technologies would help their organisations better mitigate future security breaches[3].

Building a Business Case: Strengthening Your Security Resilience Via a Cyber Range

No one should go into a battlefield unprepared. Before advancing into the cyber 'warzone', operations teams, corporate function heads and even C-Suite and the Board need to arm themselves with better knowledge on: who the enemies are and their tactics; how to defend the business against them; and what to do during a security incident.

Built to strengthen one's overall cyber readiness, a Cyber Range helps businesses to better respond to security incidents. By simulating drills, businesses can test the effectiveness of existing processes (eg. security/network operations, incident management) and train its people's readiness for real-world threats. It offers a:

- Platform for cyber warfare training in attack and defence techniques/tactics
- Simulated environment to equip cyber warriors with more effective cross-functional communication skills during a security incident

Overview: Cyber Range

Unlike traditional classroom training which focuses on theoretical understanding, Singtel Cyber Range offers a real-world, hands-on environment for realistic, vertical-focused cyber-attack scenarios. Our next-generation, technology-agnostic platform empowers businesses to learn about potential threat scenarios, how to respond to them, and how to test and ensure one's incident response effectiveness. We also have the expertise to enhance your infrastructure resiliency, test your critical infrastructure and more.

Features:

- Comprehensive operational platform: End-to-end operational environment with a comprehensive range of security solutions or technologies from both commercial and industry-leading open source partners. Empowers more realistic and experiential learning to detect, protect and respond to cyber threats.
- Realistic traffic simulation: Simulation of legitimate, malicious and manual attack traffic for realistic training and exercise.
- Extensive and updated attack scenarios: Rich library of attack scenarios that are updated regularly based on latest cyber threat intelligence. Includes both single and multi-vector attacks.
- Customer-centric and vertical-focused: Shape different attack scenarios to simulate varied types of cyber-attacks. Can be tailored for industry-specific requirements or customised for a specific organisation's threat landscape.
- Remote global access: Enable access from remote locations to facilitate the simulation of geographically-dispersed business operations.

Addressing Today's Security Challenges

Today's highly-evolved threat landscape calls for higher levels of readiness. Besides equipping with security technologies, the ability of your team (both IT and non-IT) to communicate and work cohesively under pressure during a gruelling security incident is key to your success in identifying, mitigating and responding to cyber threats.

Deepening Executives' Cyber Awareness

We offer an Executive Programme that include Management Cyber Readiness and Board Cyber Oversight workshops to help senior executives, CXOs and the Board deepen their awareness on cyber threats and their impacts.

These will help them:

Understand the challenges of a SOC/NOC analyst and the specialised skillset required to ensure the first-line of cyber surveillance is well taken care of.

Get equipped with critical information needed to ensure an effective organisation-wide cyber resilience programme.

Rethink their security readiness plan through scenario role-play exercises.

Cyber Range Workshops: Gearing You Up with an Effective Organisation-Wide Cyber Resilience Programme

Cyber Range Workshops provide a simulation platform with realistic attack scenarios that are relevant for your team to experience, learn and practice cyber defence/responses together. Addressing enterprise-wide cyber resilience, our comprehensive curriculum engages from the Board, C-Suite right down to your operations team. Top security concerns of business leaders are examined over scenario role-play exercises, crisis management, communication and more. To enhance cyber oversight, insightful sessions to deepen board awareness on the latest cyber security landscape are also available.

	Tactical Cyber Wargame (3 days)	**Management Cyber Readiness** (1 day)	**Board Cyber Oversight** (Half-day)
Objectives	Train IT and operations teams on varied attack and defence techniques, using security controls in a simulated or emulated environment	Train corporate function heads and C-Suite through scenario role-play exercises to: • Examine the company's current cyber response plans and their effectiveness • Make optimal decisions during a cyber breach from a risk-based approach	Equip the Board to: • Understand the possible varieties of cyber threats and their enterprise-wide impact • Make optimal decisions during a cyber breach from a risk-based approach • Devise crisis management and communication strategies
What it covers/ What you will learn	**Day 1 and 2** • Overview of Singtel Cyber Range and setup of the exercise range • Learn about single-attack vectors and how they work • How to differentiate good versus malicious traffic • Determine which security controls to use and how to configure them **Day 3** • Learn about multi-attack vector scenarios and how they work • Debrief on areas for improvement **5 teams are set up for the exercise workshop with each playing different roles:**	• Understand crisis management and communication strategies • Understand the day-to-day challenges of the operations team by playing the role of a SOC/ NOC analyst • Undergo cyber risk management exercise to test how one makes decisions in response to trigger factors simulating a security incident • Experience simulated threat factors with scenario role-plays to examine the effectiveness of incident response and escalation processes during a security incident • Examine crisis management and communication processes involving the handling of media and more to achieve a desirable outcome in protecting your reputation during a cyber breach • Debrief after each session to highlight observations, complete with an executive summary report with pragmatic recommendations on next steps to heighten security readiness.	• Overview of the evolution of the cyber security landscape • Understand the Board's role in cyber risk management via exercise that tests how one makes decisions in response to trigger factors simulating a security incident • Examine crisis management and communication processes involving the handling of media and more to achieve a desirable outcome in protecting your reputation during a cyber breach

Red
Typically played by the ethical hacker to simulate manual attacks on the exercise network.

Green
Typically played by Cyber Range team to simulate legitimate traffic that mimics a typical IT/OT environment.

Blue
Typically played by participants to monitor exercise network for security anomalies and attempt to defend or respond to them.

Yellow
Typically played by participants 'acting' as unaware users who trigger off phishing emails.

White
Typically played by the trainer who will observe Blue Team's response throughout the exercise and provide debrief on how they fair and areas to improve.

Cyber Range Workshops: Gearing You Up With an Effective Organisation-Wide Cyber Resilience Programme (Continued)

	Tactical Cyber Wargame (3 days)	**Management Cyber Readiness** (1 day)	**Board Cyber Oversight** (Half-day)
Who should attend	IT and security staff from Security Operations (SOC), Network Operations (NOC) and Cyber Incident Response Team (CIRT).	C-Suite and Corporate Function Heads.	Board members.

We understand that every business may be at varying levels of security maturity and readiness, that is why we have designed Cyber Range workshops to be customisable to meet your specific requirements.

Cyber Security Matters: The Future Does Not Wait

Being prepared today does not mean being foolproof tomorrow. To establish a reliable cyber defence perimeter around your organisation, security needs to remain 'top-of-mind' to ensure your people are ready to respond during a security incident and your incident response processes are constantly updated to address evolving threats.

Cyber Range Subscription Service: Get Armed for Better Navigation

The Cyber Range Subscription Service helps you review your threat management efforts – so you can stay current on evolving cyber threats that are relevant to your business or industry. The annual subscription programme consists of 3 components:

- Threat modelling and incident management facilitation workshop
- Threat simulation workshop powered by Singtel Cyber Range
- Threat intelligence subscription specific to your business or industry

	Cyber Range Subscription Service: 3 Components
One-Time	Cyber Range Consultants work with you to: • Discover your threat landscape based on business operational risk and threat intelligence • Conduct threat modelling to establish threat scenarios specific to your environment • Understand your current security incident management processes • Design attack scenarios and emulate environment in Singtel Cyber Range • Conduct Cyber Wargame exercise with executive summary report
Half-Yearly	Two sessions of 1-day threat updates specific to your organisation
	Choice of: Option 1: Two sessions of 2-day Cyber Wargame Exercise based on the simulation environment setup. OR Option 2: 1-year threat intelligence subscription specific to your cyber security needs

Cyber-Proofing Your Network Architecture

Besides your people and processes, a holistic approach to cyber threat management also involves cyber-proofing your network architecture. While you may have relied on a paper-based design network architecture in the past, in today's climate – can you be absolutely certain about its effectiveness without testing it? Yet, the dilemma is: it is simply too risky to test on your 'live' production or Critical Information Infrastructure (CII) environment.

To help businesses overcome this predicament, Cyber Range Consulting Services recommend assessing and examining your critical infrastructure in an emulated environment for in-depth, fail-safe testing.

Security Resilience Testing	CII Security Assessment
• Test the security resilience of a simulated production environment using 'live' traffic, without disrupting business operations • Assess and recommend the optimal usage/ placement of security equipment or solutions • Review the extensive functionalities of security solutions to ensure comprehensive proof of concept • Investigate the impact of upcoming rule/ configuration changes or new rules; this is critical to avoid excessive false positives before introducing the changes into the 'live' production environment	• Emulate your critical infrastructure (eg. SCADA) for more intrusive penetration testing that is risky in actual environment • Assess non-IT or OT systems (eg. utility plants) in simulated environments at ease, without having to bring down critical operations or worry about disrupting them

Why Singtel

Technology agnostic platform for cyber wargames and simulation

- Comprehensive commercial and open-source security solutions for detection, protection and response to cyber threats
- Reduce risks and minimise potential business disruption by emulating one's CII or production environment for fail-safe testing
- Assess the impact of planned changes to existing security network architecture
- Gain deeper understanding on effectiveness of security operations and incident response processes through cyber wargames and tests
- Enable hands-on assessment of products/services before making informed investment decisions
- Deliver organisation-wide cyber resilience programme from Board, C-Suite to operations team
- Deepen cyber awareness amongst Board members for better cyber security oversight

Vertical-focused and tailored to your specific needs

- Learn about vertical-specific threats, regulatory requirements, and cyber-attack scenarios via realistic cyber wargames
- Benefit from tailored cyber-attack scenarios to specific organisation's needs
- Gain insights into vertical-specific threats with threat intelligence via cyber range subscription services

Realistic and experiential learning to develop cyber warriors

- Benefit from Singtel's extensive library of updated attack scenarios simulated in a realistic combination of legitimate, malicious and manual attack traffic
- Validate one's incident response effectiveness through realistic and experiential cyber exercises
- Gain experience and advanced skills through experiential responses to simulated real-world cyber world attacks; Develop cyber warriors and sharpen competitive advantage amidst global security talent shortage

Expert cyber range consultancy services to address dynamic cyber challenges

- Stay vigilant with regular updates and exercises on emerging threats via cyber range subscription service
- Address your cyber challenges by understanding cyber threats and their enterprise-wide impact to make informed decisions and investments
- Reduce costs by relying on a trusted supplier

Footnotes:
1. https://www.lancope.com/sites/default/files/Lancope-Ponemon-Report-Cyber-Security-Incident-Response.pdf
2. Ibid.
3. Ibid.

About Singtel

Singtel is Asia's leading communications group providing a portfolio of services including voice and data solutions over fixed, wireless and Internet platforms as well as infocomm technology and pay TV. The Group has presence in Asia, Australia and Africa with over 610 million mobile customers in 24 countries, including Bangladesh, India, Indonesia, the Philippines and Thailand. It also has a vast network of offices throughout Asia Pacific, Europe and the United States.

Awards

Frost & Sullivan Singapore Excellence Awards 2016
Managed Security Service Provider of the Year

Frost & Sullivan's Asia Pacific ICT Awards 2016
Telco Cloud Service Provider of the Year

NetworkWorld Asia Info Mgmt Awards
Security-as-a-Service (2012 - 2016)

NetworkWorld Asia Readers' Choice Awards
Managed Infrastructure Services (2012 - 2015)
Managed Security Services (2014 - 2015)

NetworkWorld Asia Info Mgmt Awards
Disaster Recovery & Business Continuity (2014 - 2016)

Telco Cloud Forum Awards 2016
Telco Cloud of the Year

October 2016

For more information www.singtel.com/security g-cyberrange@singtel.com Contact your Account Manager