แนวทางการสร้างกำลังคนด้านความมั่นคงปลอดภัยไซเบอร์

การสัมนาทางวิชาการ
แนวทางพัฒนาบุคลากรเพื่อสนับสนุนเทคโนโลยีสารสนเทศและการสื่อสาร และอุตสาหกรรม

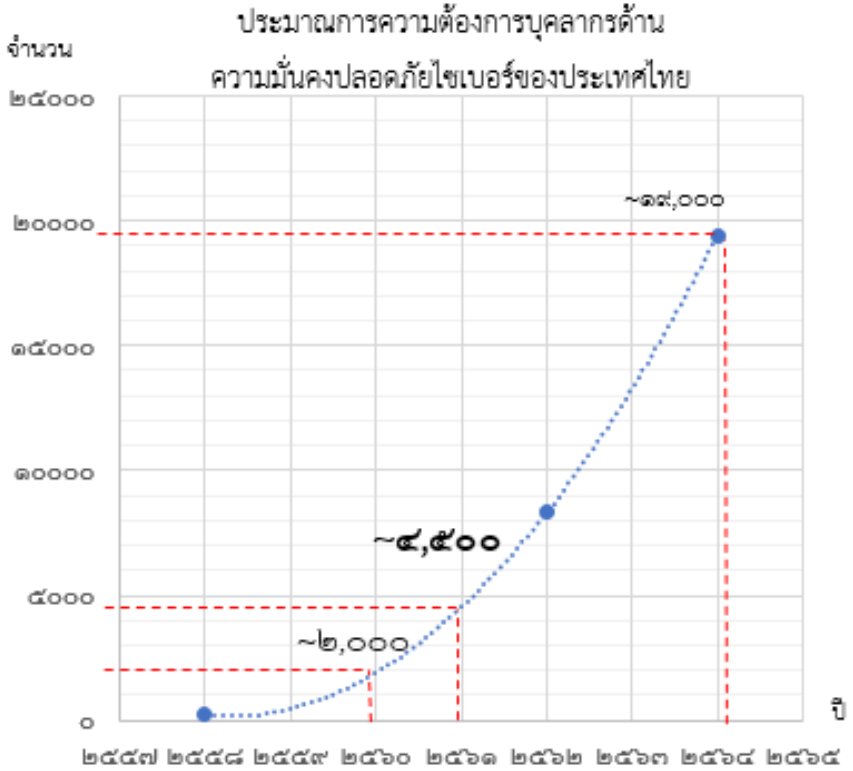
วันพฤหัสบดีที่ 28 มิถุนายน 2561

ระเบียบวาระ

- ประมาณการความต้องการบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ
- แนวทางการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ระยะเร่งด่วน ๑,๐๐๐ คน
- หลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์
- แนวทางการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์เพื่อตอบประเทศในระยะยาว

ประมาณการความต้องการบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ

ประมาณการความต้องการบุคลากรไซเบอร์ของโลก
ได้มีการประมาณการว่าในปีพ.ศ. ๒๕๖๔ โลกจะขาดแคลนบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ถึง ๓,๕๐๐,๐๐๐ คน[๑] ในปีพ.ศ. ๒๕๖๒ จะขาดแคลน ๑,๕๐๐,๐๐๐ คน[๒]



ในปี พ.ศ. ๒๕๖๑
ประเทศไทยจะขาดแคลนบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ประมาณ ๔,๕๐๐ คน[๓]

ความพร้อมบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศในปัจจุบัน

กำลังพลสายกลาโหม ๔๕๙ คน
(กองบัญชาการกองทัพไทย และ ๓ เหล่าทัพ)

เจ้าหน้าที่ตำรวจ (พนักงานสอบสวน) ๑๖๒ คน

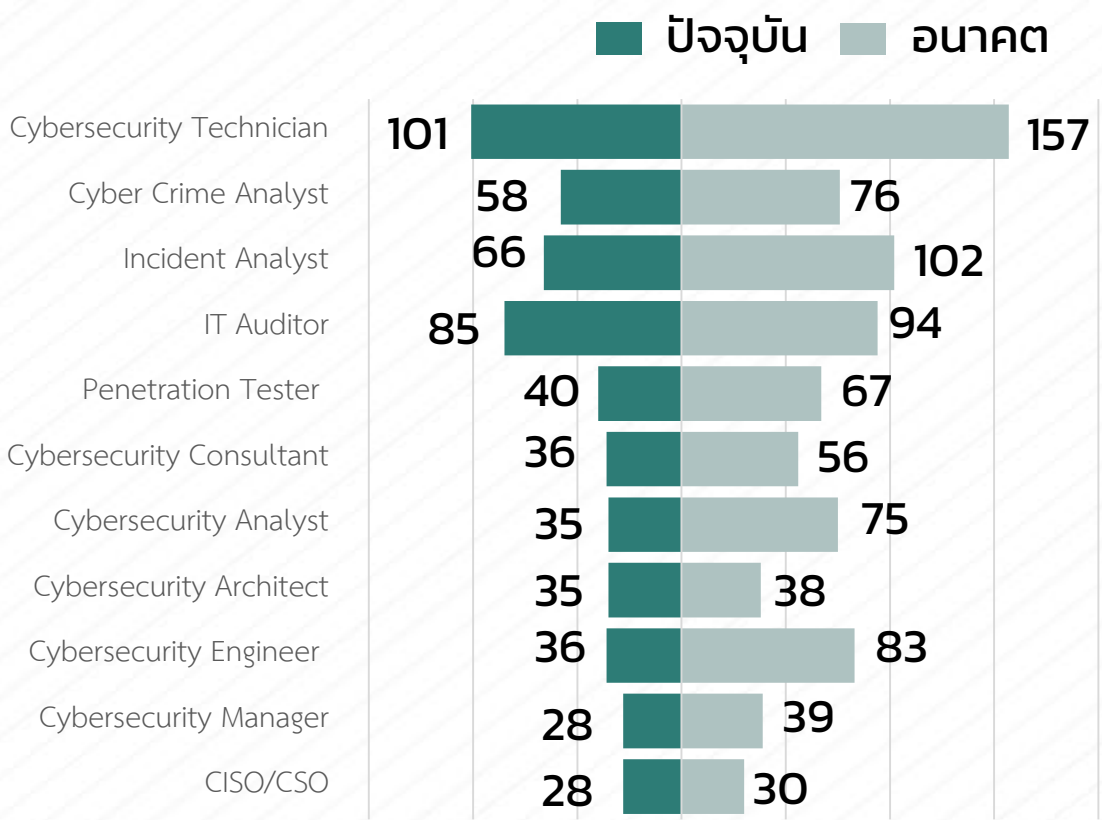
พนักงานเจ้าหน้าที่ (ตำรวจ + พลเรือน) ๘๘ + ๘๕ คน
(พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐)

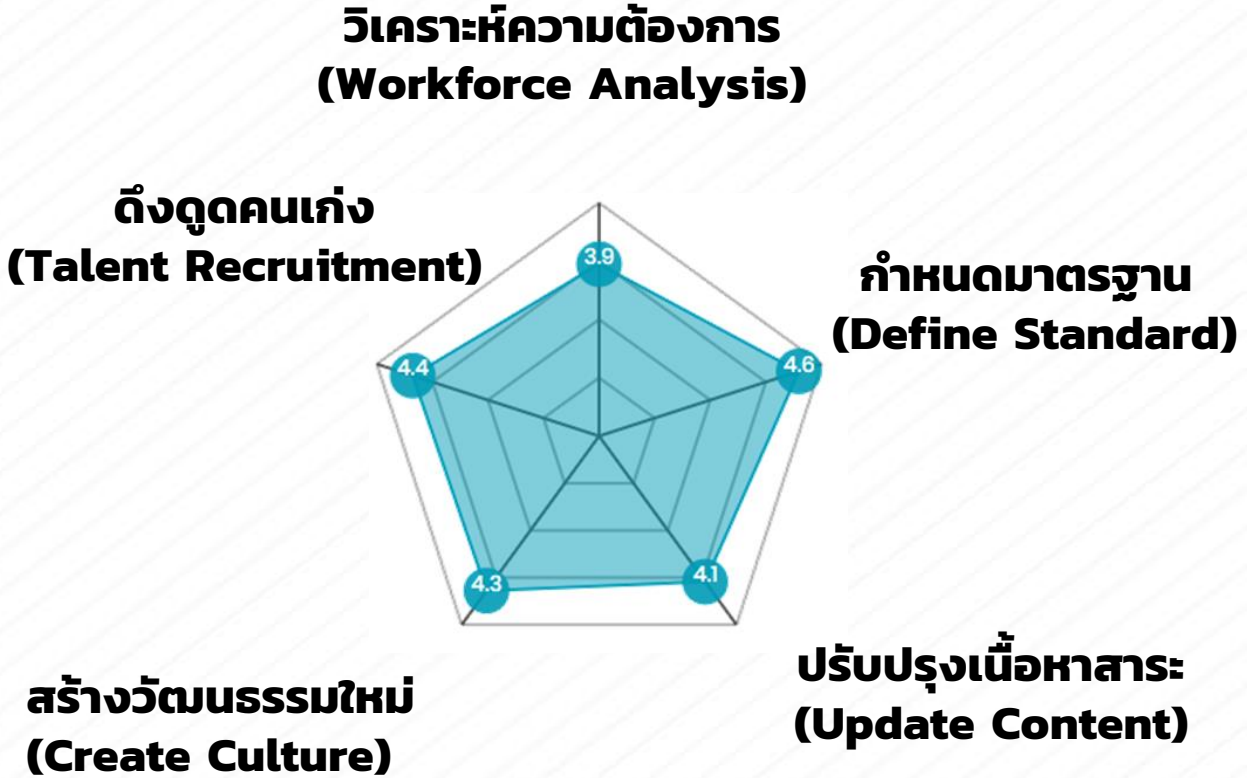
ผู้เชี่ยวชาญและผู้ปฏิบัติงานรับมือภัยคุกคามไซเบอร์ ๕๐ คน
(ThaiCERT, TB-CERT, TCM-CERT)

หมายเหตุ : อาจมีส่วนซ้อนทับกัน

๑. ที่มาจากบริษัทไซเบอร์ซีเคียวริตี้เวนเจอร์ส, **๒.** ที่มาจากบริษัทไซมานเทค,
๓. ประเมินความขาดแคลนจากสัดส่วน GDP ประเทศไทยและโลก

ผลสำรวจความเห็นต่อกลยุทธ์ของแผนพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์

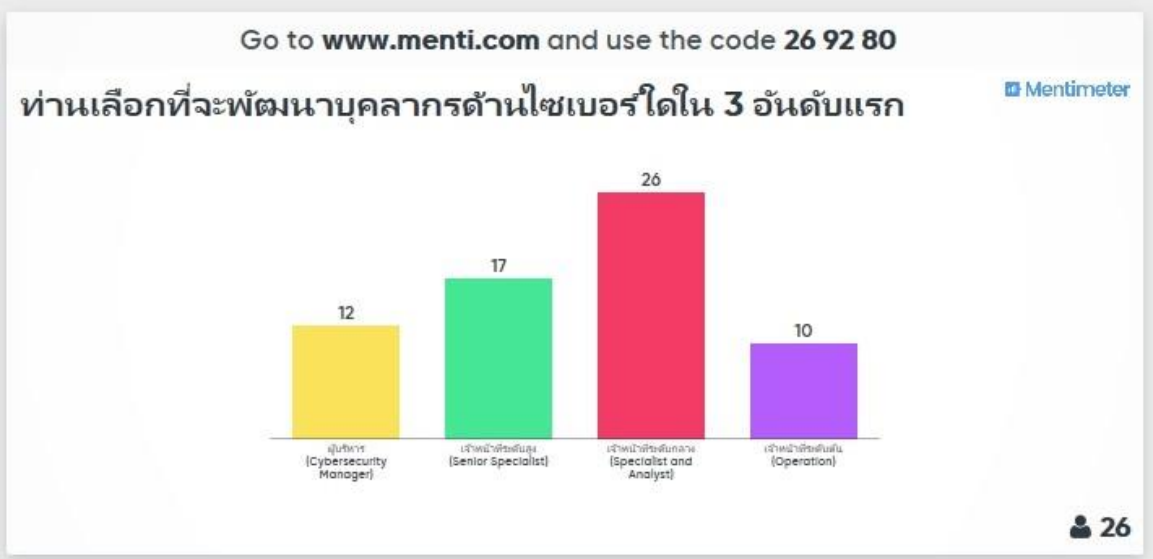




หมายเหตุ: แบบสำรวจ ๒๓ ท่าน

16 มกราคม พ.ศ. 2561

ผลการสำรวจความต้องการบุคลากรด้านไซเบอร์ (Telecom Sector)



ผลสำรวจจากการนำเสนอแนวนโยบายโครงสร้างพื้นฐานสำคัญสารสนเทศของประเทศ(การพัฒนาบุคคลด้านความมั่นคงปลอดภัยไซเบอร์) จัดโดยสมาคมโทรคมนาคมแห่งประเทศไทย เมื่อวันที่ 17 พ.ค. 2561 พบว่า

1) ท่านเลือกที่จะพัฒนาบุคลากรด้านไซเบอร์ เรียงตามลำดับดังนี้ (ตอบแบบสอบถาม 26)
   เจ้าหน้าที่ระดับกลาง จำนวน 26 คน
   เจ้าหน้าที่ระดับสูง จำนวน 17 คน
   ผู้บริหาร จำนวน 12 คน
   เจ้าหน้าที่ระดับต้น จำนวน10 คน

2) โดยมีความสนใจในหลักสูตรดังต่อไปนี้ (ตอบแบบสอบถาม 16)
- Fundamentals of Incident Handling คะแนน 4.1/5
- Advanced Incident Handling คะแนน 4.5/5
- IT Security Governance and Audit คะแนน 3.8/5
- Secure Coding คะแนน 3.9/5
- Advanced System and Network Administration คะแนน 4.4/5
- Big Data, Log Analysis and Machine Learning คะแนน 4.1/5

DD.MM.YEAR

แนวทางการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ระยะเร่งด่วน ๑,๐๐๐ คน

Core cybersecurity roles *are the most commonly requested job categories across the cybersecurity ecosystem. They are classified as entry-level, mid-level, or advanced-level based upon the experience, education levels, and credentials requested by employers.*

ผู้บริหารระดับสูง (๒%)

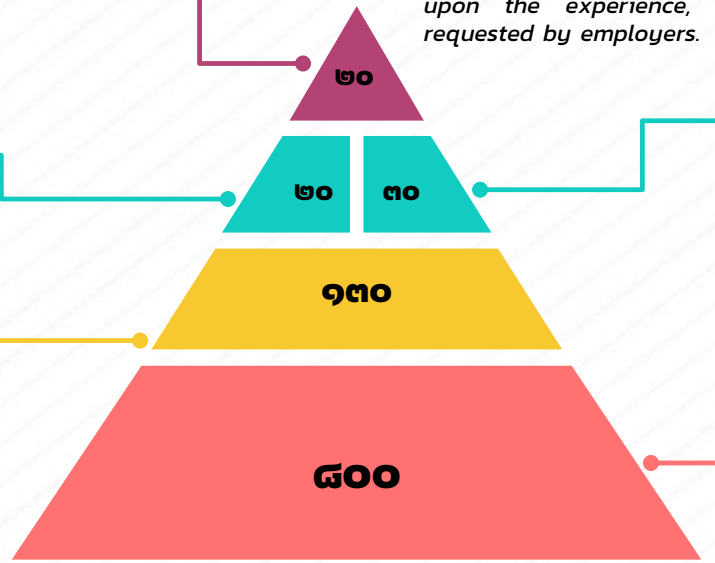
Board Level
CISO/CSO

เจ้าหน้าที่ระดับสูง (๒%)

Cybersecurity Engineer
Cybersecurity Architect

เจ้าหน้าที่ระดับกลาง (๑๓%)

Cybersecurity Analyst
Cybersecurity Consultant
Penetration Tester



ผู้บริหาร (๓%)

Cybersecurity Manager

เจ้าหน้าที่ระดับต้น (๘๐%)

Cybersecurity Technician
Cyber Crime Analyst
Incident Analyst
IT Auditor

ความต้องการของประกาศนียบัตรวิชาชีพเฉพาะทาง จำเป็นต้องมี ควรมี

ผู้บริหารระดับสูง	เจ้าหน้าที่ระดับสูง	ผู้บริหาร	เจ้าหน้าที่ระดับกลาง	เจ้าหน้าที่ระดับต้น
iSEC-M3 CISM CSX	iSEC-M3 iSEC-T3 Security+ Network+ CISSP CSSLP CCSP CSX	iSEC-M3 iSEC-T2 CISSP CISA CISM	iSEC-M2 iSEC-T2 หรือ iSEC-T3 Security+ Network+ CSX CISSP CCSP CISM CSA+ CSSLP SSCP CISA CEH	iSEC-M1 iSEC-T1

ประกาศนียบัตร **iSEC (Thailand Information System Security Professionals Certification) ด้านบริหาร (M) และด้านเทคนิค (T)** พัฒนาขึ้นโดยความร่วมมือระหว่าง สพธอ. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และสมาคมความมั่นคงปลอดภัยระบบสารสนเทศ (Thailand Information Security Association: TISA) โดยอ้างอิงจากโมเดล Essential Body of Knowledge (EBK) จาก Department of Homeland Security (DHS) สหรัฐอเมริกา เพื่อเป็นประกาศนียบัตรด้านความมั่นคงปลอดภัยของไทย **(Thailand Local Certificate)**

แนวทางการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ระยะเร่งด่วน

หลักสูตรทั่วไป

Silver Workforce

หลักสูตรเฉพาะทาง

Gold Workforce
๑,๐๐๐ คน

หลักสูตร

Platinum Workforce
๒๐๐ คน

กลุ่มเป้าหมาย

๑. บุคลากรในหน่วยงาน CI, หน่วยงานรัฐ และภาคเอกชน
๒. อาจารย์มหาวิทยาลัย + นักเรียนทุน
๓. นิสิต/นักศึกษา + นักเรียนอาชีวะ

ได้รับการรับรอง

LOCAL certificate

ได้รับการรับรอง

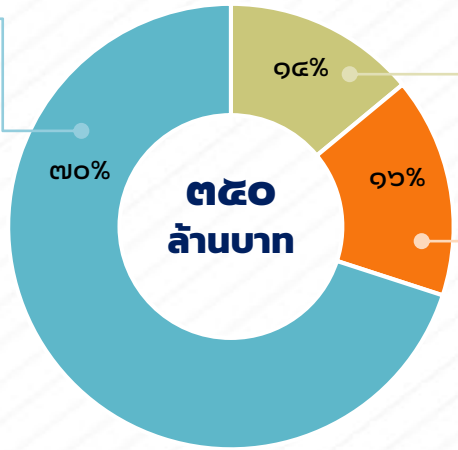
INTER certificate

Public-private-partnership ร่วมกับสถาบันอบรม มหาวิทยาลัยรัฐและเอกชน*
พัฒนาหลักสูตร จัดอบรม/สอบ และผลิตประชาคม Thai Cyber Workforce

*ลงนาม MoU แล้ว ๖ แห่ง

งบประมาณ

ค่าหลักสูตร การฝึกอบรมและค่าสอบวัดผล (จ่ายตามจำนวนคน)
- หลักสูตรทั่วไป
- หลักสูตรเฉพาะทาง
- หลักสูตรผู้เชี่ยวชาญ



ค่าพัฒนาระบบและสื่อการเรียนออนไลน์ (จ่ายครั้งเดียว)

ค่าบริหารจัดการ

DD.MM.YEAR

ภาพรวมการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ระยะเร่งด่วน ๑,๐๐๐ คน

อบรมผู้สอน
(Train the Trainer)

- บูธแคมป์
- หลักสูตรนานาชาติ

อบรมแล้วในเบื้องต้น
จำนวน ๓๐ คน
(อาจารย์มหาวิทยาลัย + อุตสาหกรรม)

สิ่งที่ได้รับ

หลักสูตร
ระดับพื้นฐาน/ ระดับกลาง/ ผู้เชี่ยวชาญ

ข้อสอบ ๓๐๐ ข้อ

SILVER

PRE-TEST

ถ่ายทอดความรู้ให้บุคลากร
(อบรม & สอบ)
จำนวน ๕,๐๐๐ คน

GOLD

POST-TEST

คาดว่าจะสอบผ่าน
จำนวน ๑,๐๐๐ คน

PLATINUM

EXAMINAION

ผู้เชี่ยวชาญ
จำนวน ๒๐๐ คน

กลุ่มเป้าหมาย

SUPPLY

MOU
- ม.เกษตร
- ม.มหิดล
- ม.ธรรมศาสตร์
- ม.ศิลปากร
- ม.รังสิต
- ม.หอการค้า

MOU+
- ม.สยาม
- ม.ราชมงคลตะวันออก
- ม.ราชมงคลธัญบุรี
- CMKL
- SANS
- APNIC

DEMAND

1) หน่วยงาน CI, CII
2) เครือข่ายผู้เชี่ยวชาญ
3) อาจารย์ไซเบอร์
4) นิสิต/นักศึกษา
5) บริษัทเอกชน
6) หน่วยงาน CERT
7) กิตติมศักดิ์
8) ประชาชนทั่วไป

แผนกิจกรรมบูธแคมป์ ๓ ระยะ ภายใน ๑ ปี

สัปดาห์ที่	๑ - ๕	๖ - ๑๐	๑๑ - ๒๐	๒๑ - ๓๐	๓๑ - ๔๐	๔๑ - ๕๐

Silver Workforce

๕,๐๐๐ คน

เตรียมงาน

อบรม ๕,๐๔๐ คน ภายใน ๓๐ สัปดาห์

(๑๖๘ คน / ๓๐ ครั้ง)

Gold Workforce

๑,๐๐๐ คน

อบรม ๑,๐๐๘ คน ภายใน ๓๐ สัปดาห์

(๓๔ คน / ๓๐ ครั้ง)

Platinum Workforce

๒๐๐ คน

อบรม ๒๑๐ คน ภายใน ๑๐ สัปดาห์

(๒๑ คน / ๑๐ ครั้ง)

ดูงานการทำงานของ CERT ณ ประเทศอิสราเอล

ประมาณ
สัปดาห์ที่ ๔๑

หลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์

Carnegie Mellon University
Software Engineering Institute

SANS

APNIC

TRANSITS

AJCCBC
ASEAN JAPAN CYBERSECURITY CAPACITY BUILDING CENTRE
Partnership by ASEAN and Japan

Carnegie Mellon University

Software Engineering Institute

- Fundamentals of Incident Handling
- Advanced Incident Handling
- IT Security Governance and Audit
- Secure Coding
- Advanced System and Network Administration
- Big Data, Log Analysis and Machine Learning

https://www.sei.cmu.edu/education-outreach/courses/index.cfm

APNIC

PriceTHB 20,000
Duration2 Days

Date : **May 24 – 25 , 2018**
Time : **9:00 -17:30**

Workshop
WSEC01: Network Security

Duration	3 days
Level of Study	Intermediate

Course Fee
Standard: 20, 000 THB
Early Bird: 15,000 THB
APNIC Members : Please contact us at training@interlab.ait.ac.th or Call (66-2)524-6611

*Early-bird registration fees must be paid before or on **24 April 2018** where as Standard registration fees must be paid before or on **24 May 2018** by cheque or wire transfer payment.*

Group rate: please contact training@interlab.ait.ac.th

Venue:
inteRLab, AIT (GOOGLE MAP)

Instructors:
Jamie Gillespie, APNIC
Tashi Phuntsho, APNIC

Course Duration: **2 days**

Maximum number of attendees:
The workshop can accommodate up to **40 participants.**

Synopsis:
The workshop is intended for network engineers, System administrators/operators, managers and policy makers to understand security threats, preventions and recovery. Device and network infrastructure security is examined with a focus on different layers to establish a robust, stable and secure network and protect the data from various kind of attack.

https://training.apnic.net/courses/wsec01-network-security/

DD.M.YEAR

Explore this interactive training roadmap to find the right courses for your immediate cyber security skill development and for your long-term career goals. More than 60 courses deliver critical skills in the cyber defense operations, digital forensics, software development, and management practice areas of cyber security.

1. BASELINE SKILLS

2. FOCUS JOB ROLES

3. CRUCIAL SKILLS, SPECIALIZED ROLES

Core Techniques
Prevent, Defend, Maintain
2 COURSES

Every Security Professional Should Know

Security Essentials	SEC401
Hacker Techniques	SEC504

Monitoring & Detection
Intrusion Detection, Monitoring Over Time
2 COURSES

Penetration Testing
Vulnerability Analysis, Ethical Hacking
2 COURSES

Incident Response & Threat Hunting
Host & Network Forensics
3 COURSES

Cyber Defense Operations
Harden Specific Defenses
8 COURSES

Advanced Penetration Testing
Advanced Techniques & Areas
8 COURSES

Threat Intel & Forensics
Specialized Investigative Skills
5 COURSES

Development & Secure Coding
4 COURSES

Industrial Control Systems
3 COURSES

Security Management
Managing Technical Security Operations
2 COURSES

CISSP® Training MGT414

Advanced Management
Advanced Leadership, Audit, Legal
5 COURSES

Introduction to Cyber Security SEC301

https://www.sans.org/cyber-security-skills-roadmap

TRANSITS provides affordable, high-quality training to both new and experienced Computer Security and Incident Response Team (CSIRT) personnel,

TRANSITS-I

The TRANSITS-I course is aimed at new or potential CSIRT personnel who wish to gain a good grounding in the main aspects of working in an incident handling and response team. Over the years, operatives have been trained for commercial, governmental, military and national CSIRTs, as well as those in the research and education sector.

Organisation, Technical, Operational, Legal

TRANSITS II

The TRANSITS-II course is aimed at more experienced personnel working for established CSIRTs. It provides an in-depth study of key areas in incident handling and response operations, training in how to improve communications with constituents, along with practical exercises.

NetFlow Analysis, Forensics, Communication, CSIRT Exercises

https://www.terena.org/activities/transits/

AJCCBC
ASEAN JAPAN CYBERSECURITY CAPACITY BUILDING CENTRE
Partnership by ASEAN and Japan

CYDER
Cyber Defense Exercise for Recurrence

Focus on the improvement of **the incident response ability to correspond against the cyber-attacks**, trainees can experience and learn the method of incident handling based on an actual cyber attack.

- **Basic Knowledge & Tools**
- **Practical Exercise**
- **Team Discussion & Report**

Forensic

Trainee can learn lectures and practical exercises to **investigate the infringement situation** attacked by malware or APT and to **preserve the trail** left in memory etc. after being attacked.

- **Basic Knowledge**
- **Tools & Practical Exercise**
- **Investigation & Preservation**

Malware Analysis

Trainee can learn **how to analyze malware** discovered by antivirus software and forensic analysis. **Exercises will be carried out** based on examples that analysts frequently face as practical.

- **Environment & Flow**
- **Tools & Analysis**
- **Practical Exercise**

แนวทางการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ระยะเร่งด่วน เพื่อตอบประเทศในระยะยาว (ร่วมตอบโจทย์ความต้องการด้านดิจิทัล)

แพลตฟอร์ม

ระบบ หลักสูตร และสื่อการเรียนออนไลน์

+

โมเดล

บูทแคมป์ ๓ ระยะ

เป็นต้นแบบสำหรับปรับใช้ในหน่วยงานอื่นๆ / SECTOR-CERT / ประเทศในอาเซียน

ประยุกต์เพื่อตอบโจทย์

สำนักงาน ก.พ.
OCSC
Office of the Civil Service Commission

๔๗,๘๙๒ อัตรา

IT ..... ๔,๙๓๙ อัตรา

ข้าราชการ | พนักงานราชการ | อื่นๆ

Non-IT ..... ๔๒,๙๕๖ อัตรา

S ๓๙๐
M ๒,๐๐๓
K
O ๔๐,๕๖๐

๖ กลุ่ม CII

สรุปประเด็น

- ความต้องการบุคลากรด้านไซเบอร์ของประเทศและในกลุ่ม Sector
- โครงการเร่งรัดการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ (Intensive cybersecurity Capacity building Programme)
- หลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์
- แนวทางในระยะกลางและระยะยาว