HKBN
ENTERPRISE SOLUTIONS

Preparing for first HK Cybersecurity Law for Critical Infrastructure Operators

Alvin Chun

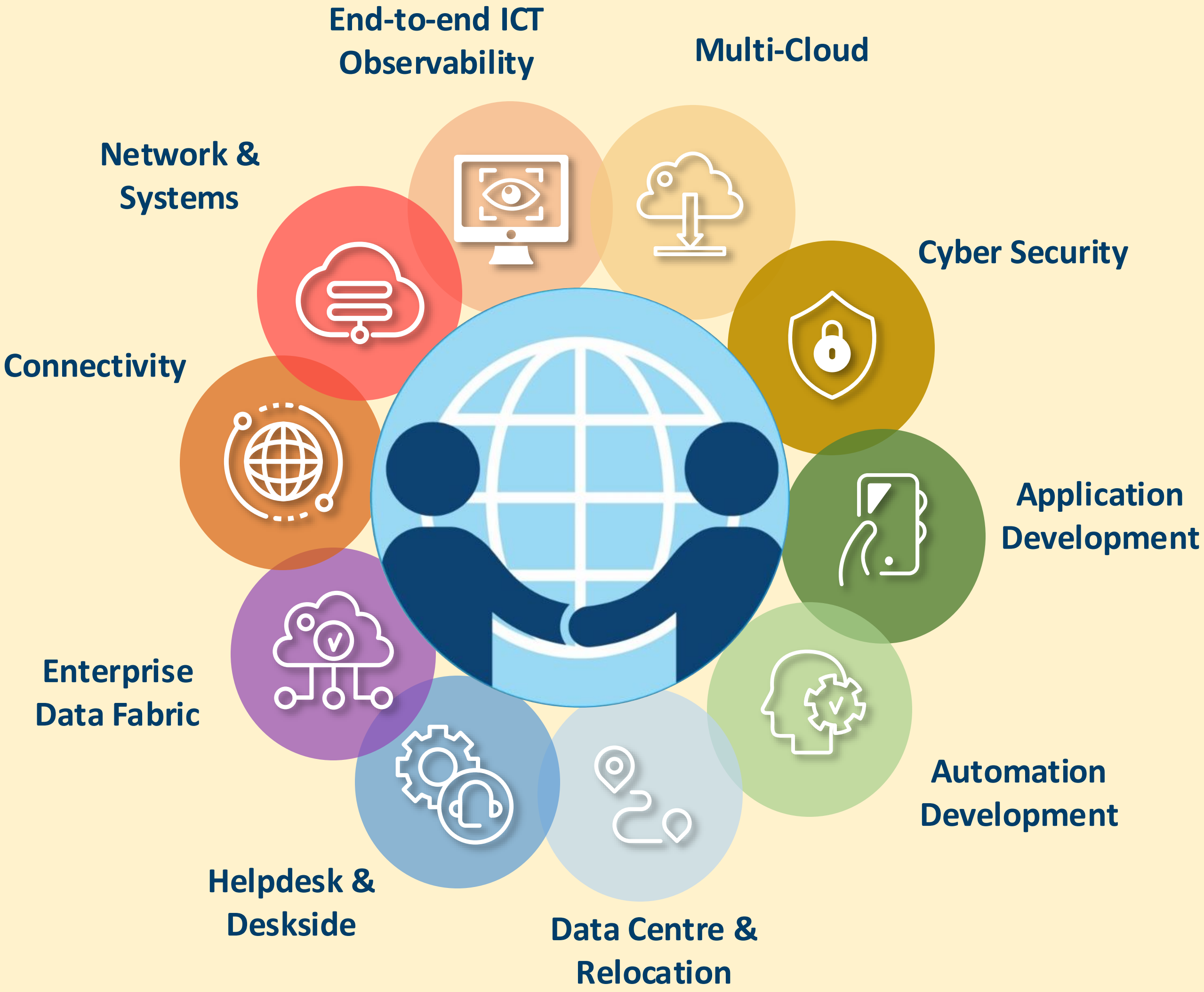
AVP – Sales Engineering (Cyber Security)

GDSA, CCSP, CISA, CEH, SABSA

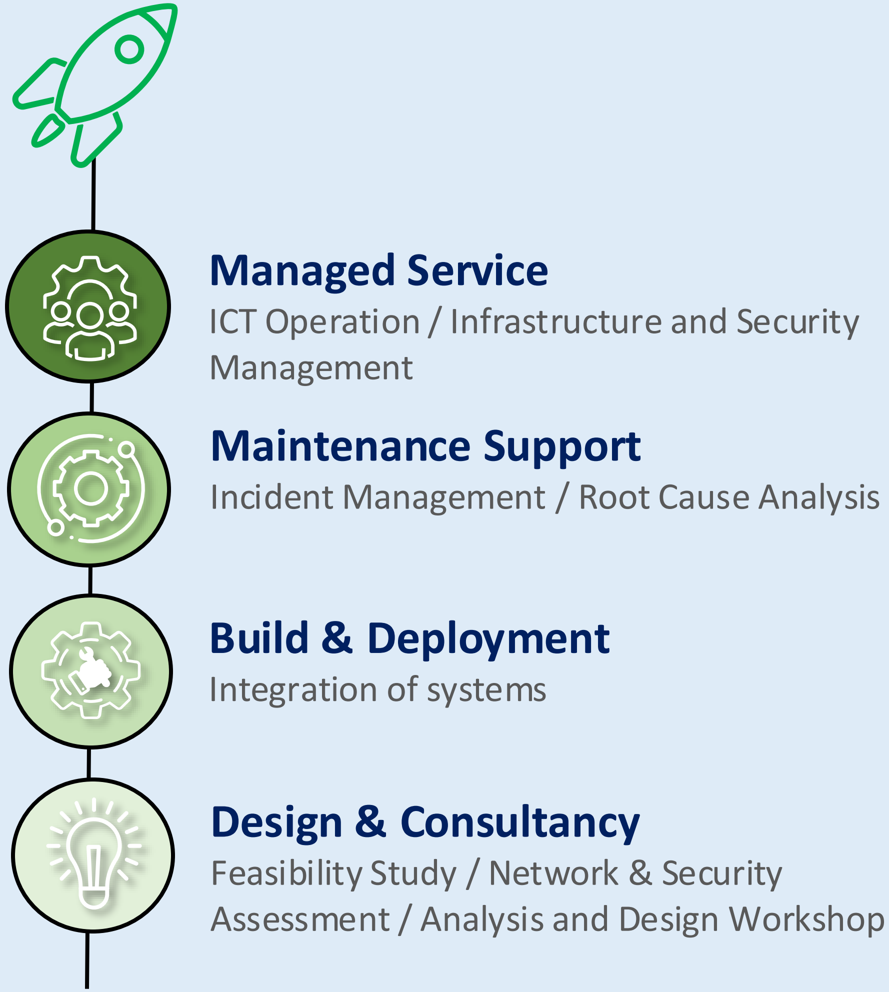
One-Stop-Shop Solutions and Services

HKBN
ENTERPRISE SOLUTIONS

Diverse and Bespoke ICT Solutions



All-Rounded ICT Life-Cycle Management Services



Managed Service
ICT Operation / Infrastructure and Security Management

Maintenance Support
Incident Management / Root Cause Analysis

Build & Deployment
Integration of systems

Design & Consultancy
Feasibility Study / Network & Security Assessment / Analysis and Design Workshop

Background

Purpose

Through requiring CIOs to fulfill framework, strengthen the security of their computer systems and minimize the chance of essential services being disrupted or compromised due to cyberattacks

Relevant Laws

Mainland: 中華人民共和國網絡安全法 (2016年) & 關鍵信息基礎設施安全保護條例 (2021 年)
Macau: 網絡安全法 (2019 年)；
Other ref: Australia, UK, Singapore, EU, US, Canada

Organizations

- Energy
- Information Technology
- Banking and Financial Services
- Healthcare Services
- Communications and Broadcasting
- Land Transport
- Air Transport
- Maritime
- Major sports and performance venues
- Research and development parks

Reference Link: https://www.legco.gov.hk/yr2024/english/panels/se/papers/se20240702cb2-930-3-e.pdf

Framework

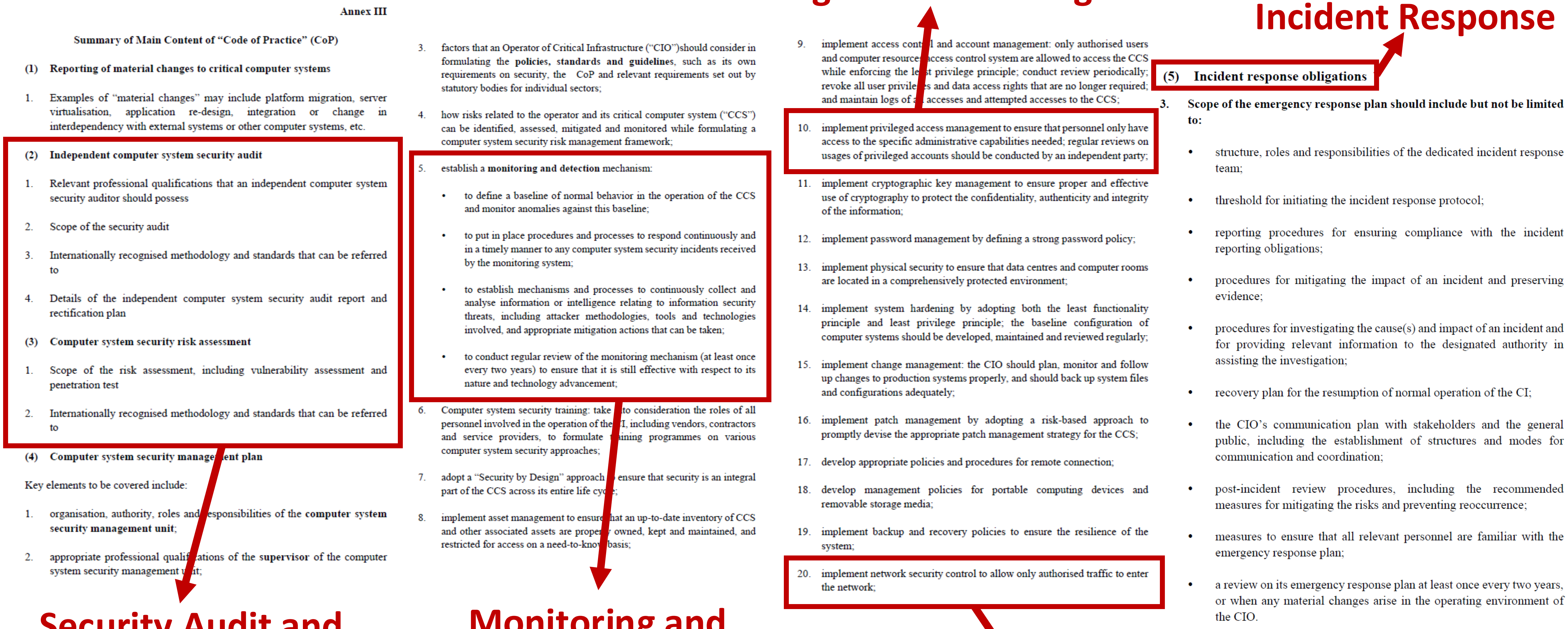
HKBN
ENTERPRISE SOLUTIONS

Categories	Statutory obligations
Organizational	Maintain address and office in Hong Kong
	Report any changes in ownership and operatorship
	Dedicated supervisor with Professional Knowledge and Certifications
Preventive	Inform any materials changes of the CCS (Includes platform migration, server virtualization, application re-design, integration or change in interdependency with external systems or other computer systems)
	Computer System Security Management Plan
	Security risk assessment • Vulnerability assessment (at least once a year) • Penetration test (at least once a year)
	Security Audit (at least once every two years)
	Third party service providers management
Incident Reporting & Response	Security Drill Test (at least every two years, performed by Commissioner's Office)
	Emergency Response Plan
	Report Security Incident

Failed or late to behave, inform, perform or submit would introduce fine-
Fines from $500,000 to $5,000,000- Continue offence introduce extra fine per day

Content of "Code of Practice"

HKBN
ENTERPRISE SOLUTIONS



Annex III

Summary of Main Content of "Code of Practice" (CoP)

(1) Reporting of material changes to critical computer systems

1. Examples of "material changes" may include platform migration, server virtualisation, application re-design, integration or change in interdependency with external systems or other computer systems, etc.

(2) Independent computer system security audit

1. Relevant professional qualifications that an independent computer system security auditor should possess

2. Scope of the security audit

3. Internationally recognised methodology and standards that can be referred to

4. Details of the independent computer system security audit report and rectification plan

(3) Computer system security risk assessment

1. Scope of the risk assessment, including vulnerability assessment and penetration test

2. Internationally recognised methodology and standards that can be referred to

(4) Computer system security management plan

Key elements to be covered include:

1. organisation, authority, roles and responsibilities of the **computer system security management unit**;

2. appropriate professional qualifications of the **supervisor** of the computer system security management unit;

3. factors that an Operator of Critical Infrastructure ("CIO")should consider in formulating the **policies, standards and guidelines**, such as its own requirements on security, the CoP and relevant requirements set out by statutory bodies for individual sectors;

4. how risks related to the operator and its critical computer system ("CCS") can be identified, assessed, mitigated and monitored while formulating a computer system security risk management framework;

5. establish a **monitoring and detection** mechanism:

   - to define a baseline of normal behavior in the operation of the CCS and monitor anomalies against this baseline;
   - to put in place procedures and processes to respond continuously and in a timely manner to any computer system security incidents received by the monitoring system;
   - to establish mechanisms and processes to continuously collect and analyse information or intelligence relating to information security threats, including attacker methodologies, tools and technologies involved, and appropriate mitigation actions that can be taken;
   - to conduct regular review of the monitoring mechanism (at least once every two years) to ensure that it is still effective with respect to its nature and technology advancement;

6. Computer system security training: take into consideration the roles of all personnel involved in the operation of the CI, including vendors, contractors and service providers, to formulate training programmes on various computer system security approaches;

7. adopt a "Security by Design" approach to ensure that security is an integral part of the CCS across its entire life cycle;

8. implement asset management to ensure that an up-to-date inventory of CCS and other associated assets are properly owned, kept and maintained, and restricted for access on a need-to-know basis;

9. implement access control and account management: only authorised users and computer resources; access control system are allowed to access the CCS while enforcing the least privilege principle; conduct review periodically; revoke all user privileges and data access rights that are no longer required; and maintain logs of all accesses and attempted accesses to the CCS;

10. implement privileged access management to ensure that personnel only have access to the specific administrative capabilities needed; regular reviews on usages of privileged accounts should be conducted by an independent party;

11. implement cryptographic key management to ensure proper and effective use of cryptography to protect the confidentiality, authenticity and integrity of the information;

12. implement password management by defining a strong password policy;

13. implement physical security to ensure that data centres and computer rooms are located in a comprehensively protected environment;

14. implement system hardening by adopting both the least functionality principle and least privilege principle; the baseline configuration of computer systems should be developed, maintained and reviewed regularly;

15. implement change management: the CIO should plan, monitor and follow up changes to production systems properly, and should back up system files and configurations adequately;

16. implement patch management by adopting a risk-based approach to promptly devise the appropriate patch management strategy for the CCS;

17. develop appropriate policies and procedures for remote connection;

18. develop management policies for portable computing devices and removable storage media;

19. implement backup and recovery policies to ensure the resilience of the system;

20. implement network security control to allow only authorised traffic to enter the network;

(5) Incident response obligations

3. Scope of the emergency response plan should include but not be limited to:

- structure, roles and responsibilities of the dedicated incident response team;
- threshold for initiating the incident response protocol;
- reporting procedures for ensuring compliance with the incident reporting obligations;
- procedures for mitigating the impact of an incident and preserving evidence;
- procedures for investigating the cause(s) and impact of an incident and for providing relevant information to the designated authority in assisting the investigation;
- recovery plan for the resumption of normal operation of the CI;
- the CIO's communication plan with stakeholders and the general public, including the establishment of structures and modes for communication and coordination;
- post-incident review procedures, including the recommended measures for mitigating the risks and preventing reoccurrence;
- measures to ensure that all relevant personnel are familiar with the emergency response plan;
- a review on its emergency response plan at least once every two years, or when any material changes arise in the operating environment of the CIO.

Privilege Access Management

Incident Response

Security Audit and Risk Assessment

Monitoring and Detection

Network Security Control

Highlights of the Legislative Framework

Governance

- Adopt a "Security by Design" Approach
- Data access right
- Backup and recovery policies to ensure the resilience of the system;

Identification

- Identify organization, authority, roles and responsibilities of the computer system security management unit
- Privileged access management to ensure that personnel only have access to the specific administrative capabilities needed
- Up-to-date inventory of CCS and other associated assets are properly owned, kept and maintained, and restricted for access

Protection

- **Implement network security control to allow only authorized traffic to enter the network**
- **Appropriate policies and procedures for remote connection**

Detection

- Establish a monitoring and detection mechanism and define a baseline of normal behavior
- Conduct Regular review of the monitoring mechanism
- System hardening with regular review

Incident Response and Recovery

- Structure, roles and responsibilities of the dedicated incident response team
- Procedures for mitigating the impact of an incident, investigating the causer and resumption of normal operation
- Review on its emergency response plan at least once every two years, or when any material changes arise

Security Assessment

- Risk assessment (vulnerability assessment and penetration test) at least once every year and submit report to Commissioner's Office
- Audit at least once every two year and submit report to Commissioner's Office
- Participate drill test by Commissioner's Office at least once every two years

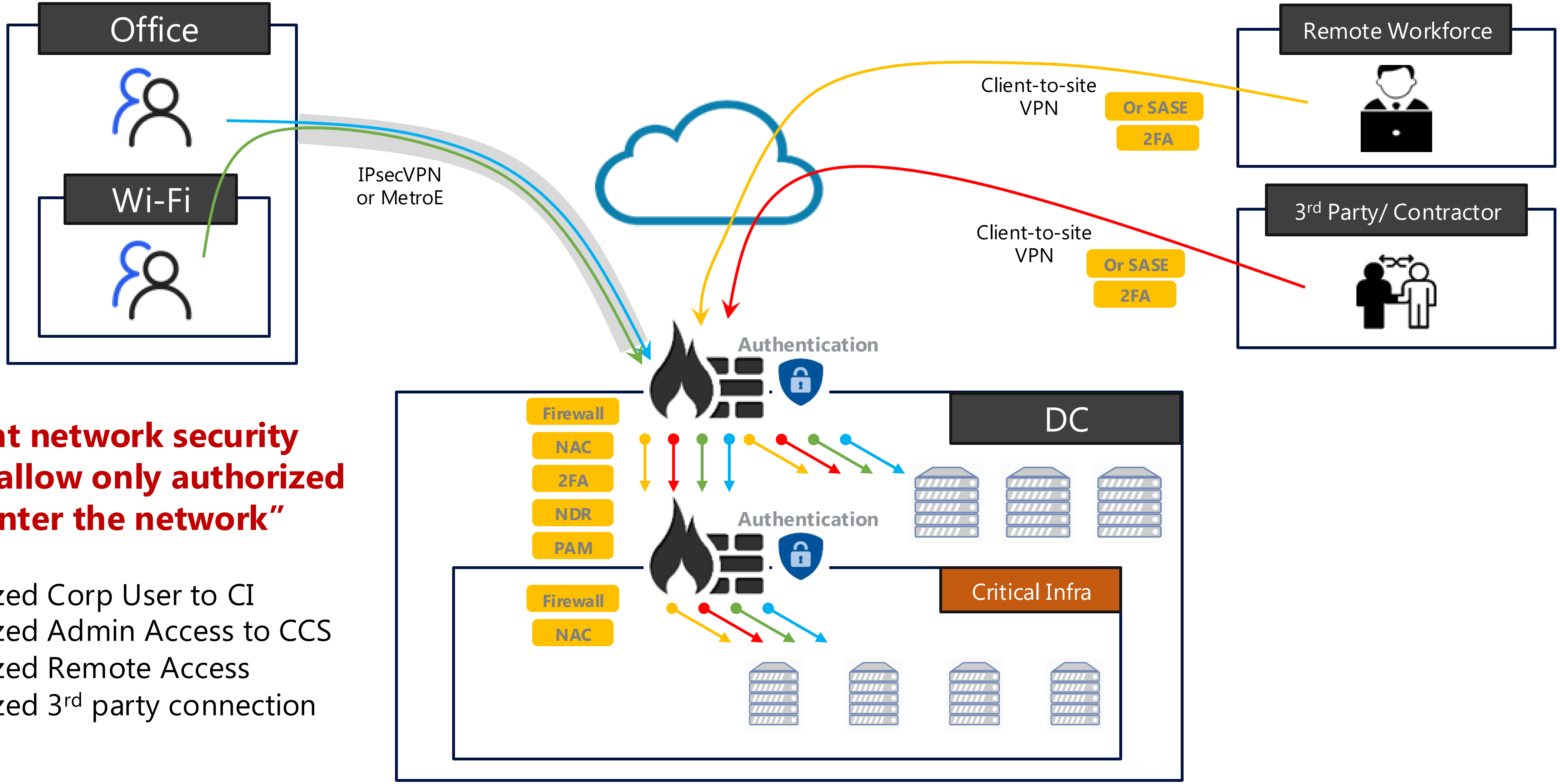
Qualification & Training

- Critical infrastructure must be supervised by dedicated and certified supervisor (or dedicated supervisor with certified service provider)
- Training programs on various computer system security approaches

Network Security Control for Critical Infrastructure

HKBN ENTERPRISE SOLUTIONS

Zero-Trust Network Access (ZTNA) Architecture



"Implement network security control to allow only authorized traffic to enter the network"

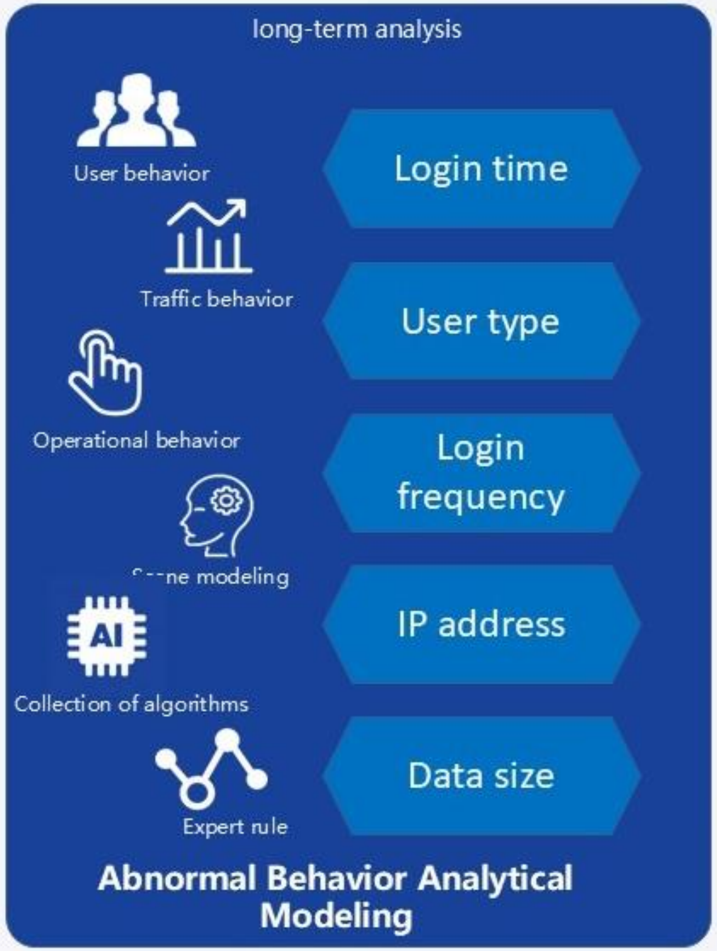
1. Authorized Corp User to CI
2. Authorized Admin Access to CCS
3. Authorized Remote Access
4. Authorized 3rd party connection

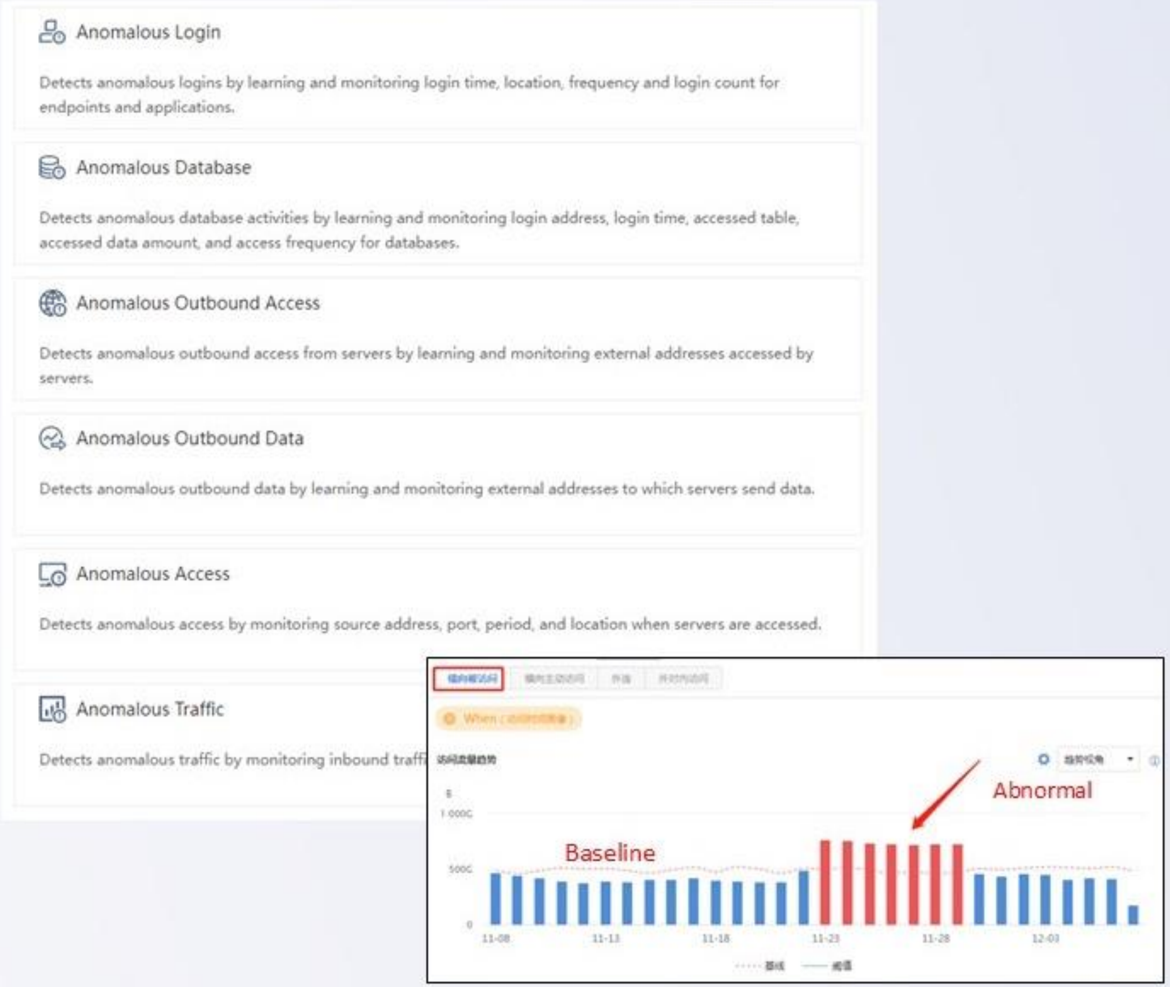
Highlights of the Legislative Framework

Governance	• Adopt a "Security by Design" Approach • Data access right • Backup and recovery policies to ensure the resilience of the system;
Identification	• Identify organization, authority, roles and responsibilities of the computer system security management unit • Privileged access management to ensure that personnel only have access to the specific administrative capabilities needed • Up-to-date inventory of CCS and other associated assets are properly owned, kept and maintained, and restricted for access
Protection	• Implement network security control to allow only authorized traffic to enter the network • Appropriate policies and procedures for remote connection
Detection	• **Establish a monitoring and detection mechanism and define a baseline of normal behavior** • **Conduct Regular review of the monitoring mechanism** • System hardening with regular review
Incident Response and Recovery	• Structure, roles and responsibilities of the dedicated incident response team • Procedures for mitigating the impact of an incident, investigating the causer and resumption of normal operation • Review on its emergency response plan at least once every two years, or when any material changes arise
Security Assessment	• Risk assessment (vulnerability assessment and penetration test) at least once every year and submit report to Commissioner's Office • Audit at least once every two year and submit report to Commissioner's Office • Participate drill test by Commissioner's Office at least once every two years
Qualification & Training	• Critical infrastructure must be supervised by dedicated and certified supervisor (or dedicated supervisor with certified service provider) • Training programs on various computer system security approaches

Baseline Monitoring

Establish a monitoring and detection mechanism and define a baseline of normal behavior





Anomalous Login

Detects anomalous logins by learning and monitoring login time, location, frequency and login count for endpoints and applications.

Anomalous Database

Detects anomalous database activities by learning and monitoring login address, login time, accessed table, accessed data amount, and access frequency for databases.

Anomalous Outbound Access

Detects anomalous outbound access from servers by learning and monitoring external addresses accessed by servers.

Anomalous Outbound Data

Detects anomalous outbound data by learning and monitoring external addresses to which servers send data.

Anomalous Access

Detects anomalous access by monitoring source address, port, period, and location when servers are accessed.

Anomalous Traffic

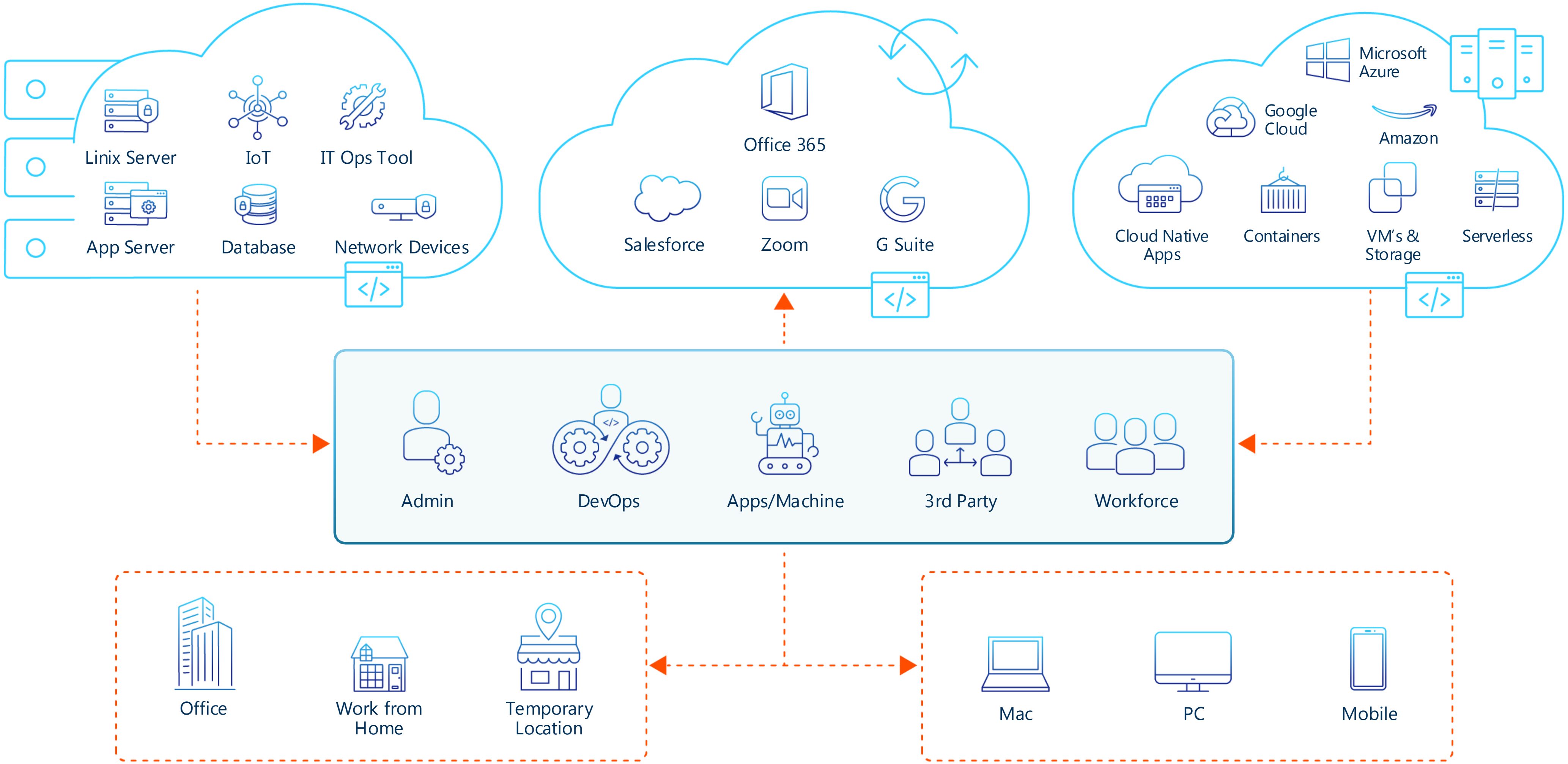
Detects anomalous traffic by monitoring inbound traffi

Highlights of the Legislative Framework

Governance	• Adopt a "Security by Design" Approach • Data access right • Backup and recovery policies to ensure the resilience of the system;
Identification	• Identify organization, authority, roles and responsibilities of the computer system security management unit • **Privileged access management to ensure personnel only have access to the specific admin. capabilities needed** • Up-to-date inventory of CCS and other associated assets are properly owned, kept and maintained, and restricted for access
Protection	• Implement network security control to allow only authorized traffic to enter the network • Appropriate policies and procedures for remote connection
Detection	• Establish a monitoring and detection mechanism and define a baseline of normal behavior • Conduct Regular review of the monitoring mechanism • System hardening with regular review
Incident Response and Recovery	• Structure, roles and responsibilities of the dedicated incident response team • Procedures for mitigating the impact of an incident, investigating the causer and resumption of normal operation • Review on its emergency response plan at least once every two years, or when any material changes arise
Security Assessment	• Risk assessment (vulnerability assessment and penetration test) at least once every year and submit report to Commissioner's Office • Audit at least once every two year and submit report to Commissioner's Office • Participate drill test by Commissioner's Office at least once every two years
Qualification & Training	• Critical infrastructure must be supervised by dedicated and certified supervisor (or dedicated supervisor with certified service provider) • Training programs on various computer system security approaches

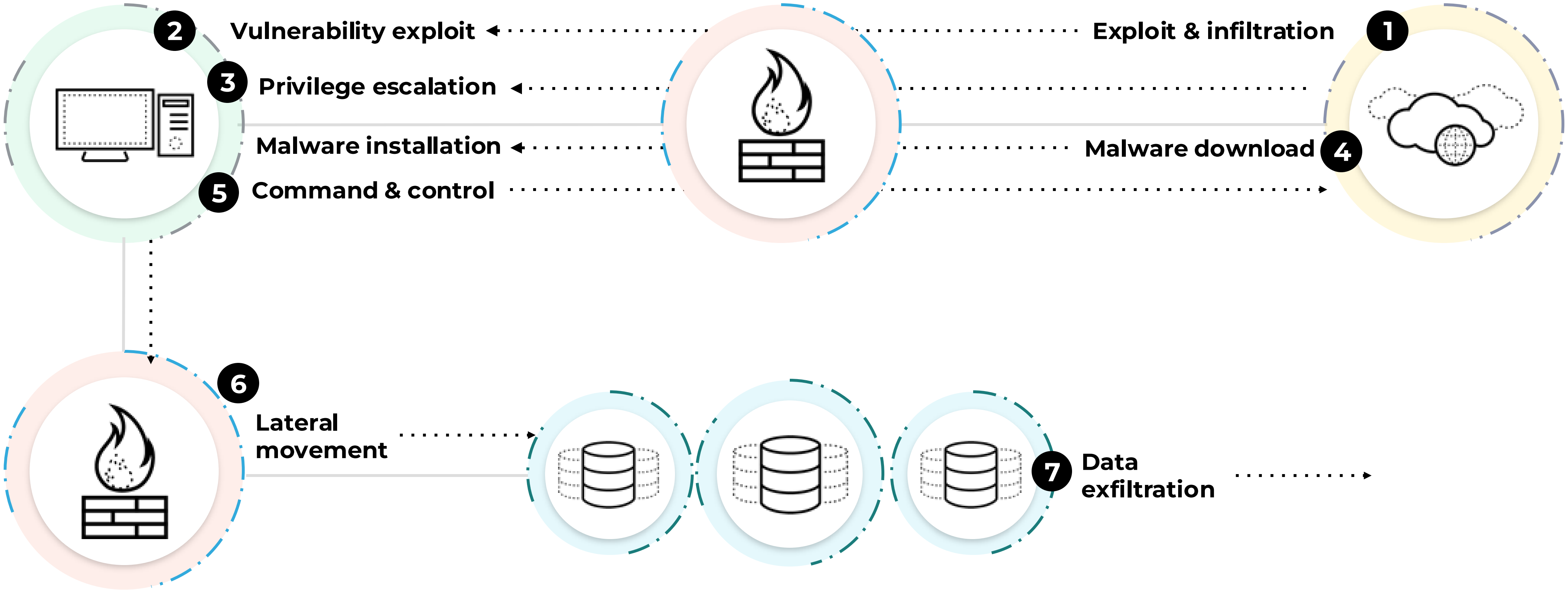
Privilege is everywhere.

All identities can become privileged under certain conditions.

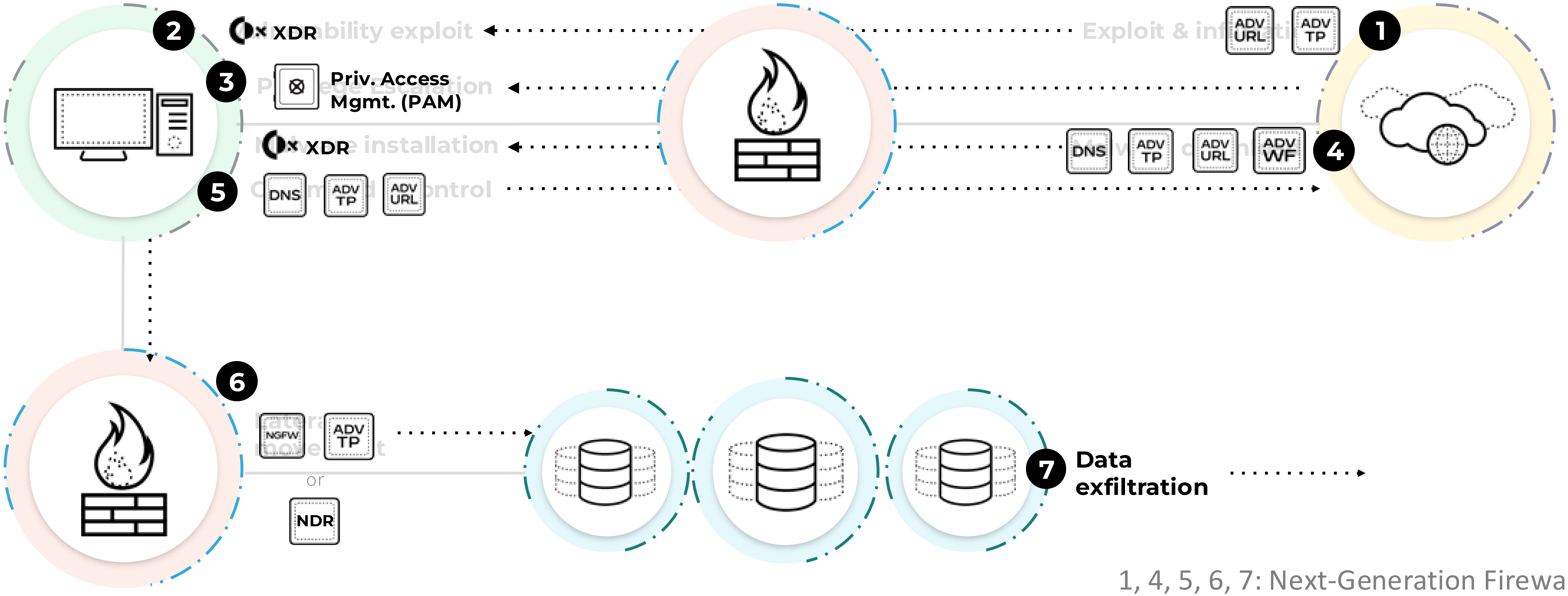


Typical Attack Lifecycle

HKBN
ENTERPRISE SOLUTIONS



Multi-Layer Defense across Attack Lifecycle



1, 4, 5, 6, 7: Next-Generation Firewall

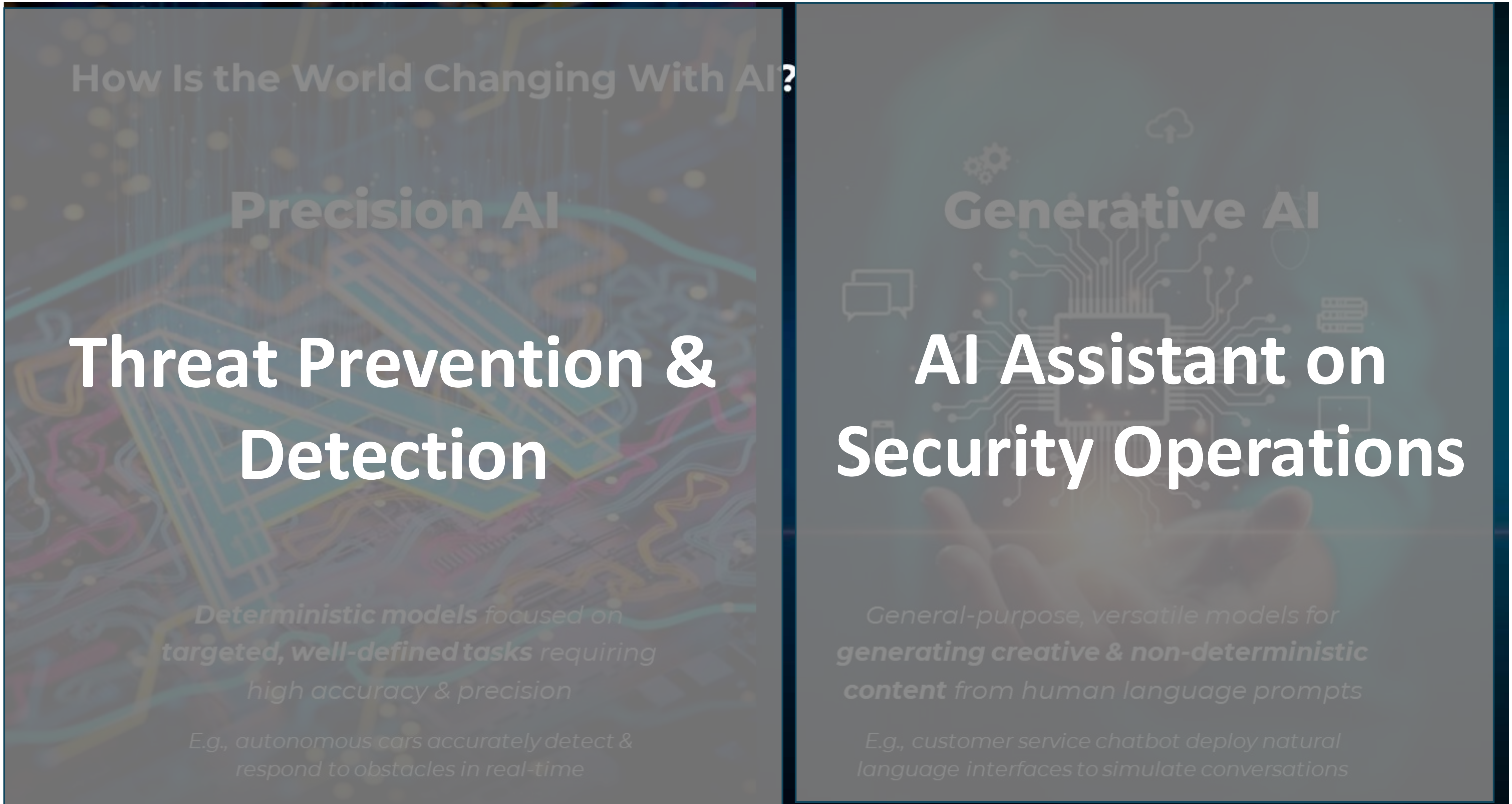
2, 4: EDR / XDR

3: Privilege Access Security (PAM)

6: Network Detect & Response (NDR)

7: Data Loss Prevention / Database Firewall

How AI assists in Cyber Defense



How Is the World Changing With AI?

Precision AI

***Deterministic models** focused on **targeted, well-defined tasks** requiring high accuracy & precision*

E.g., autonomous cars accurately detect & respond to obstacles in real-time

Generative AI

*General-purpose, versatile models for **generating creative & non-deterministic content** from human language prompts*

E.g., customer service chatbot deploy natural language interfaces to simulate conversations

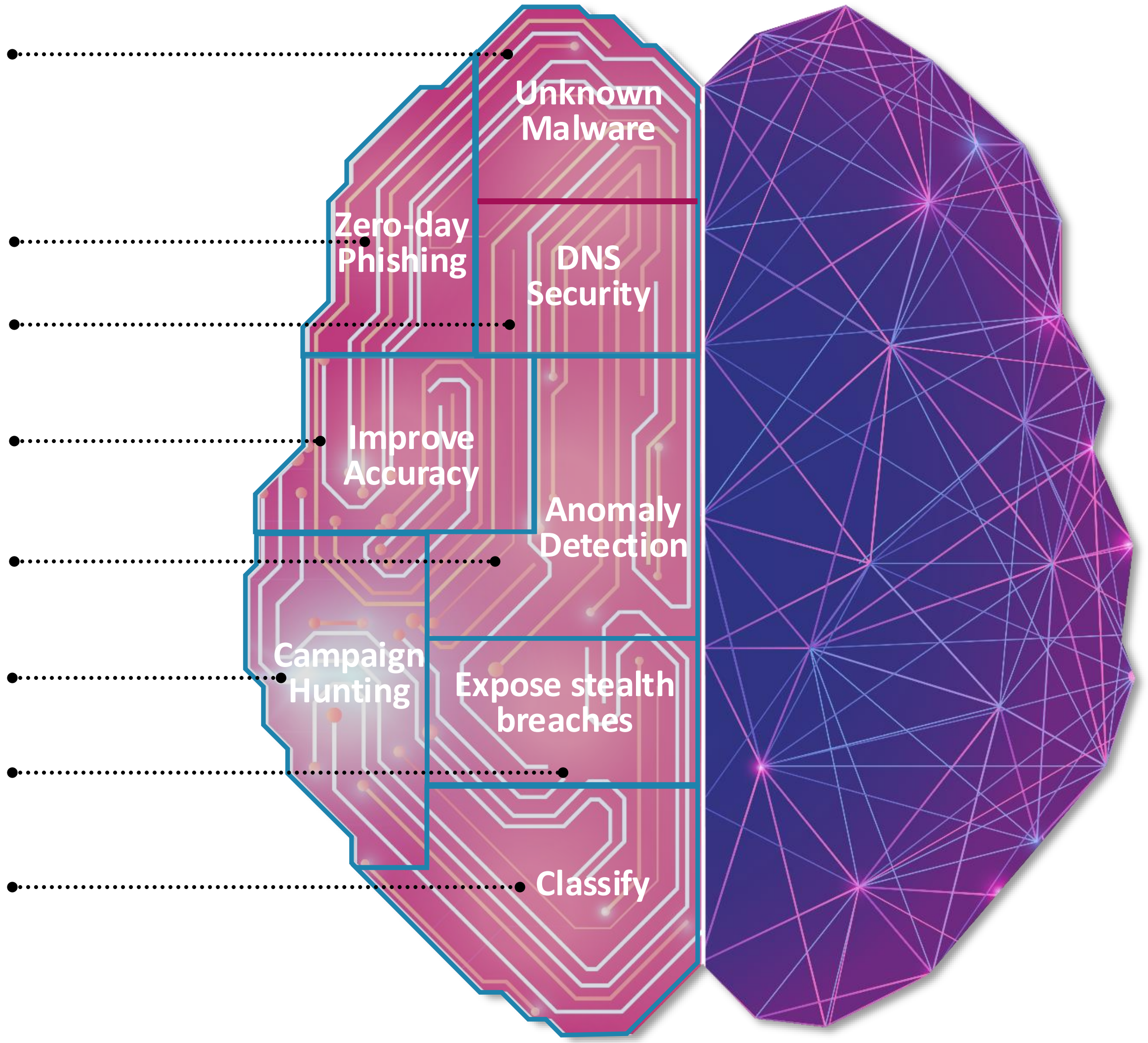
Threat Prevention & Detection

AI Assistant on Security Operations

AI-based technologies leveraged by ThreatCloud

HKBN
ENTERPRISE SOLUTIONS

50+ engines across different security functionality

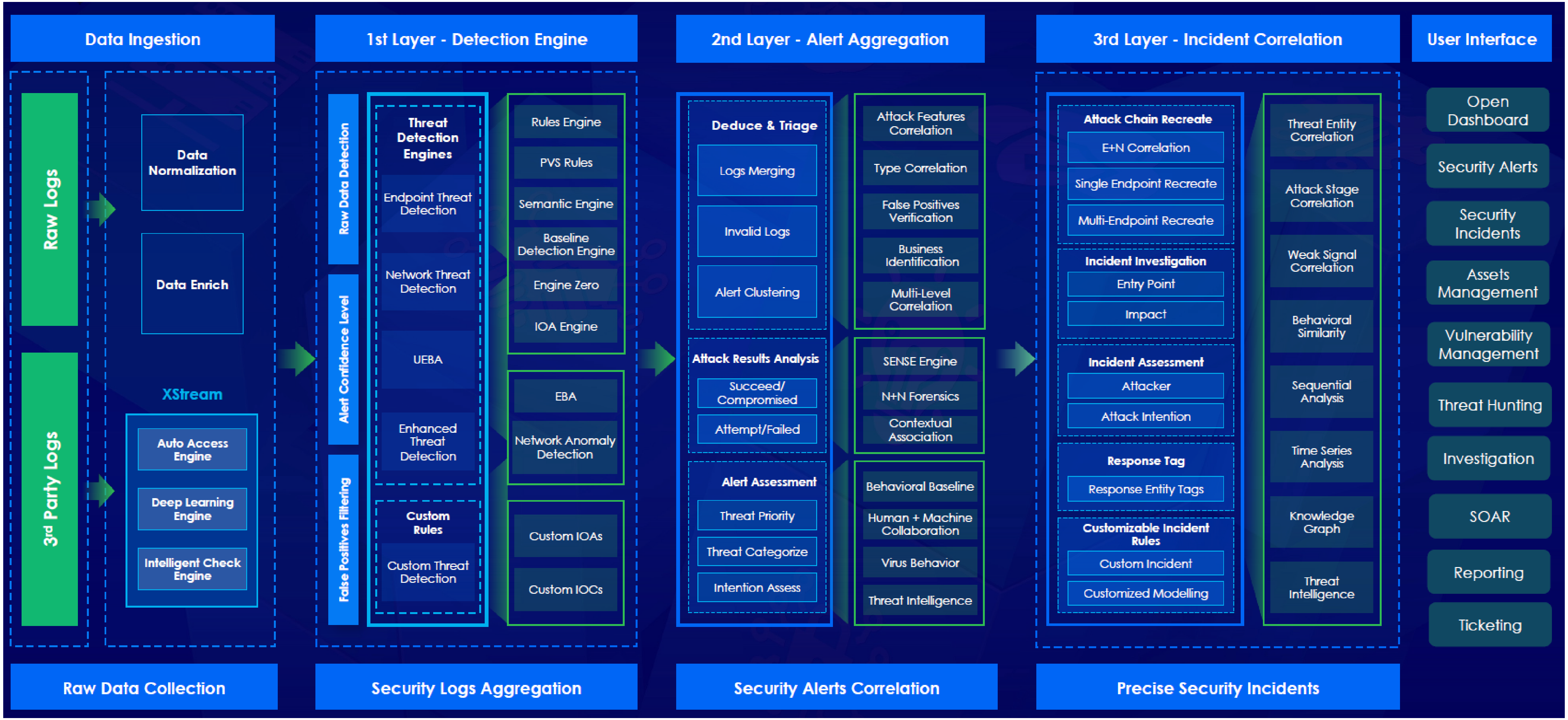


Infected hosts detection Sandbox static analysis executables Sandbox static analysis documents Sandbox static analysis macros Sandbox dynamic analysis	Unknown Malware
Email static analysis Network zero-phishing detection Mobile zero-phishing detection Anti-Phishing AI engine HTML body NLP	Zero-day Phishing
DNS Tunneling DNS Slow tunneling DGA Domain Generation Algorithm	DNS Security
Network AI engines aggregator Mobile AI engines aggregator Machine validated signature	Improve Accuracy
Cloud networks anomaly detection XDR/XPR user behavior analysis SSH tunneling	Anomaly Detection
ThreatCloud Campaign Hunting	Campaign Hunting
Analyst Mind Malicious activity detection	Expose stealth breaches
Documents meta classifier Vectorization family classifier XDR/XPR incidents aggregation ML Similarity Model MRAT Classifier IP Port	Classify

Slide from Check Point Software Technologies Ltd.

XDR Architecture with AI engines

HKBN
ENTERPRISE SOLUTIONS



Data Ingestion

Raw Logs

3rd Party Logs

Data Normalization

Data Enrich

XStream

Auto Access Engine

Deep Learning Engine

Intelligent Check Engine

Raw Data Collection

1st Layer - Detection Engine

Raw Data Detection

Alert Confidence Level

False Positives Filtering

Threat Detection Engines

- Endpoint Threat Detection
- Network Threat Detection
- UEBA
- Enhanced Threat Detection

Rules Engine

PVS Rules

Semantic Engine

Baseline Detection Engine

Engine Zero

IOA Engine

EBA

Network Anomaly Detection

Custom Rules

- Custom Threat Detection

Custom IOAs

Custom IOCs

Security Logs Aggregation

2nd Layer - Alert Aggregation

Deduce & Triage

- Logs Merging
- Invalid Logs
- Alert Clustering

Attack Features Correlation

Type Correlation

False Positives Verification

Business Identification

Multi-Level Correlation

Attack Results Analysis

- Succeed/ Compromised
- Attempt/Failed

SENSE Engine

N+N Forensics

Contextual Association

Alert Assessment

- Threat Priority
- Threat Categorize
- Intention Assess

Behavioral Baseline

Human + Machine Collaboration

Virus Behavior

Threat Intelligence

Security Alerts Correlation

3rd Layer - Incident Correlation

Attack Chain Recreate

- E+N Correlation
- Single Endpoint Recreate
- Multi-Endpoint Recreate

Incident Investigation

- Entry Point
- Impact

Incident Assessment

- Attacker
- Attack Intention

Response Tag

- Response Entity Tags

Customizable Incident Rules

- Custom Incident
- Customized Modelling

Threat Entity Correlation

Attack Stage Correlation

Weak Signal Correlation

Behavioral Similarity

Sequential Analysis

Time Series Analysis

Knowledge Graph

Threat Intelligence

Precise Security Incidents

User Interface

Open Dashboard

Security Alerts

Security Incidents

Assets Management

Vulnerability Management

Threat Hunting

Investigation

SOAR

Reporting

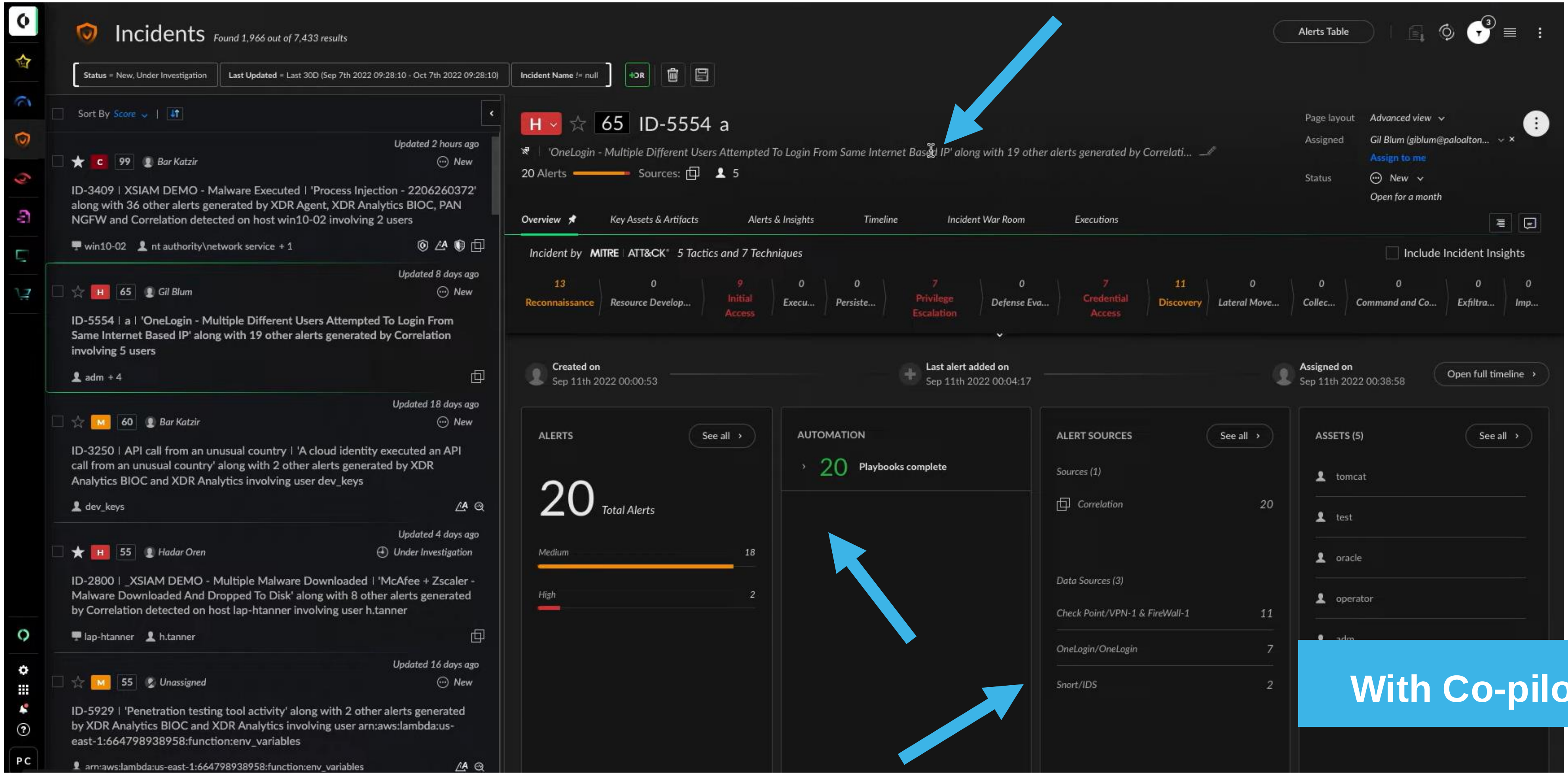
Ticketing

Slide from Sangfor Technologies Ltd.

AI-driven Security Operations Platform

HKBN
ENTERPRISE SOLUTIONS

Sample Use Case: Multiple User Login attempt from same source along with other alerts



Incidents Found 1,966 out of 7,433 results

Status = New, Under Investigation | Last Updated = Last 30D (Sep 7th 2022 09:28:10 - Oct 7th 2022 09:28:10) | Incident Name != null

Sort By Score

Updated 2 hours ago
C 99 Bar Katzir — New
ID-3409 | XSIAM DEMO - Malware Executed | 'Process Injection - 2206260372' along with 36 other alerts generated by XDR Agent, XDR Analytics BIOC, PAN NGFW and Correlation detected on host win10-02 involving 2 users
win10-02 nt authority\network service + 1

Updated 8 days ago
H 65 Gil Blum — New
ID-5554 | a | 'OneLogin - Multiple Different Users Attempted To Login From Same Internet Based IP' along with 19 other alerts generated by Correlation involving 5 users
adm + 4

Updated 18 days ago
M 60 Bar Katzir — New
ID-3250 | API call from an unusual country | 'A cloud identity executed an API call from an unusual country' along with 2 other alerts generated by XDR Analytics BIOC and XDR Analytics involving user dev_keys
dev_keys

Updated 4 days ago
H 55 Hadar Oren — Under Investigation
ID-2800 | _XSIAM DEMO - Multiple Malware Downloaded | 'McAfee + Zscaler - Malware Downloaded And Dropped To Disk' along with 8 other alerts generated by Correlation detected on host lap-htanner involving user h.tanner
lap-htanner h.tanner

Updated 16 days ago
M 55 Unassigned — New
ID-5929 | 'Penetration testing tool activity' along with 2 other alerts generated by XDR Analytics BIOC and XDR Analytics involving user arn:aws:lambda:us-east-1:664798938958:function:env_variables
arn:aws:lambda:us-east-1:664798938958:function:env_variables

H 65 ID-5554 a

'OneLogin - Multiple Different Users Attempted To Login From Same Internet Based IP' along with 19 other alerts generated by Correlati...

20 Alerts Sources: 5

Page layout: Advanced view
Assigned: Gil Blum (giblum@paloalton...
Assign to me
Status: New
Open for a month

Incident by MITRE | ATT&CK® 5 Tactics and 7 Techniques

☐ Include Incident Insights

13	0	9	0	0	7	0	7	11	0	0	0	0	0
Reconnaissance	Resource Develop...	Initial Access	Execu...	Persiste...	Privilege Escalation	Defense Eva...	Credential Access	Discovery	Lateral Move...	Collec...	Command and Co...	Exfiltra...	Imp...

Created on Sep 11th 2022 00:00:53
Last alert added on Sep 11th 2022 00:04:17
Assigned on Sep 11th 2022 00:38:58

ALERTS
20 Total Alerts
Medium 18
High 2

AUTOMATION
20 Playbooks complete

ALERT SOURCES
Sources (1)
Correlation 20
Data Sources (3)
Check Point/VPN-1 & FireWall-1 11
OneLogin/OneLogin 7
Snort/IDS 2

ASSETS (5)
tomcat
test
oracle
operator
adm

With Co-pilot to assist you

Screenshot from Palo Alto Networks Cortex XSIAM

Latest Example on GenAI in Cybersecurity

Alvin Chun

Assistant Vice President
of Sales Engineering

Contact us: es-enquiry@hkbn.com.hk

HKBN Enterprise Solutions

Organizational Functional structure of the holding
PROGRESSION

Thank you