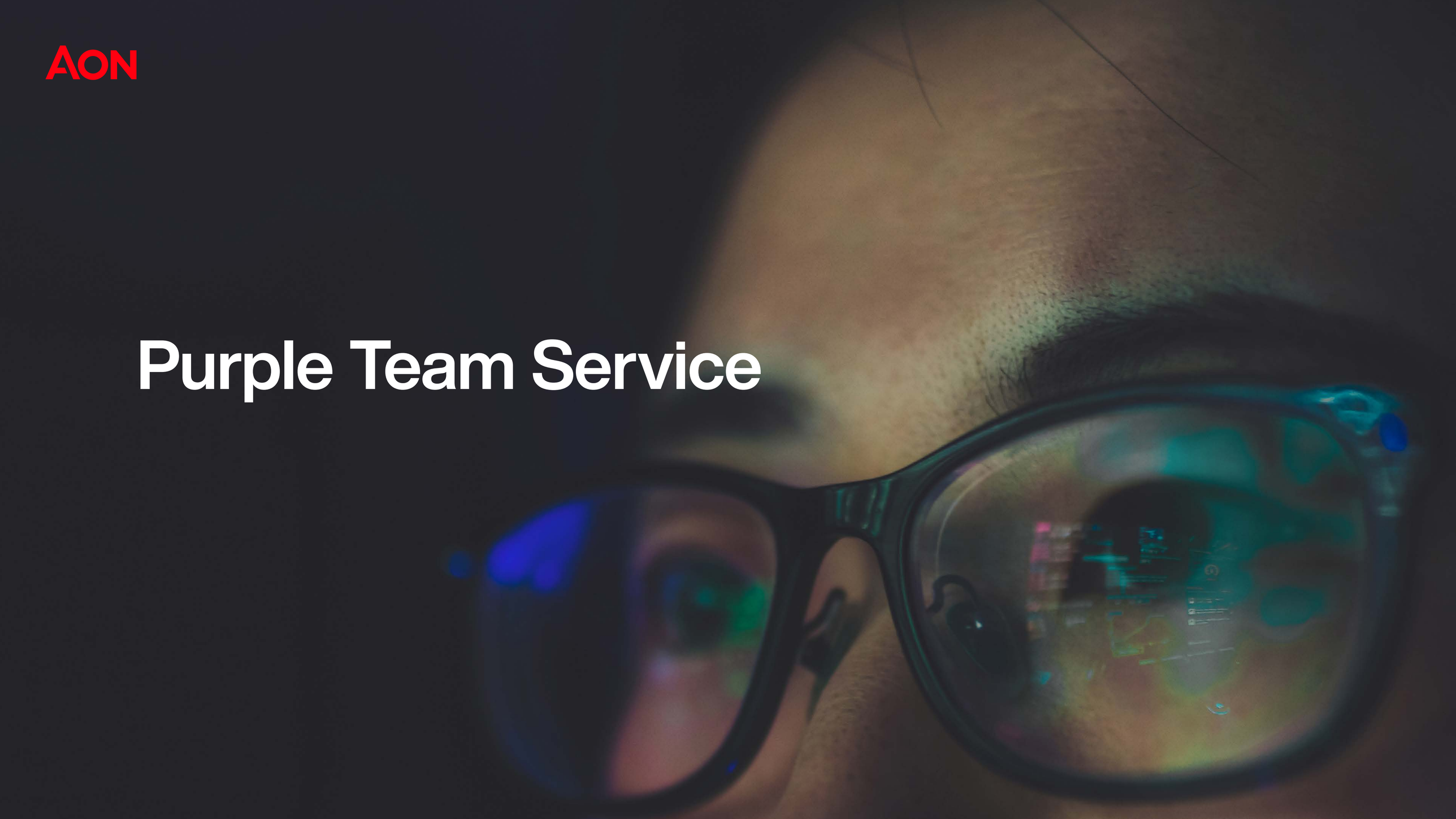
AON

# Purple Team Service

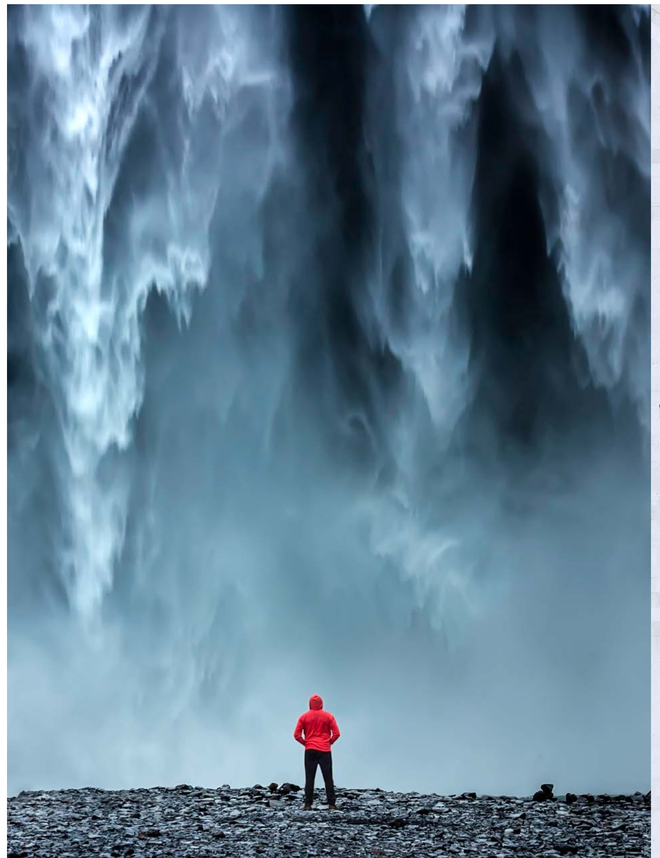


# Enhancing Cyber-Attack Detection Capability and Benchmarking Progress



It can come as a surprise when an organisation that follows security best practices and regularly conducts security risk assessments, is suddenly subject to a major cyber breach, often resulting in significant business interruption, financial losses, and reputational damage.

A popular approach to assessing cyber resilience is to conduct security audits, risk assessments and security testing of discreet assets (e.g., penetration testing systems that store or process sensitive data). Whilst these activities are valuable for securing the individual systems, the approach is asset-centric, and does not factor in the sophisticated methods and attack paths employed by advanced threat actors.



Major cyber breaches can result in significant business interruption, financial losses, and reputational damage.

# A “Threat-Centric” Approach

The Tactics, Techniques and Procedures (TTPs) used by cyber criminals typically involve initial access through social engineering and/or exploitation of perimeter network weaknesses; the compromise of legitimate user accounts and systems access; and misuse of those accounts to persist and further position the attackers for actions on criminal objectives, such as identifying confidential data and intellectual property to exfiltrate for cyber extortion.

Once all the required components for a successful attack are complete, e.g., the compromise of privileged accounts that have access to critical systems and data, the attack can be executed. This is typically timed on a weekend or public holiday when resources are likely to be limited, thereby reducing the likelihood of detection or a robust response.

Even organisations with isolated sensitive systems (e.g., air-gapped networks), can still come under threat as sophisticated attackers gain access by targeting the air-gapped systems users and administrators.

Our Purple Team Service is designed to replicate such attacks using sophisticated TTPs. This threat-centric approach allows your organisation to effectively assess your cyber-attack detection controls across the cyber kill chain, providing a true measure of resilience by identifying, benchmarking, and providing appropriate remedial guidance to address gaps.

Assessing cyber-attack detection capability enables you to better prepare and achieve successful outcomes during a real-world cyber-attack.

# What is a Purple Team?



In cyber security, a purple team is a collaboration between an attacking team (red team) and a defending team (blue team) to determine the effectiveness of cyber-attack detection controls.

Aon's purple team service is delivered by globally certified professionals in collaboration with your response team, to identify and help remediate cyber-attack detection gaps and enhance your organisation's attack detection capability.

**Attack Detection Gap Analysis**

Cyber-attack techniques are executed to determine your organisation's current detection efficacy. Results are analysed to identify detection gaps for prioritised remediation.

**Enhance Attack Detection Capability**

Support for detection rules and corresponding alerts are implemented, based on available data sources, detection technology and access provided.

**Attack Detection Knowledge Transfer**

Different types of threat intelligence are used to personalise adversary attack scenarios to determine appropriate adversary attack techniques. Identified adversary attack techniques are mapped to MITRE ATT&CK® (an internationally recognised framework) for consistency and benchmarking. Attack detection efficacy tracking systems are also implemented to logically record and benchmark progress.

Even when companies have adopted the latest technologies and managed services such as Endpoint Detection & Response (EDR), Security Operations Centre (SOC) and Managed Detection & Response (MDR), detection gaps can still exist. Purple team exercises validate your organisation's technologies and services are operating effectively, providing reassurance that cyber-attack techniques and behaviours can be reliably detected by your response team.

# How Long do Purple Team Exercises Take?

Based on the agreed scope, purple team exercises are typically conducted over a 2-6 week period to determine your current detection gaps and to assist with remediation and enhancements.

Cyber-attack techniques are constantly evolving. It is recommended regular follow ups or retainer-based purple team exercises are conducted to ensure your organisation is continually testing detection capability based on the latest cyber-attack techniques.

# Key Deliverables

The following deliverables are provided during a purple team exercise to track and improve your detection capability:

**1. Summary Report**

The summary report details your results and the improvements implemented during your purple team exercise, including:

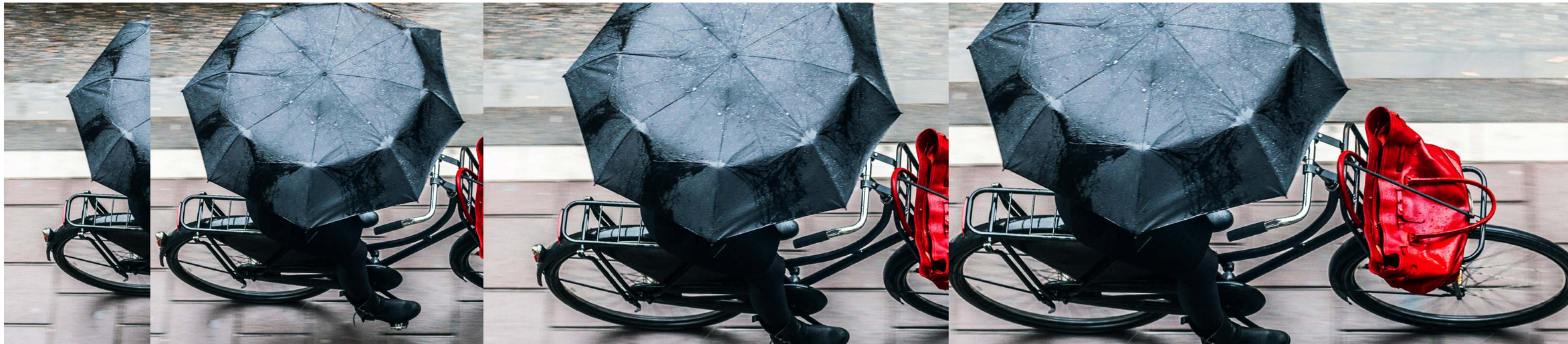
- MITRE ATT&CK Tactics coverage summary
- Detection results summary benchmarked against MITRE ATT&CK showing progress and enhancements to detection capability
- Detection rules and alerts implemented during the engagement
- Strategic recommendations
- Technical supporting evidence for detection techniques identified, implemented and tested as well as other referenced material.

**2. Attack Technique Worksheet**

The attack technique worksheet is a full log of the purple team exercise activities including the in-scope attack techniques executed, attack tool commands, attack execution timestamps and detection timestamps.

**3. MITRE ATT&CK Enterprise Navigator Heat Map**

A MITRE ATT&CK Navigator JSON file is included with your report to highlight detection gaps based on your in-scope MITRE ATT&CK techniques. The MITRE ATT&CK Navigator tool can be used to easily visualise detection gaps.



# Why Aon?

Aon Cyber Solutions purple team operators are highly accredited with internationally recognised qualifications, complimented by extensive experience conducting penetration testing and adversary attack simulation exercises.

**Consultant Qualifications**

Aon Cyber Solutions purple team operators hold specialist certifications and are experienced at conducting adversary attack simulations under regulatory frameworks such as Hong Kong Monetary Authority (HKMA) Cyber Resilience Assessment Framework (C-RAF) intelligence-led Cyber Attack Simulation Testing (iCAST), and the Association of Banks in Singapore (ABS) red team guidelines.

**Internationally Recognised Methodology**

- Aon Cyber Solutions adversary attack simulation methodology adheres to the following international regulator standards and guidelines:
- UK Bank of England CBEST scheme
- CREST STAR (Simulated Targeted Attack and Response)
- Threat Intelligence Based Ethical Red teaming (TIBER-NL/TIBER-EU)
- Monetary Authority of Singapore (MAS)/Association of Banks in Singapore (ABS) Adversarial Attack Simulation Exercises (AASE) guidelines or “red teaming” guidelines
- Hong Kong Monetary Authority (HKMA) Cyber Resilience Assessment Framework (C-RAF) intelligence-led Cyber Attack Simulation Testing (iCAST)

Aon Cyber Solutions offers a world-class accredited and experienced team of certified consultants, leveraging the latest advanced targeted attack knowledge, discovered by our Digital Forensics and Incident Response (DFIR) team, and providing organisations with actionable remediation steps, and strategic guidance to enhance organisational cyber resilience.

# Accreditations



**CREST Accredited Member Company**

Aon is a member company of the Council for Registered Ethical Security Testers (CREST), offering certified services under the scheme including penetration testing, intelligence led penetration testing, security architecture and vulnerability assessment services.

**CBEST and CREST STAR (Simulated Target Attack and Response)**

CBEST is a framework to deliver controlled, bespoke, intelligence-led cyber security tests. The tests replicate behaviours of threat actors, assessed by the UK Government and commercial intelligence providers, as posing a genuine threat to systemically important financial institutions.

CBEST and CREST STAR testing differ from other security testing in that it is threat intelligence based, less constrained and focuses on more sophisticated and persistent attacks on critical systems and essential services. This provides a holistic assessment of a financial services or infrastructure provider's cyber capabilities by testing people, processes and technology in a single test which will be less time constrained than traditional penetration testing.

**GBEST**

GBEST is a scheme based on the CBEST model utilised by UK Government Departments. The overall scheme is co-ordinated by the cabinet office, but each exercise is procured, led, and ultimately owned by the Government Department carrying out the exercise. The National Cyber Security Centre (NCSC) provide validation of the threat intelligence and general technical assurance to each exercise.

**TIBER-EU**

The Threat Intelligence-Based Ethical Red Teaming for the European Union (TIBER-EU) is the first EU-wide guide on how authorities, entities and threat intelligence and red team providers should work together to test and improve the cyber resilience of entities by carrying out a controlled cyber attack.

TIBER tests mimic the TTPs of real-life attackers, based on bespoke threat intelligence. They are tailor-made to simulate an attack on the critical functions of an entity and its underlying systems. The test is intended to reveal the strengths and weaknesses of the tested entity, enabling it to reach a higher level of cyber maturity.

**iCAST**

Intelligence-led Cyber Attack Simulation Testing (iCAST) is a framework introduced by the Hong Kong Monetary Authority (HKMA) in response to the changing cyber security landscape, similar in structure and approach to the CBEST scheme in the UK.

## Contact Us

Chris Rees
Managing Director – ACSG – Cyber Proactive
+65 9459 3985
chris.rees@aon.com

aon.com/apac

## About

Aon plc (NYSE: AON) exists to shape decisions for the better—to protect and enrich the lives of people around the world. Our colleagues provide our clients in over 120 countries with advice and solutions that give them the clarity and confidence to make better decisions to protect and grow their business.

©2022 Aon plc. All rights reserved.

The information contained herein and the statements expressed are of a general nature and are not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information and use sources we consider reliable, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The inclusion of MITRE ATT&CK does not imply endorsement or support from MITRE.