WORKGROUP 3
CYBER SECURITY

SERVICES AND DIGITAL ECONOMY
TECHNOLOGY
ROADMAP

19 NOVEMBER 2018

SG:D
EMPOWERING POSSIBILITIES

INFOCOMM
MEDIA
DEVELOPMENT
AUTHORITY

OUTLINE

A MARKET STUDY

1. Market Potential
2. Key Drivers
3. Others

B TECHNOLOGY STUDY

1. Technology Readiness Map
2. Application Use cases

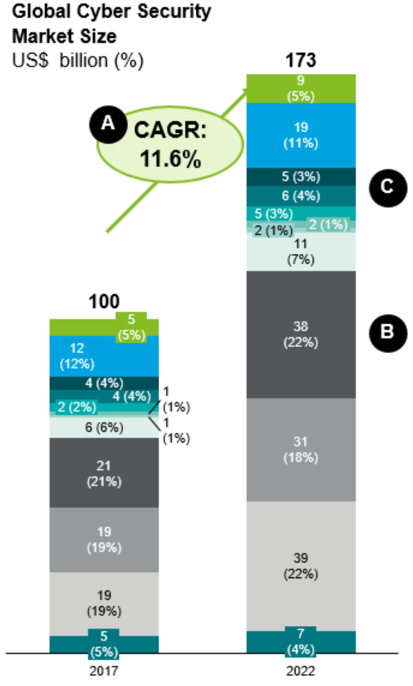
C CONCLUSIONS

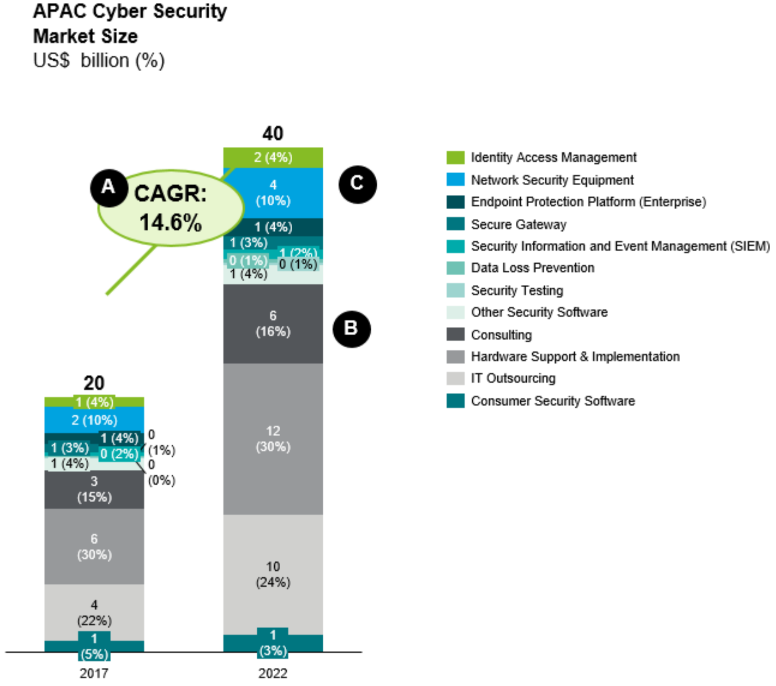
1. SWOT Analysis
2. Recommendations

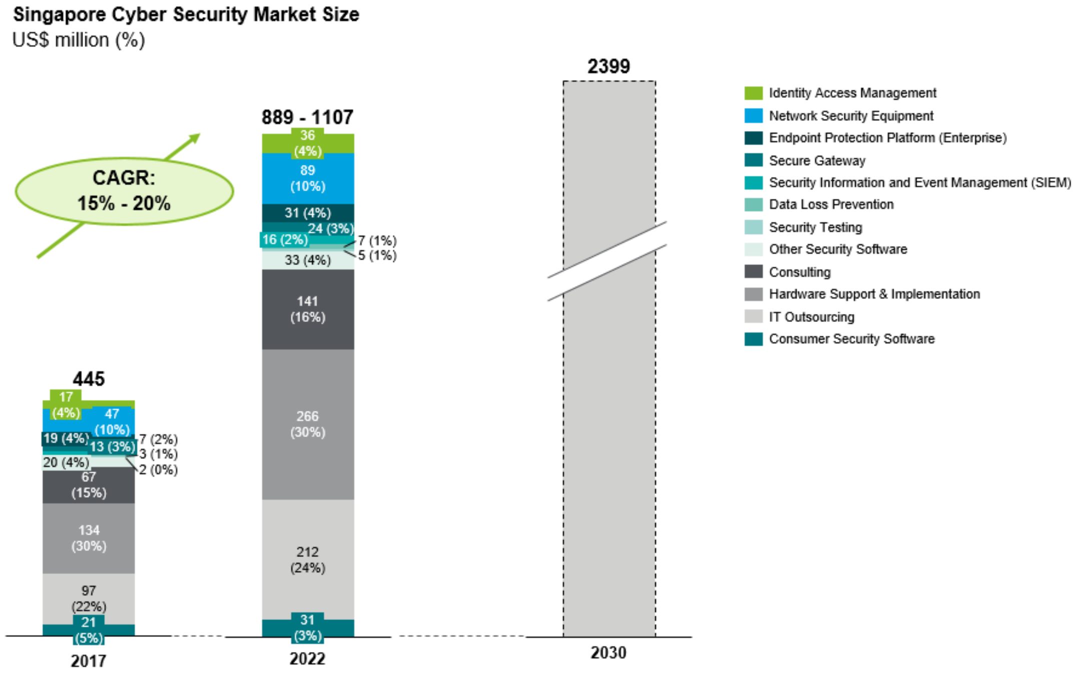
OUTLINE

- A MARKET STUDY
  - 1 Market Potential
  - 2 Key Drivers
  - 3 Others
- B TECHNOLOGY STUDY
  - 1 Technology Readiness Map
  - 2 Application Use cases
- C CONCLUSIONS
  - 1 SWOT Analysis
  - 2 Recommendations

MARKET POTENTIAL


Global Cyber Security Market Size
US$ billion (%)


APAC Cyber Security Market Size
US$ billion (%)


Singapore Cyber Security Market Size
US$ million (%)

Source: Gartner, Netscribes IDC, Pardee Center for International Futures , Trustwave, IMF; Monitor Deloitte Analysis

Worldwide Security Spending by Segment, 2017-2019 (Millions of U.S. Dollars)**

Market Segment	2017	2018	2019
Application Security	2,434	2,742	3,003
Cloud Security	185	304	459
Data Security	2,563	3,063	3,524
Identity Access Management	8,823	9,768	10,578
Infrastructure Protection	12,583	14,106	15,337
Integrated Risk Management	3,949	4,347	4,712
Network Security Equipment	10,911	12,427	13,321
Other Information Security Software	1,832	2,079	2,285
Security Services	52,315	58,920	64,237
Consumer Security Software	5,948	6,395	6,661
Total	101,544	114,152	124,116

Source: Gartner Forecast: Information Security, Worldwide 2016-2022, 2Q18 Update), Monitor Deloitte Analyses

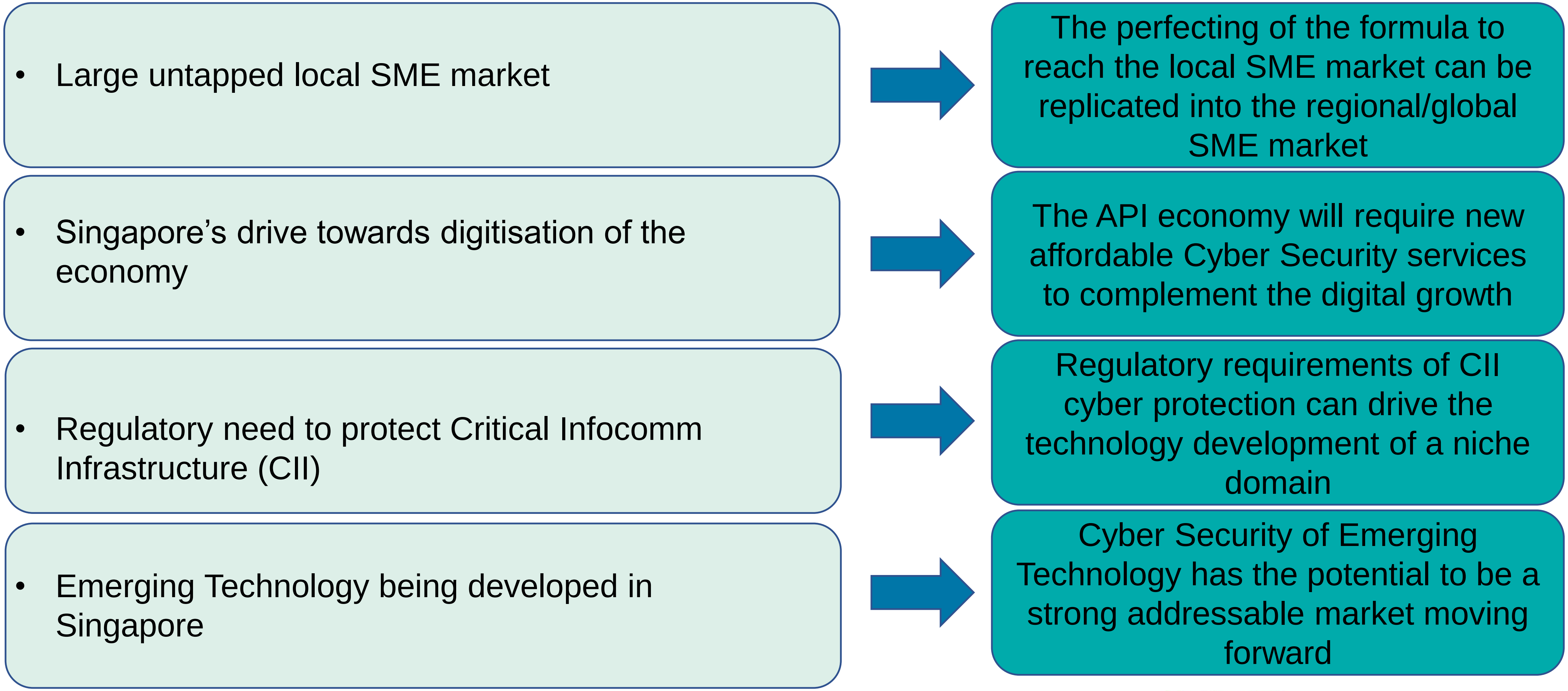
Key Drivers

- Security Risk due to Evolving Cyber Threats
- Digital Transformation
- Data Protection Regulatory Requirements

Key Trends

- Digital Transformation Initiatives will drive additional security service spending
- Businesses will spend on GDPR related consulting and implementation
- Cyber Services would form 50% of security software delivery by 2020

The Case for Singapore



- Large untapped local SME market → The perfecting of the formula to reach the local SME market can be replicated into the regional/global SME market
- Singapore’s drive towards digitisation of the economy → The API economy will require new affordable Cyber Security services to complement the digital growth
- Regulatory need to protect Critical Infocomm Infrastructure (CII) → Regulatory requirements of CII cyber protection can drive the technology development of a niche domain
- Emerging Technology being developed in Singapore → Cyber Security of Emerging Technology has the potential to be a strong addressable market moving forward

Source: IMDA

OUTLINE

A MARKET STUDY

1 Market Potential

2 Key Drivers

3 Others

B TECHNOLOGY STUDY

1 Technology Readiness Map

2 Application Use cases

C CONCLUSIONS

1 SWOT Analysis

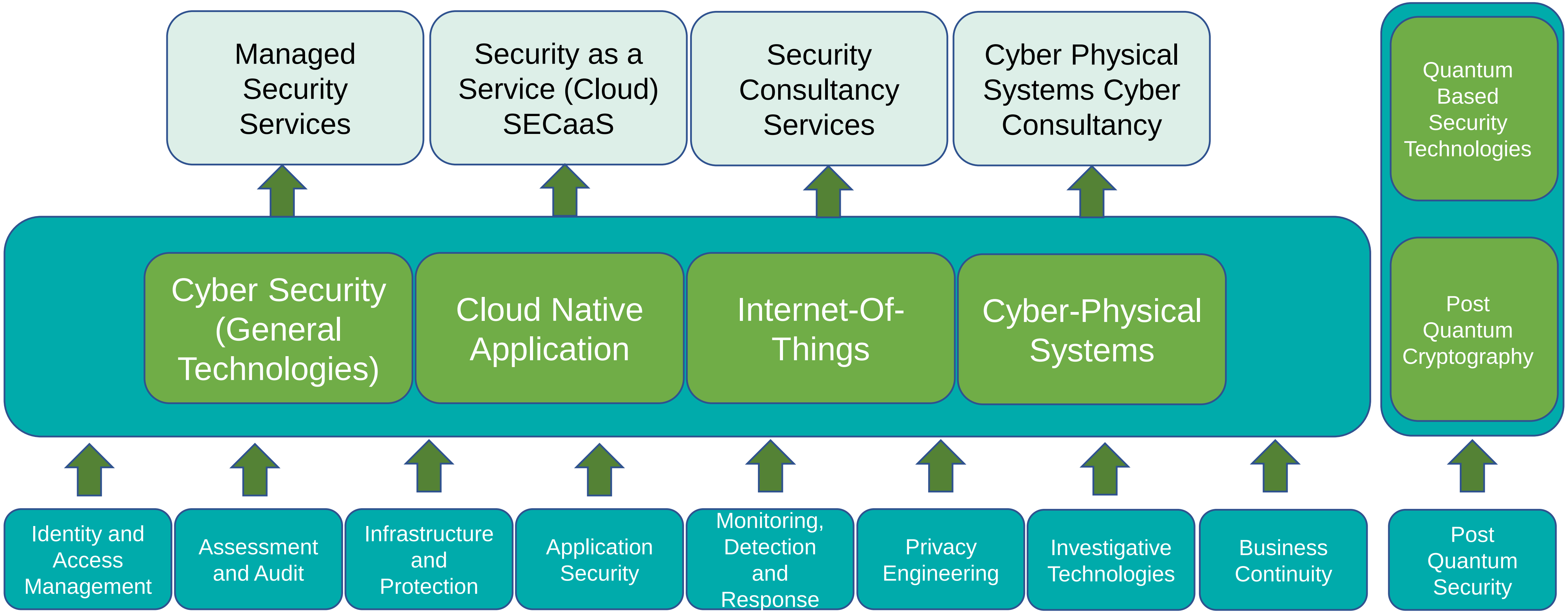
2 Recommendations

SG:D EMPOWERING POSSIBILITIES

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

TECHNICAL WRITE-UP SUMMARY

Cyber Security as a Technology Area cuts across everything. For the purpose of this report, the focus would be on Cyber Security useful to the Singapore Digital Economy where Singapore has a right to play


Managed Security Services
Security as a Service (Cloud) SECaaS
Security Consultancy Services
Cyber Physical Systems Cyber Consultancy
Quantum Based Security Technologies
Cyber Security (General Technologies)
Cloud Native Application
Internet-Of-Things
Cyber-Physical Systems
Post Quantum Cryptography
Identity and Access Management
Assessment and Audit
Infrastructure and Protection
Application Security
Monitoring, Detection and Response
Privacy Engineering
Investigative Technologies
Business Continuity
Post Quantum Security

Source: IMDA

TECHNOLOGY READINESS MAP

Cyber Security (General Technologies)

Categories	NOW - 2 years	3 - 5 years	> 5 years
Identify & Access Management	Tokenisation, Continuous Behaviour Authentication	Scalable Attribute Based Encryption	Fine-grained authentication and access control
Assessment and Audit	Orchestration of Simulation	Breach and Attack Simulation	Human Agents Simulation
Infrastructure Protection	Deception Technology Physically Unclonable Function (PUF)	Security Orchestration and Automation Tools	Self-Shielding Dynamic Network Architecture
Application Security	Runtime Application Self-Protection (RASP)	Binary Analysis and Assessment	Automated Software Patching Tools
Monitoring, Detection and Response	AI/ML enabled Cyber Security	Threat Hunting	Fusion of Cyber threat Intelligence
Privacy Engineering	Secure multi-part Communications	Privacy-Preserving Technologies (1)	Privacy-Preserving Technologies (2)
Investigative Technologies	Cyber Forensics – Blockchain, Multimedia, Video	Cyber Forensics – Vehicular, Infotainment, Drone	Cyber Forensics - Robotics, Autonomous Systems, Certification Testing Tools
Business Continuity	Integrated Orchestration of heterogeneous network	Resource Efficient Continuous Data Protection (CDP)	Blockchain in Disaster Recovery

Source: IMDA

SG:D EMPOWERING POSSIBILITIES

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

TECHNOLOGY READINESS MAP

Cloud Native Application Cyber Security

Categories	Now - 2 years	3 - 5 years	> 5 years
Identify & Access Management	Federated Identity Technology	Key Management	
Assessment and Audit	Cyber Security Ratings services	Cloud security testing and assessment tools	
Infrastructure Protection	Service Mesh\Automated Application Security Orchestration	Software Define DDoS detection algorithm	Platform based Security Automation
Application Security	Container Security Technologies	Security Tools integration for Continuous Development	Security Tools integration for regulatory compliance
Monitoring, Detection and Response	Microservice endpoint Threat Monitoring , Prevention and Response	Engineering Principle Based Detection	Chaos Engineering
Investigative Technologies		Continuous monitoring and support for investigation	
Business Continuity	Recovery by Snapshots Recovery by Redeployment	Federated Cluster Deployment	

Source: IMDA

TECHNOLOGY READINESS MAP

Internet-Of-Things Cyber Security

Categories	Now - 2 years	3 - 5 years	> 5 years
Identify & Access Management	Biometrics, Certificates and Lightweight Key Management, eSIM		Integration of authentication protocols
Assessment and Audit	Security Testing and vulnerability Analysis	IoT framework assessment tools	Cyber validation tools for regulatory assessment for sector specific domains
Infrastructure Protection	IoT Honeypots Microsegmentation	5G Security Tools for auto-patching of vulnerable embedded systems	Next Generation IoT Infrastructure protection
Application Security	Lightweight DTLS chips	Source and Binary code application protection for IoT Devices	Modelling and Analysis of Wireless Sensor Networks
Monitoring, Detection and Response	Real time monitoring for continuous threat detection and management	Dynamic detection, profiling, and accounting of IoT connections	Emerging threats research specific to IoT architectures
Privacy Engineering	Secure aggregation or fusion of sensor data for privacy	Edge computing data security	Personal gateway
Investigative Technologies	IoT Memory Forensics		Tools to support IoT forensic framework

Source: IMDA

TECHNOLOGY READINESS MAP

Cyber-Physical System Cyber Security

Categories	Now - 2 years	3 - 5 years	> 5 years
Identify & Access Management	Trusted Computing Based Identity Protection	Access management framework to all components in CPS	
Assessment and Audit	Digital Twin	Software & Framework Extension to Digital Twin	Model-based security testing for cyber-physical systems
Infrastructure Protection	Data Diodes	Deception based Protection	Layered Defence
Application Security			Techniques for auto-patching of CPS vulnerability
Monitoring, Detection and Response	Real time monitoring threat detection in CPS	Automation in vulnerability detection and incident response in CPS	Protocol-oblivious anomaly detection in CPS
Privacy Engineering		Data Protection and Security of Training Data	Lightweight and resilient crypto for Cyber-Physical Systems

Source: IMDA

TECHNOLOGY READINESS MAP

Post Quantum Computing

Categories	Now - 2 years	3 - 5 years	> 5 years
Technology	Quantum random number generation (QRNG)		
	Quantum Key Distribution (QKD) (Free Space Terrestrial)	Quantum Key Distribution (QKD) (Satellite QKD)	Quantum Proof Cryptography
	Quantum Key Distribution (QKD) (Fibre QKD)	Quantum Key Distribution (QKD) (Terrestrial) Re-broadcast	Network QKD

Source: IMDA

USE CASES FOR CYBER SECURITY

1 SECURITY OPERATIONS CENTRE

- Use of **ML/ AI** in Cyber Security enables **contextual awareness** for threat identification & conducting automated testing leading to several benefits
  - **Increase accuracy** to threat detection
  - Reduce **workload** of security analysts
  - Reduces **cost of providing service** lowering barriers to customer adoption

2 SECURITY-AS-A-SERVICE

- Cloud Native Application Endpoint Protection
- Cyber Health Checks
- Business Continuity / Disaster Recovery
- Identity-As-A-Services **(IDaaS)**
- Automated Security Orchestration

3 SECURITY CONSULTING SERVICES

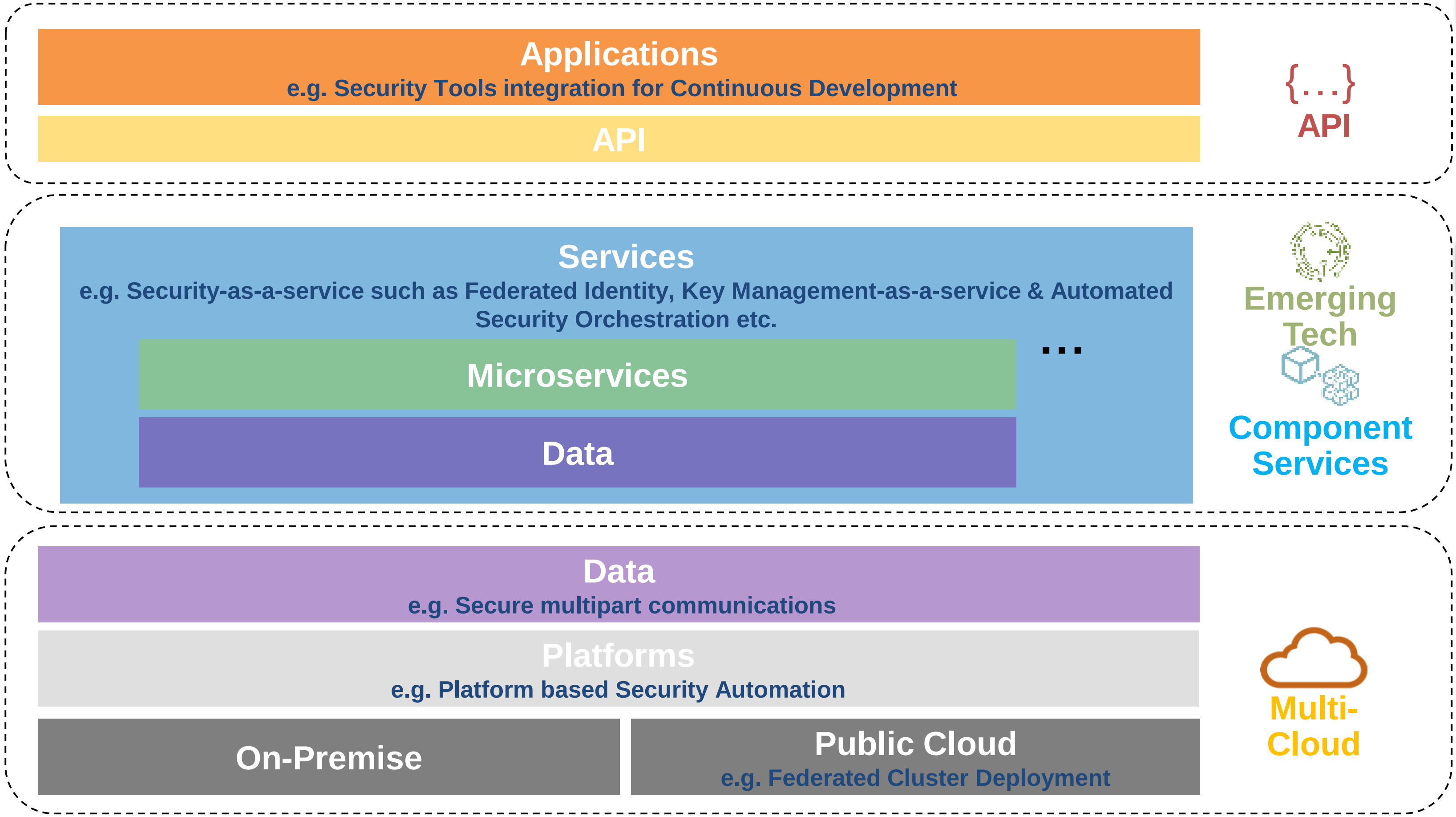
- Emerging Technology Cyber Forensics Services
- Bug Bounty Services
- Digital Twin Services

Source: IMDA

SG:D EMPOWERING POSSIBILITIES

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

ALIGNMENT TO CLOUD NATIVE ARCHITECTURE



Applications
e.g. Security Tools integration for Continuous Development

API

{...} API

Services
e.g. Security-as-a-service such as Federated Identity, Key Management-as-a-service & Automated Security Orchestration etc.

Microservices

Data

...

Emerging Tech

Component Services

Data
e.g. Secure multipart communications

Platforms
e.g. Platform based Security Automation

On-Premise

Public Cloud
e.g. Federated Cluster Deployment

Multi-Cloud

1 Identity and Access Management

1.1 Federated Identity Technology
1.2 Key Management

Utilising multiple environmental or biological indicators as well as behaviors to authenticate identities and to manage access control.

2 Monitoring, Detection and Response

2.1 API service endpoint for Threat Monitoring
2.2 Prevention and Response
2.3 Engineering Principle Based Detection

Threat detection solutions and services will be enhanced with pre-emptive detection and contextual correlation capabilities.

3 Infrastructure Protection

3.1 Service Mesh/Automated Application Security Orchestration
3.2 Software Defined DDoS detection algorithm
3.3 Platform based Security Automation

Infrastructure protection will be enhanced by technologies that will enable higher levels of resiliency

Source: IMDA

OUTLINE

A MARKET STUDY	1 Market Potential	2 Key Drivers	3 Others
B TECHNOLOGY STUDY	1 Technology Readiness Map	2 Application Use cases	
C CONCLUSIONS	**1 SWOT Analysis**	**2 Recommendations**	

SWOT ANALYSIS

STRENGTHS

1. Clear Government Regulation in Cyber Security
2. High Quality Education
3. Cyber R&D Investment
4. Cyber Security Industry Investment in Technology
5. High Concentration of Cyber Technology Companies

WEAKNESSES

1. Lack of scale in country
2. Rate of Adoption of Cyber Security
3. Small talent pool spread over multiple technology domains
4. Shortage of Cyber Entrepreneurs
5. Shortage of Data for Research in academia

OPPORTUNITIES

1. Physical access to serve regional market
2. Branding of Trusted and Competent Country in Cyber Security
3. ASEAN region embracing Digital economy
4. Regional Cyber Security Support Center
5. Digital Transformation

THREATS

1. Well-Funded Global Competition
2. Lack of clarity in regulations for emerging technologies

Source: IMDA

7 Key Strategies are recommended as per the DE Framework for Action to Achieve Services 4.0 Objectives

DIGITALISING INDUSTRIES

- **Enhanced SECaaS capabilities**
  - Identity and Access Management
  - Threat Monitoring and Response
  - Business Continuity
- Common Service Marketplace
- Data Protection Platform for Data Governance and compliance

TALENT

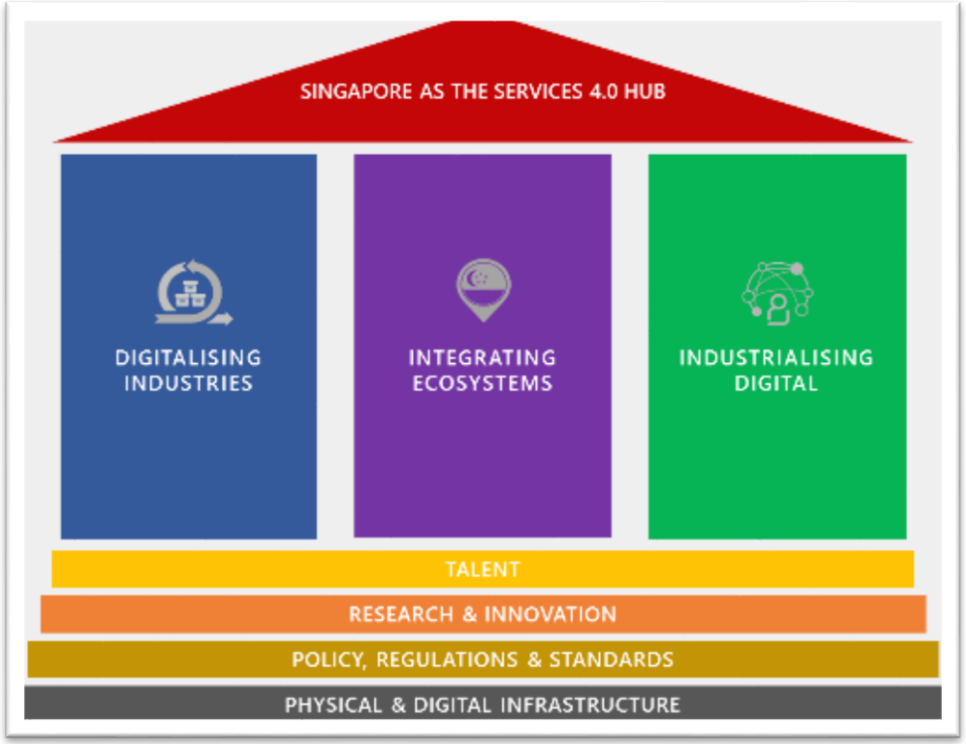
- **Cyber Security Developer Skills Framework**
- **Cyber Security Product Development Skills Framework**
- Entrepreneurship in Cyber Curriculum

POLICY, REGULATION & STDS

- **IoT Security Framework & Certification**
- Regulations for Emerging Technology

INTEGRATING ECOSYSTEMS

- **Cyber Security Hub For Emerging Technologies (Quantum, Forensics, Blockchain, Drones, CPS)**
- Cloud Service Providers collaboration in auto-security orchestration


SINGAPORE AS THE SERVICES 4.0 HUB
DIGITALISING INDUSTRIES
INTEGRATING ECOSYSTEMS
INDUSTRIALISING DIGITAL
TALENT
RESEARCH & INNOVATION
POLICY, REGULATIONS & STANDARDS
PHYSICAL & DIGITAL INFRASTRUCTURE

INDUSTRIALISING DIGITAL

- **Novel cyber trust platforms for locally developed cyber products/technologies.**
- Secure Development, Implementation and Operations
- Digital consent platform for data sharing
- IoT Security Concentration
  - Transport, Healthcare, Logistics, Manufacturing, Payment

RESEARCH & INNOVATION

- ML/AI for Cyber Security
- Cyber Forensics of Emerging Technology
- Privacy Engineering (Data Sharing 2.0 / PP Tech)
- IoT Security
- **Innovation to reduce cost of cyber adoption**

PHYSICAL & DIGITAL INFRA

- Secure Infrastructure (5G, NG-NBN)

Source: IMDA

RECOMMENDATION – CLOUD NATIVE APPLICATION EVERYTHING-AS-A-SERVICE

01 Catalyse the availability of cloud delivered application security for Cloud Native Applications

02 Catalyse the local Identity and Access Management service providers

03 Collaborate with Cloud Service Providers (CSP) to enable automation in Security Orchestration of Cloud Native Application Deployment

04 Create a Common (Cloud) Service Marketplace

Source: IMDA

RECOMMENDATION – PRIVACY ENGINEERING AND PROTECTION

01 Increase Research and Translation Funding in Data Privacy Technologies

02 Establish Digital Economy tools to encourage Data sharing such as Data sharing consent services / platforms

03 Establish Data compliance / protection platforms to enable Compliance to Data regulation

Source: IMDA

RECOMMENDATION – INTERNET-OF-THINGS CYBER SECURITY

01 Establish a IoT Cyber Security Framework

02 Identifying and commercialising key areas for IoT Cyber Security

03 Encouraging use of technologies such as eSIM that will enable IoT Identity/Asset Management

Source: IMDA

RECOMMENDATION – CYBER HUB FOR EMERGING TECHNOLOGY

The Singapore Government should develop relevant talent, enhance research capabilities and encourage industry collaboration to make Singapore a Cyber Hub for the following:

01 **Cyber Investigation Tools of Emerging Technology**

02 **Blockchain Cyber Security**

03 **Cyber-Physical System Security**

04 **Quantum Security Technologies**

Source: IMDA

RECOMMENDATION – AWARENESS, ADOPTION AND ECOSYSTEM DEVELOPMENT

01 Groom Cyber entrepreneurs to create simple and affordable Cyber services

02 Establishing critical infrastructure including novel platforms for local developed Cyber products

03 Developing relevant talent pipeline for development of secure products to the implementation and operations of the Cyber Security systems

Source: IMDA

SG:D EMPOWERING POSSIBILITIES

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

RECOMMENDATION – PATHWAYS TO TECHNOLOGY COMMERCIALISATION

01 **Allow Research Spin-offs and the Bridging of Research & Commercialisation**

02 **Building a Global Cyber Security Community**

Source: IMDA