RALFKAIROS

CYBERSECURITY ASIAN PROVIDER

ADD. 103-401 460 Hongeun-dong,
Seodaemun-gu, Seoul, Poonglim I-ONE
South Korea, 03600 | 010-2030-7493 |
contact@ralfkairos.com |
www.ralfkairos.com

RK Europe
85 rue de Saussure
75017 Paris | +33 6 45 75 96 15 |
marc@ralfkairos.com |
www.purplehackademy.com

RALFKAIROS IDENTITY

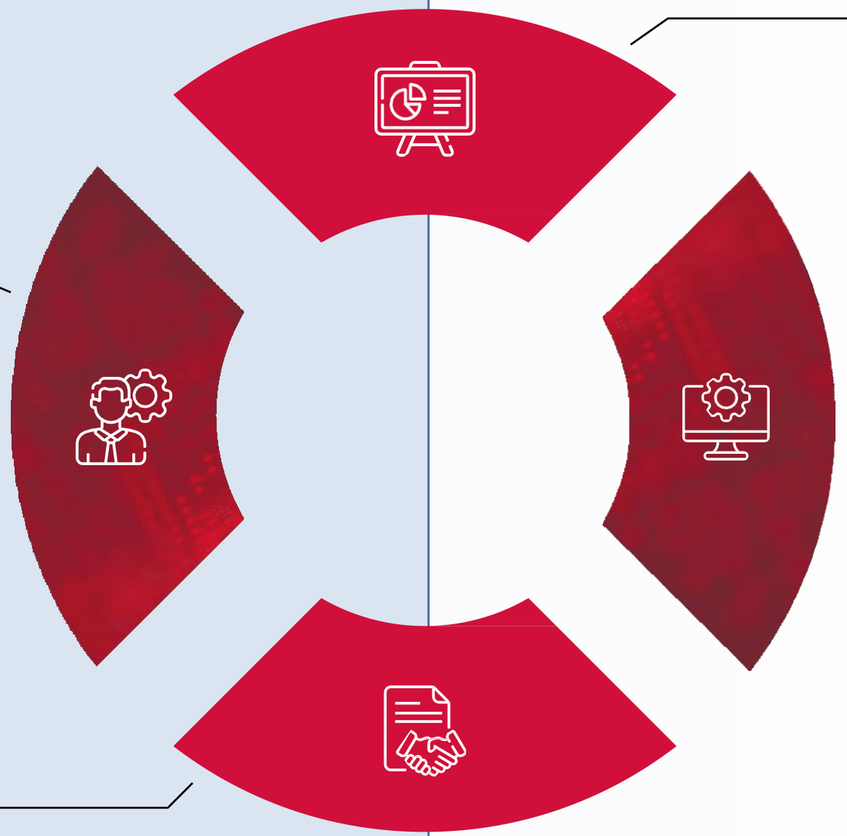
- Independent, pure player, 100% dedicated to Cyber since 2015 in Korea
- Consulting Services in Cybersecurity, IT audit, Forensic investigation, Compliance and training
- European trusted certified expertise
- Lectures in Korea for executive business members at KITRI, EU, ECCK, FKCCI, la French Tech
- Entry point for addressing security needs, from fraud audit to continuous penetration test, bugbounty, remediation, IT security architecture
- 20+ year experience in high-grade cyber defence for customers

RALFKAIROS SERVICES PORTFOLIO

50% Security Training & Lectures

30% Consulting

- Risk Management Review IT
- Security Audit Forensic
- Configuration and deployment



20% CISO Assistance

- Cyber maturity review
- Incident response report
- Project Management

Partnerships

- Red Team, Bug bounty, IT Infrastructure

COMMERCIAL OFFERS

I. Penetration Test

II. Training & BootCamp

III. Security Audit

COMMERCIAL OFFERS

I. PENETRATION TEST

<Trying to compromise your digital assets with ethical hackers to identify your vulnerabilities>

The Goal

To improve information security awareness

To assess risk

To mitigate risk immediately

To reinforce the IS process

To assist in decision making processes

INPUT = website, api, network architecture etc…
OUTPUT = vulnerability report, wrap up meeting, remediation actions

COMMERCIAL OFFERS

I. PENETRATION TEST

- **Internal testing**

  carried out while connected directly or close to the network under test, on either ‘full knowledge’ or ‘zero knowledge’ engagements.

  The purpose is to demonstrate that an IT system has been configured in a manner that makes it as secure as possible.

- **Internet testing**

  “black box” (zero-knowledge) approach and is often used to understand what target information attackers can discover from the Internet and other public domain resources.

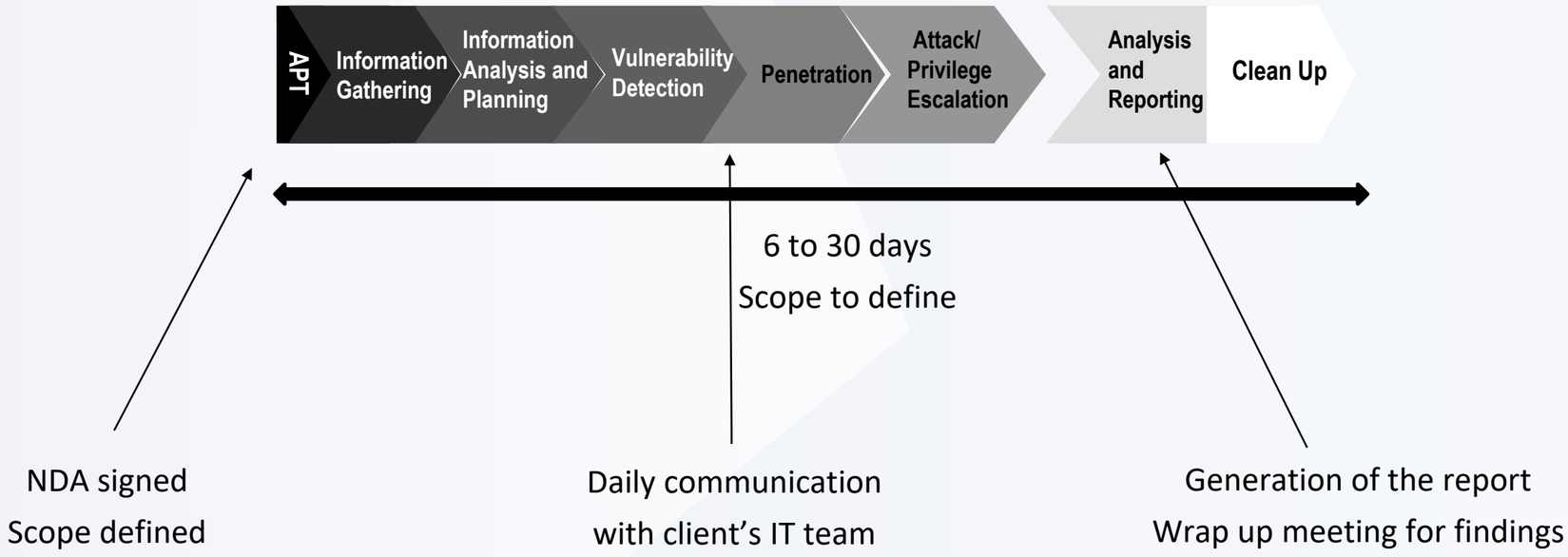
- **Remote testing** is conducted from external networks to which the IT system is connected.

  There is generally some sort of perimeter security, for example, a firewall or filtering router that is designed to limit the access available from a given external network to the IT system under test.

- **Web application testing** ensures that an application has been configured securely so that attackers cannot gain unauthorized access to it or its data; users cannot access data for which they are not authorized; and there are no vulnerabilities that users can leverage to gain access to services outside of their restricted operating environment.

COMMERCIAL OFFERS

I. PENETRATION TEST



International norms for ethical hacking

COMMERCIAL OFFERS

II. TRAINING & BOOTCAMP

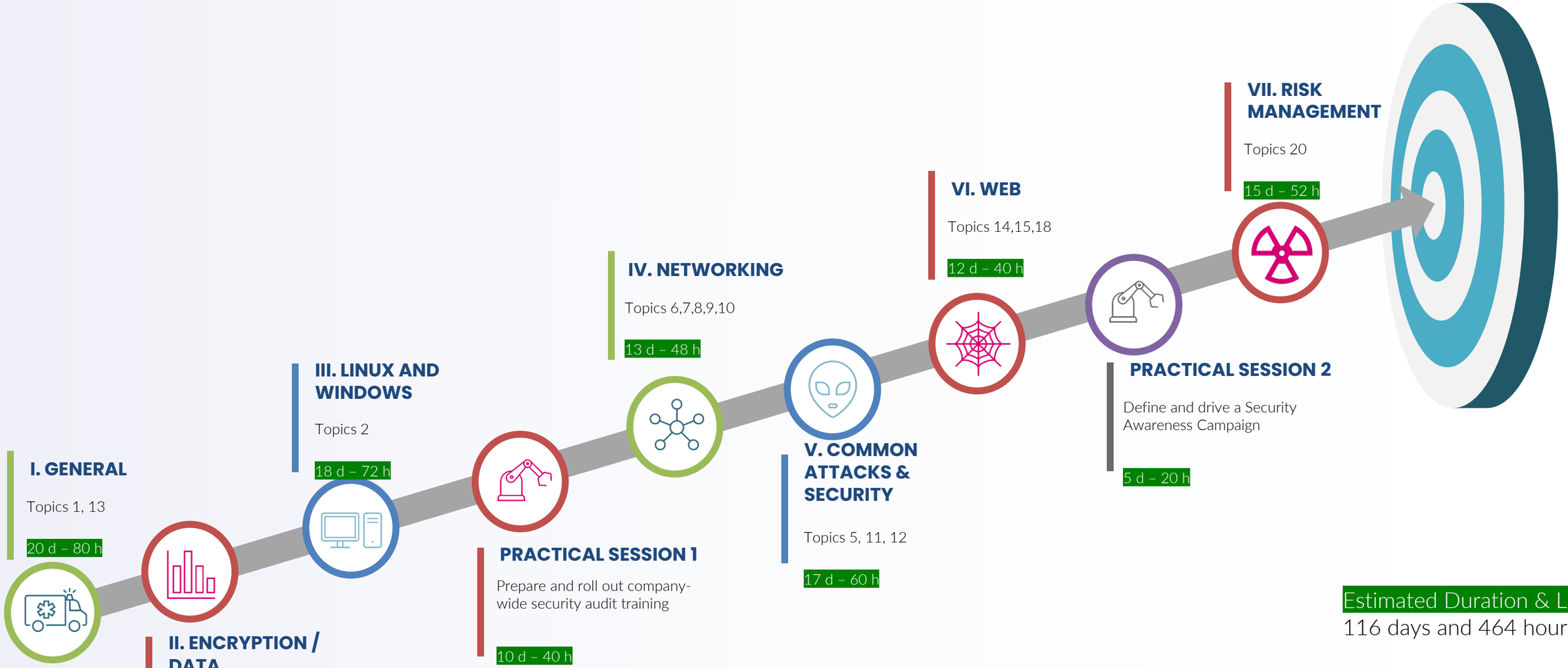
A module-based cybersecurity BOOTCAMP with an adapted curriculum suited to your objectives and public

20 Modules, + 300 hours of courses and workshops, transform your workforce into professionals !

- 1. INTRODUCTION TO CYBERSECURITY
- 2. OS FUNDAMENTALS AND SECURITY
- 3. REGULATION, COMPLIANCE AND RISK MANAGEMENT
- 4. INTRODUCTION TO NETWORK SECURITY
- 5. PACKET INSPECTION AND ATTACK AGAINST AVAILABILITY
- 6. NETWORK SECURITY IN ETHICAL HACKING
- 7. NETWORK ACCESS CONTROL, SIEM TOOLS AND ADDITIONAL SECURITY MEASURES
- 8. CRYPTOGRAPHIC KEY MANAGEMENT, PKI, AND DIGITAL SIGNATURES
- 9. IDENTITY ACCESS MANAGEMENT
- 10. CLOUD APPLICATION SECURITY
- 11. DIGITAL FORENSICS
- 12. DATA AND DATABASE SECURITY
- 13. SECURED NETWORKS SYSTEM WITH FIREWALL
- 14. ETHICAL HACKING AND ADVANCED CONCEPTS IN CYBERSECURITY
- 15. CRYPTOGRAPHY AND ENCRYPTION
- 16. INTRODUCTION TO APPLICATION SECURITY
- 17. ATTACKS ON IDENTITY & PHISHING
- 18. WEB-BASED APPLICATIONS AND VULNERABILITIES
- 19. PENETRATION TESTING & OWASP, FUZZING
- 20. WEB SECURITY, COOKIES AND TRACKING

COMMERCIAL OFFERS

II. TRAINING & BOOTCAMP



I. GENERAL

Topics 1, 13

20 d – 80 h

II. ENCRYPTION / DATA

Topics 3, 4, 16

6 d – 24 h

III. LINUX AND WINDOWS

Topics 2

18 d – 72 h

PRACTICAL SESSION 1

Prepare and roll out company-wide security audit training

10 d – 40 h

IV. NETWORKING

Topics 6,7,8,9,10

13 d – 48 h

V. COMMON ATTACKS & SECURITY

Topics 5, 11, 12

17 d – 60 h

VI. WEB

Topics 14,15,18

12 d – 40 h

PRACTICAL SESSION 2

Define and drive a Security Awareness Campaign

5 d – 20 h

VII. RISK MANAGEMENT

Topics 20

15 d – 52 h

Estimated Duration & Load

116 days and 464 hours

COMMERCIAL OFFERS

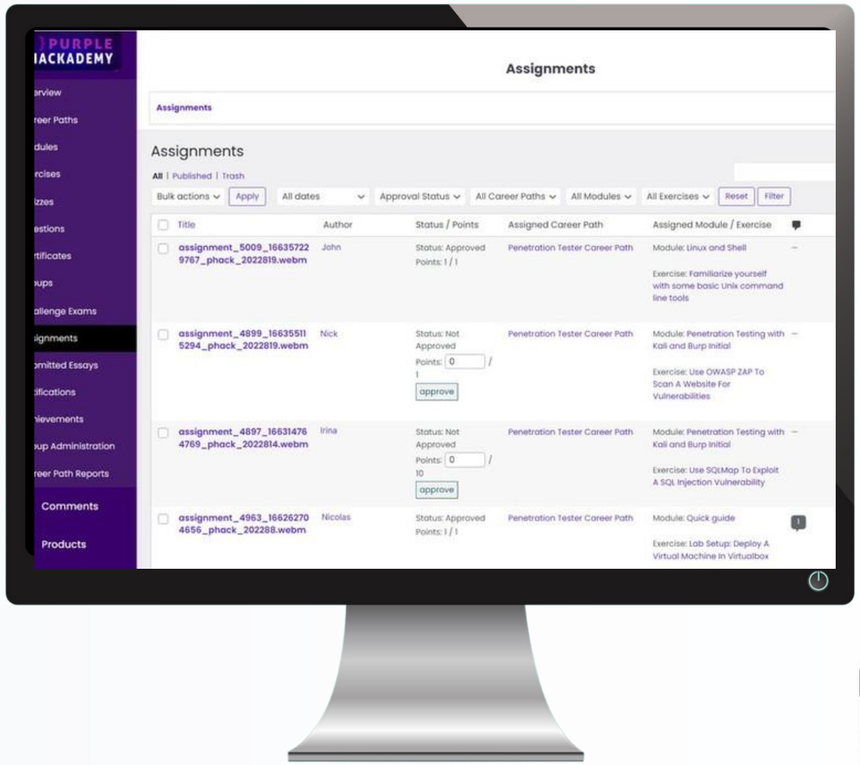
II. TRAINING & BOOTCAMP

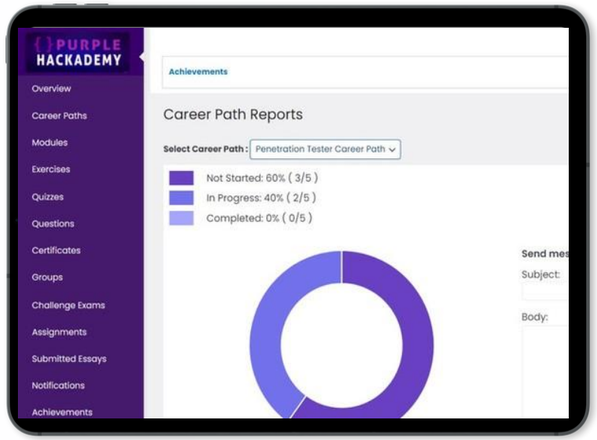
PRESENTATION

How to become a cybersecurity professional with Live online training ?

Hundreds of practical exercises extracted from real job tasks, virtual labs, experimental tools, practice tests, resources, assessments and certifications upon completing the course.

Purple Hackademy is a platform prepared by RALFKAIROS company. We are cybersecurity company, based in Seoul and Paris, providing hands-on, vendor-independent quality assurance and consulting cybersecurity services.





COMMERCIAL OFFERS

II. TRAINING & BOOTCAMP

Penetration Tester Exam

Duration: 5 hours

A penetration test, or a pen test, is a simulated cyber assault on your computer system designed to detect exploitable flaws.

Assess Technical skills, Problem-Solving skills & Communication with our test

Ensure that your new employees can improve your overall organization's security posture

Pentester Path

Duration: 200 hours

To get a better idea of what Ethical Hacking is, it is important to first understand what hacking actually is. Unlike malicious hacking, where a hacker could cause harm to your computer system, this form of hacking entails the use of computer programs and resources to gain unauthorized access into a computer system by exploiting weaknesses or vulnerabilities.

SOC Analyst Career Path

Duration: 170 hours

Become a SOC Analyst (CSA) - a cybersecurity professional who monitors and detects potential threats, triages the alerts and appropriately escalates them. A SOC is a service where you can find Security Event and Log Analysts (SOC), Incident Responders (CSIRT), Threat intelligence (CERT)

Chief Information Security Officer Career Path

Duration: custom

Upskill a CISO, or an executive in an organization who oversees the protection of information and data. A CISO is responsible for developing the vision, strategy, and program that will protect a company's data assets and technologies.

Chief information security officers can find employment in all kinds of organizations, including private firms, governmental bodies, and NGOs.

Contact us

COMMERCIAL OFFERS

III. SECURITY AUDIT

INITIAL SITUATION

STATUS:

- ✗ **No risks assessment**
- ✗ **No policy or no review**
- ✗ **IT management without strong security**
- ✗ **«Oral» incident plan**
- ✗ **Unknown vulnerabilities**
- ✗ **Ransomware or compromission threats**

STARTER TECHNICAL INSPECTION

Survey 25 Control Points | Action plan

OUTPUT:

- ☑ **Healthcheck report including**
- ☑ **Action plan**
- ☑ **Score based on categories**
- ☑ **Best practices**
- ✗ **No follow-up**
- ☑ **4 documents provided:**
  User policy, security policy, architecture document, template, dashboard template

2h onsite 3h offsite

SUPPORTED TECHNICAL INSPECTION

Survey 30 Control Points | Action plan | Follow up Training

OUTPUT:

- ☑ **Healthcheck report including Action plan**
- ☑ **Wrap Up meeting and best practices**
- ☑ **+ 2h Follow-up meeting after action plan 6**
- ☑ **documents reviewed or provided**:
  User policy, security policy, architecture document template, dashboard template, 3rd party contractor, Compliance certification 1-year delivery

6h onsite 6h offsite

COMMERCIAL OFFERS

III. SECURITY AUDIT

30 control points – 5 categories


Data Privacy


Incident Management


Monitoring Controls


Patch Management


Physical Security

45 min IT manager
30 min CFO / COO /CEO
45 min visit Cloud infrastructure
30 min interview user
2h30 on site IT & Risk
1h awareness training review

Healthcheck report including Action plan – wrap up meeting (1h30)

+ 2h Follow-up meeting after action plan (contre visite)

6 documents provided: user policy, security policy, architecture document, template, dashboards template, 3rd party contractor

- **Analysis of survey**
- **Review of existing**
- **Documentation:** architecture, backup, incident, IT operations, Clients PII management

COMMERCIAL OFFERS

III. SECURITY AUDIT

1 Setting the stage

Explanation email sent to client
Fine tuning of the survey adapted to the target
Survey sent to counterparts
List of documents sent to client
Kickoff meeting (optional)

2 Survey and Documentation Review

Client fill survey
Survey is analyzed
Documentation is received and analyzed
Additional questions are sent (optional)

3 On site IT review

Interviews with IT manager, CFO/CFO/COO/CEO
Inspection of Cloud infrastructure and other facilities
Clients PII general assessment
User interview (supported inspection only)

4 Delivery and Wrap-up

Healthcheck report including Action plan
Wrap-up meeting
Sample documents provided
Follow-up meeting (supported inspection only)
Awareness training

COMMERCIAL OFFER

III. SECURITY AUDIT

LIST OF CONTROL POINTS

Domain	Control Point	25 or 30 control points	Example / Procedure to be conducted (to be completed by MdS)
General Information			
0	Name of Client	3i inc.	
0,1	Brief description of the client and services	TBD	
1-Data Privacy :IT Supplier Contract Management, Cloud Services and Other Sub-Contractors			
10	Which legal jurisdiction governs the entity and the data stored?	25	e.g. Korean, European, etc. Do you comply with PIPA, GDPR?
11	Does the contract between Client and the Supplier contain security requirements ?	25	e.g. the right to audit, passwords, encryption, secure exchange of information, disposal requirements
12	What Client information / types of data will the Supplier be accessing (receiving, storing, processing or transmitting)?	25	e.g. Customer Data; Logistic Data; Intellectual Property; Credit Card Data; Human Resources Data; Marketing Data; Corporate or Financial Data; Physical Security Data; IT Infrastructure Data; Personal Data; Other Data
13	Is the Information Security Policy available?	25	Please provide documentation
14	Do you use cloud services ?	25	public or private cloud
15	[redacted]	25	e.g. design, legal, compliance, finance
15,1	What technical security controls are in place?	25	e.g. IDS, IPS, application firewalls
15,2	[redacted]	25	
16	[redacted]	25	
16,1	What actions are in place to prevent unauthorized viewing of customer information?	25	
16,2	[redacted]	25	
16,3	What security certifications does each sub-contractor have?	25	
17	Do you monitor and review the services provided by the sub-contractors?	25	
17,1	Do you do audits on the sub-contractors?	30	If yes. Provide audit report
2-Incident Management, Backup Procedures and Business Continuity			
3-Physical Security, HR Security and Access Controls			
	How is physical access managed?	25	

COMMERCIAL OFFER

III. SECURITY AUDIT

ISS06	Insufficient Data Access Management		
Description	PII are not properly identified and more generally so are business sensitive data. Although there is a certain level of protection to access those data (logical access based on password), there is no single sign-on and no directory management. Also there is no periodic review of rights to the system and network. SaaS shared accounts and passwords are stored in a software purchase ledgers file.		
Risk Level	High	Impact	Major
Risks Associated	User accounts left open to public Unauthorized access to data Unauthorized handling of data These two risks can lead to business disadvantages (loss/theft of source code) and to company reputation (to clients and investors)		
Supporting Evidence	Interviews with executive and officers at XXX. No review of access rights, no history of incidents Equipment and software purchase ledgers		

Recommendation	- Optimize identity and access management to treat identity as the primary security perimeter :
	  - Elaborate, distribute and enforce of an identification/ password policy : the password requirement should comply with latest good practices (n-factors, rotation, history, complexity)
	  - Centralize sign-on and account directory management with an identity and authentication solution like **Jamf** or **Fleetsmith**
	  - Grant minimum access rights needed to perform duties.
	  - Timely deactivate access of employees leaving the organization.
	  - Review periodically access rights, including appropriateness. Review of bucket access rights in AWS
	- Protect data in its different states :
	  - At rest: This includes all information storage objects, containers and types that exist statically on physical media - magnetic or optical disks. e.g : encryption
	  - In transit: When data is being transferred between components, locations, or programs, it's in transit. Examples are transfer over the network, from on-site premises to the cloud and vice-versa. e.g : vpn, email, database
	- Maintain control of keys that access and encrypt your data. Collect shared or individual accounts and passwords for external SaaS in a digital key vault. Typical solutions include access right management and multi-browser integration : **Roboform**, **Splashld** or **PassPack** etc		

Additional Comments			
Follow Up	XXXX	Implementation Date	30/09/2021

DATA AND SYSTEM ACCESS

COMMERCIAL OFFER

III. SECURITY AUDIT

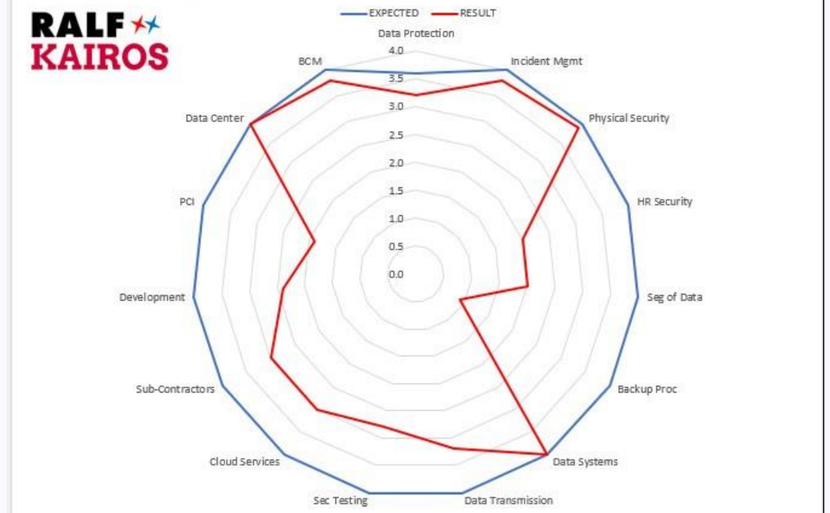
Technical Inspection approach: Survey & Healthcheck report

Domain	Question	Example	Answers	Importance	Rating	Rating Rationale
General Information						
	Name of Client		<<Text>>			
	Brief description of the client and services		<<Text>>			
Data Protection and IT Supplier Contract Management				Is this section applicable (Y/N)?	Yes	<<Comments entered here are visible in the dashboard>>
	Which legal jurisdiction governs the entity and the data stored?	e.g. Korean, European, etc.	<<Text>>	(4) High	2	
	Does the contract between Client and the Supplier contain security requirements ?	e.g. the right to audit, passwords, encryption, secure exchange of information, disposal requirements	<<Text>>	(4) High	2	
	What Client information / types of data will the Supplier be accessing (receiving, storing, processing or transmitting)?	e.g. Customer Data; Logistic Data; Intellectual Property; Credit Card Data; Human Resources Data; Marketing Data; Corporate or Financial Data; Physical Security Data; IT Infrastructure Data; Personal Data; Other Data	<<Text>>	(4) High	2	
	Is the Information Security Policy available?	Please provide documentation	<<Text>>	(4) High	2	
Incident Management				Is this section applicable (Y/N)?	Yes	<<Comments entered here are visible in the dashboard>>
	Do you have an information security incident management procedure and process?	Please provide documentation	<<Text>>	(4) High	3	
	Did you ever had security incidents ? (focus should be on the last 12 months)	e.g. Website defacement, DDoS, phishing attack, Social Engineering	<<Text>>	(4) High	3	
Physical Security				Is this section applicable (Y/N)?	Yes	<<Comments entered here are visible in the dashboard>>
	How is physical access managed?		<<Text>>	(4) High	4	
	What physical security controls are in place?	please describe them per security zone	<<Text>>	(4) High	4	
	Do you have a procedure in place for provisionning / removing assets (procedure and authorization)	e.g. is there an authorization process	<<Text>>	(4) High	4	
	Do you have a clear screen and desk policy in place?		<<Text>>	(4) High	4	
HR Security + Access				Is this section applicable (Y/N)?	Yes	<<Comments entered here are visible in the dashboard>>
	What background checks / screening activities are performed on employees or new project members?	If applicable: What background checks / trainings on contractors / temporary staff are done?	<<Text>>	(4) High	5	
	What documents do new employees have to	e.g. terms and conditions of	<<Text>>			

25 control points survey

30 control points - SUPPORTED TECHNICAL INSPECTION

Supplier Name: Client A

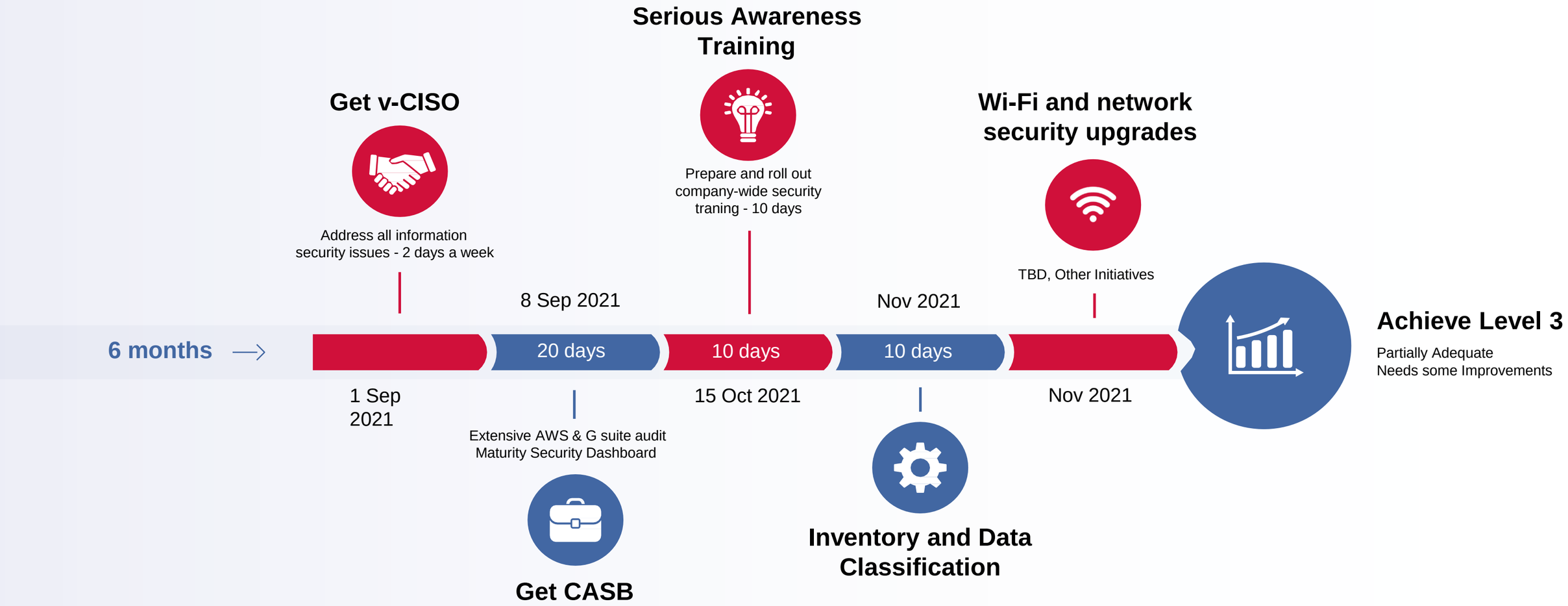


DOMAIN	EXPECTED	RESULT	COMPLIANCE	Remarks / Comments
Data Protection	3.6	3.2	40.00%	Severe non compliance with PIPA / GDPR
Incident Mgmt	4.0	3.8	58.00%	insufficient Incident management supervision
Physical Security	4.0	3.9	125.00%	full compliance with company physical sec atandards
HR Security	4.0	2.0	50.00%	HR management re access to data not fully controlled

30 control points healthcheck report & findings

COMMERCIAL OFFERS

6-MONTH CYBERSECURITY ACTION PLAN



REFERENCES

OEM	AIRBUS
BANKING	BNP PARIBAS CARDIF, mazars
MARKETING	JCDecaux, 3i, Adriel
STARTUPS	DEEPBLOCK, SECURELINK, QRyde by HBSS, GivU, nogae ASIA, LMJ
EDUCATION	SOLBRIDGE INTERNATIONAL SCHOOL OF BUSINESS, BEST OF THE BEST, Seorae Global Village Center, SUNG KYUN KWAN UNIVERSITY 1398
OTHER	BOLLORÉ LOGISTICS
INSTITUTIONS	FKCCI 한불상공회의소, ECCK EUROPEAN CHAMBER OF COMMERCE IN KOREA 주한유럽상공회의소

Certifications

CDPSE Certified Data Privacy Solutions Engineer. An ISACA® Certification

CISM Certified Information Security Manager® An ISACA® Certification

aws partner network Advanced Consulting Partner

CISA Certified Information Systems Auditor® An ISACA® Certification

ISO/IEC 27001 INFORMATION SECURITY ASSOCIATE™ J. PROVENZANO

CIA Certified Internal Auditor®

FICCA FINANCE & INDUSTRY CYBERSECURITY CONGRESS ASIA

FINANCE AND INDUSTRY CYBERSECURITY CONGRESS ASIA 2022

30,000 followers

Linkedin Community

CONFERENCES AND LECTURES

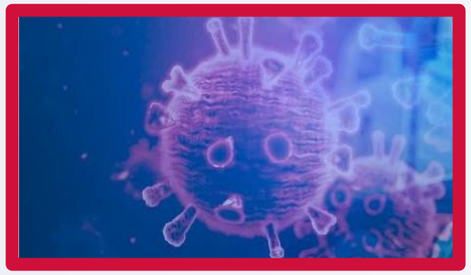
Cybersecurity - Switzerland 2017

Data Privacy in Korea 2019

Strenghtening your cybersecurity: Lessons learned in Korea 2019

FKCCI 한불상공회의소 2020

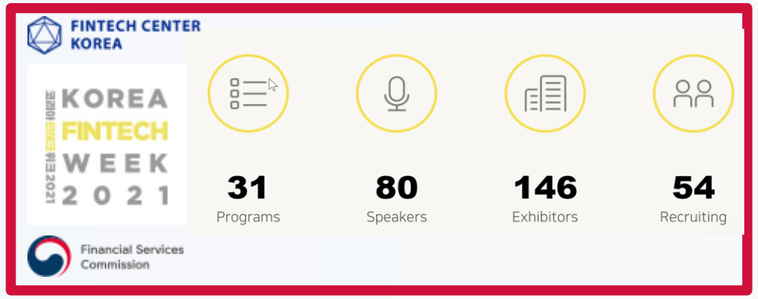
FKCCI 한불상공회의소 2020



Cybersecurity posture Pre-Post-COVID-19 2020

Cyber exam 2020

EUROPEAN CHAMBER OF COMMERCE IN KOREA 주한유럽상공회의소 2021



Fintech Center Korea 2021

FICCA – cyber asian congress
By RALFKAIROS

2021 & 2023

What is Cybersecurity in South Korea ?

2022

Hong Kong to Korea

2022

CONFERENCES AND LECTURES 2023

SINCE 1947
서경대학교
SEOKYEONG UNIVERSITY

[대학혁신] 2022 Cybersecurity Skills Challenge CTF 대회 참여 안내

SECON 2023
제22회 세계 보안 엑스포
International Security Exhibition & Conference

sweden 2023.eu
Swedish Presidency of the Council of the European Union

Ministry of Science and ICT
KISA KOREA INTERNET & SECURITY AGENCY

European Union & Republic of Korea
High-Level Conference on Cyber Security
focusing on the challenges and opportunities for industry in 2023

G20 भारत 2023 INDIA – DIA भारत 2023 INDIA
Digital Innovation Alliance

G20 DIGITAL INNOVATION ALLIANCE
[G20-DIA]

Thank you

감사합니다

contact@ralfkairos.com

www.ralfkairos.com