Trustwave®
a Singtel company

DATA SHEET

Trustwave Cyber Security Institute

EDUCATE YOUR ORGANIZATION TO PROTECT AGAINST SECURITY THREATS

Security is an enterprise-wide objective that touches all parts of your business. Your organization's defenses against cyber threats are only as strong as your weakest link and for many organizations, deficient security solutions and employees who haven't developed a vigilant culture of security are those weakest links. Trustwave, a leading cybersecurity and managed security services provider, help businesses fight cyber-attacks, protect data, and reduce security risk through a combination of comprehensive cyber security solutions, and a wide range of cyber security training program.

The Cyber Security Institute

Cyber-attacks come in many different forms – online threats, data breaches, e-crime/malware, social media/scams, mobile applications, and more – and from many different entry points into the Information Technology or Operations Technology systems. Consequently, business leaders and their staff must be fully prepared to guard against and tackle highly sophisticated, fast-mutating cyber-attacks.

The Cyber Security Institute was built to aid businesses and provide staff with the tools, training and knowledge necessary to identify, respond to and protect against security threats. At Trustwave we know that a key requirement to stopping security threats is to create an environment where every employee, from Board of Directors, C-Suite, Senior Management, IT Security, IT Operations teams to end-users and non-IT, whose role in security is more of security awareness, is empowered to detect and prevent attacks and has a clear understanding of how to respond to security incidents all while serving your customers in a secure, efficient and compliant manner.

Our goal, using our comprehensive and advanced cyber range of security solutions and up-to-date attack simulators, is to design and implement security protocols, tactical and cross-functional training such as:

TACTICAL		CROSS FUNCTIONAL
Enhancing Cyber Know-How	**Real-World Attack Simulation**	**Crisis Scenarios**
• Cyber Kill Chain®, Attack Vectors, Cyber Defense and Response • Vulnerability Management • Incident Response Management • Business Continuity Management	• Red and Blue Team Exercise • Detect, Investigate/Response, Contain/ Mitigate, Remediate • Test IR Playbook Effectiveness	• Table-Top Exercise • Dealing with Cross-Enterprise or Complex Issues • Risk-based Decision Making • Effective Communication (Internal/External)
Identify Gaps and Test Cyber Response Effectiveness		

State-of-the-Art Cyber Range

A key component of the Cyber Security Institute is the Cyber Range. The Cyber Range offers a realistic simulation platform housing an array of up-to-date cyber-attack and defense tools, which allows us to better prepare and train you and your staff. Unlike traditional trainings which focus on theoretical concepts, we offer a real-world, hands-on environment to immerse in realistic, vertical-focused cyber-attack scenarios, how to respond, and how to test and ensure one's incident response effectiveness.

The Cyber Security Institute also provides expertise to test your critical infrastructure and enhance infrastructure resiliency.

COMPREHENSIVE OPERATIONAL PLATFORM	REALISTIC TRAFFIC SIMULATION	EXTENSIVE AND UPDATED ATTACK SCENARIOS	CUSTOMER-CENTRIC AND VERTICAL-FOCUSED	REMOTE GLOBAL ACCESS
End-to-end operational environment with a comprehensive range of security solutions or technologies from both commercial and industry-leading open source partners.	Simulation of legitimate, malicious and manual attack traffic for realistic training and exercise.	Rich library of attack scenarios that are updated regularly based on the latest cyber threat intelligence, including both single and multi-vector attacks.	Shape different attack scenarios to simulate various types of cyber-attacks. Can be tailored for industry-specific requirements or customised for a specific organisation's threat landscape.	Enable access from remote locations to facilitate the simulation of geographically dispersed business operations.

Institute Training Essentials and Intermediate Modules:

A comprehensive range of cyber security training modules designed and taught by practitioners

BUILDING AN EFFECTIVE ORGANIZATION WIDE CYBER RESILIENCE PROGRAM			
Cyber Oversight for Board Members	Cyber Readiness for Management	Cyber Wargaming for Operations	Cyber Awareness for End-Users
Understand the possible varieties of cyber threats and their enterprise-wide impact. Learn to make optimal decisions during a cyber breach through a risk-based approach.	Understand how business can be impacted by cyber breaches. Run through probable threat scenarios to understand best practices and lessons learnt through case studies.	Learn to identify, defend, respond to and conduct post-mortem forensics on simulated cyber attacks.	Learn about the latest cyber security threats along with corresponding defence, protection, and preventive measures.
Modules: • Board Oversight • Risk Management • Cyber Crisis Communication • Cyber Crisis Simulation Table Top Exercise	Modules: • Risk Storm Exercises • Cyber Crisis Communication • Cyber Crisis Simulation Table Top Exercise	Modules: • Tactical Cyber Wargaming • Vulnerability Assessment • Incident Response Management • Risk Assessment • Operational Technology • Cyber Range Exercise	Modules: • Advanced Cyber Awareness • Online Security Awareness Education
1/2 Day	1 Day	3 Days	1 Day

Trustwave®
a Singtel company

For more information: www.trustwave.com