

หลักสูตร

วิศวกรความมั่นคงปลอดภัย Security Engineer

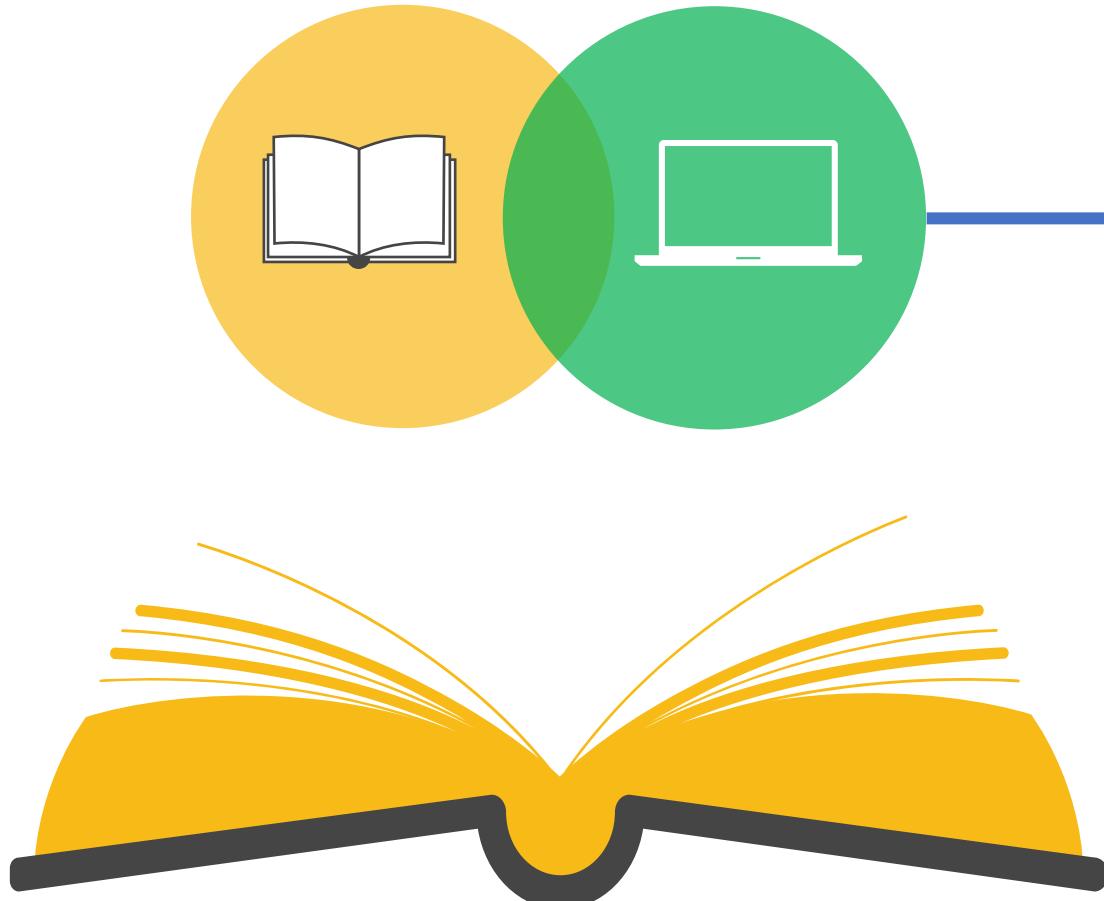
ภายใต้โครงการเส้นทางสู่วิศวกรความมั่นคงปลอดภัย สำหรับนักศึกษาจบใหม่สู่การทำงานในภาคอุตสาหกรรม

หลักสูตร วิศวกรความมั่นคงปลอดภัย Security Engineer

ภายใต้โครงการเส้นทางสู่วิศวกรความมั่นคงปลอดภัย สำหรับบัณฑิตจบใหม่สู่การทำงานในภาคอุตสาหกรรม



Agenda



Introduction to Security Principles

Risk Management & Security Controls

Identity & Access Management (IAM)

Network & Endpoint Security

Security Awareness & Incident Response

Security Best Practices

Q & A

Speaker



Mr. Angkarn Pummarin
Deputy Managing Director

GRC Director (Information Security)

Certification

- **Cloud Security Alliance CCZT (Certificate of Competence in Zero Trust)**
- **Cloud Security Alliance CCSK (Certificate of Cloud Security Knowledge)**
- **ICDL Data Protection**
- **EC-Council Associate C|CISO**
- **(ISC)² Certified in Cybersecurity Certification**
- **ITS Cybersecurity**
- **Microsoft Certified Trainer**
- **CQI and IRCA Certified BCMS ISO 22301:2019 Lead Auditor**
- **CQI and IRCA Certified ISO/IEC 20000-1:2018 Lead Auditor**
- **CQI and IRCA Certified ISO/IEC 27001:2022 Lead Auditor**
- **CompTIA Project+**
- **CompTIA Security Analytics Professional**

Etc....

អាសយដ្ឋាន ធម្មតាគម្រោងកសិករម្យ Security Engineer

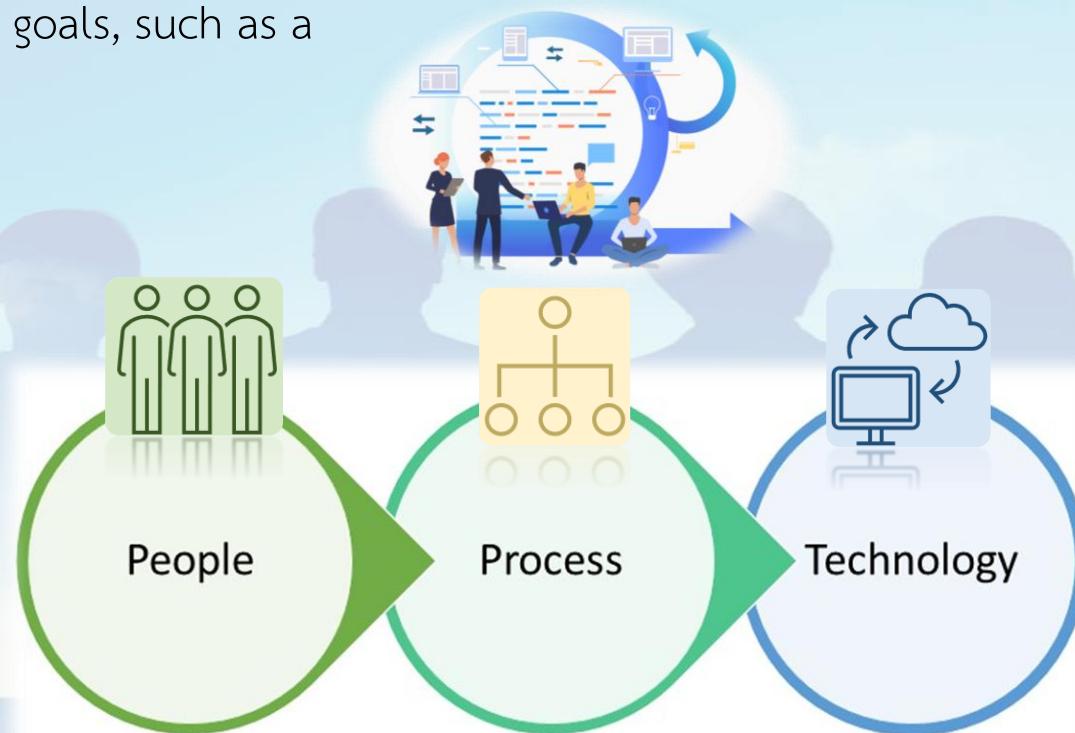
ការណាន់កម្ពស់ការងារសំខាន់សំខាន់របស់អ្នកសិករម្យ ដោយបានចូលរួមនៅក្នុងការងារកសិករម្យ។



Introduction to Security Principles

Organization

A structured group of people working together toward common goals, such as a company.



หลักสูตร วิศวกรความมั่นคงปลอดภัย Security Engineer

ภายใต้โครงการเส้นทางสู่วิศวกรความมั่นคงปลอดภัย สำหรับนักศึกษาจบใหม่สู่การทำงานในภาคอุตสาหกรรม

Why Cybersecurity IT's Importance

NotPetya cyber-attack cost TNT at least \$300m

20 September 2017



Ref: bbc.com

Acer โดน Ransomware โจมตีพร้อมเรียกค่าไถ่สูงถึง 50 ล้านดอลลาร์ แต่มีส่วนลดให้

© 25 มี.ค. 64 (17:43 น.)



Ref: sanook.com

Cyberattack โจมตี Co-op สูญเสียรายได้กว่า 275 ล้านดอลลาร์สหรัฐ ข้อมูลสماชิก 6.5 ล้านรายถูกบันทึก

เหตุการณ์ Cyberattack ที่เกิดขึ้นกับร้านค้าปลีก Co-op เมื่อเดือนเมษายนที่ผ่านมา ได้สร้างผลกระทบเป็นวงกว้าง ทั้งที่ให้เชื้อไวรัสบนเครื่องคอมพิวเตอร์และขโมยข้อมูลของลูกค้า ทำให้ร้านค้าปลีกต้องปิดตัวลง 275 จุดขายทั่วโลก ประมาณ 206 ล้านปอนด์ (ประมาณ 6.5 ล้านบาท) ที่สูญเสียไป

READ MORE

<https://securityaffairs.com/182713/security/cyberattack-on-co-op-leaves-shelves-empty-data-stolen-and-275m-in-loss-revenue.html>

Ref: thaicert.or.th



Ref: thaicert.or.th



Astral Foods สูญเงินกว่า 1 ล้านดอลลาร์จากการถูกโจมตีทางไซเบอร์ที่ระบบผลิตและจัดส่ง

Astral Foods ผู้ผลิตไก่และเนื้อสัตว์ต้องเผชิญกับเหตุการณ์โจมตีไซเบอร์ เมื่อวันที่ 16 มกราคม 2025 ส่งผลให้ใช้จ่ายเพิ่มเติมและจัดซื้อเพิ่มเติม ประมาณ 1 ล้านดอลลาร์ (ประมาณ 3.5 ล้านบาท)

READ MORE

<https://securityaffairs.com/175833/security/astral-foods-cyber-attack.html>

Ref: thaicert.or.th

Why Cybersecurity IT's Importance



CIA Triad



Confidentiality

Protecting sensitive information from unauthorized access and disclosure.

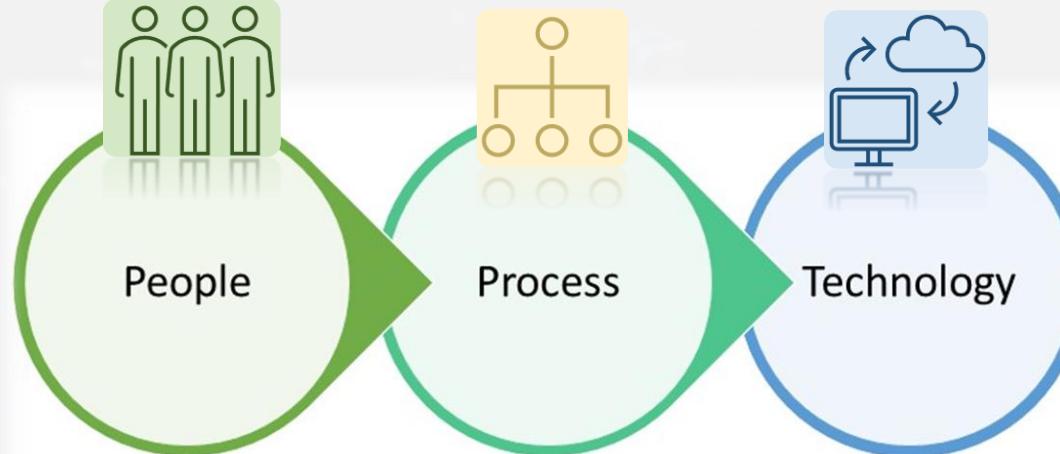
Integrity

Ensuring data is accurate, consistent, and has not been improperly modified or deleted.

Availability

Guaranteeing that systems and data are accessible to authorized users when they need them.

CIA Triad



Information security, cybersecurity and privacy protection
— Information security management systems



Understanding Information security

Information security

preservation of confidentiality, integrity and availability of information



In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

Understanding Cybersecurity

Cyber security

preservation of confidentiality, integrity and availability of information in the **Cyberspace**



In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, **which does not exist in any physical form**

អត្ថបទ ធមធានគម្រោងពលិតកាយ Security Engineer

ការងារនៃគម្រោងគម្រោងពលិតកាយគឺជាការរកចំណាំរបស់ការងារ ដែលមានប៉ុណ្ណោះថាបានបានការងារក្នុងការងារពលិតកាយ។

Security

Information security

preservation of confidentiality, integrity and availability of information



Cyber security

preservation of confidentiality, integrity and availability of information in the **Cyberspace**



Insider Threat Actors

Malicious insider threat

- Has or has had authorized access
- Employees, contractors, partners
- Sabotage, financial gain, business advantage



Unintentional insider threat

- Weak policies and procedures
- Weak adherence to policies and procedures
- Lack of training/security awareness
- Shadow IT

Standard, Framework, Legal

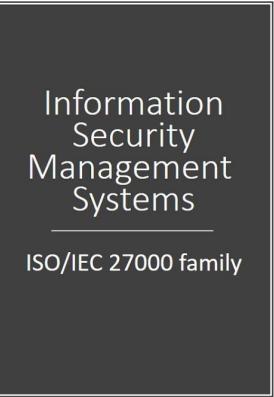
(Standard, Framework and Legal about Information security management system)

Information
Security
Management
Systems

ISO/IEC 27000 family



Standard, Framework, Legal



- ISO/IEC 27001** Information security management System
- ISO/IEC 27002** Information security controls
- ISO/IEC 27005** Information security risk management

- ISO/IEC 27032** Security techniques Guidelines for cybersecurity
- ISO/IEC 27033** Security techniques Network security
- ISO/IEC 27034** Security techniques Application security
- ISO/IEC 27035** Security techniques Information security incident management
- ISO/IEC 27701** Privacy information security management

ISMS



2022

4 Domains, 93 Controls

- **People**

if they concern individual people

- **Physical**

if they concern physical objects

- **Technical**

if they concern technology

otherwise, they are categorized as organizational.

- **Organizational**

Standard, Framework, Legal

(Standard, Framework and Legal about Information security management system)

Information
Security
Management
Systems

ISO/IEC 27000 family



NIST

Core



Desired cybersecurity outcomes organized in a hierarchy and aligned to more detailed guidance and controls

Profiles

Alignment of an organization's requirements and objectives, risk appetite and resources **using** the desired outcomes of the Framework

Framework for Improving
Critical Infrastructure Cybersecurity

Implementation Tiers

A qualitative measure of organizational cybersecurity risk management practices



NIST

What process and asset need protection

What Safeguards are available

What techniques can identify incidents

What techniques contain Impacts of incidents

What techniques can restore capabilities

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

អាគភូមិសុំ ធម្មតាអនុវត្តន៍ការងារមំបែកសម្រាប់ Security Engineer

ការងារដែលត្រូវការងារមំបែកសម្រាប់អាគភូមិសុំ ធម្មតាអនុវត្តន៍ការងារមំបែកសម្រាប់ការងារក្នុងក្រសួងពេទ្យ

NIST

Function	Category	Subcategory	Informative References
PROTECT (PR)	Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	CIS CSC , 16 COBIT 5 DSS05.04, DSS05.05, DSS05.07, DSS06.03 ISA 62443-2-1:2009 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 ISO/IEC 27001:2013 , A.7.1.1, A.9.2.1 NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	CIS CSC 1, 12, 15, 16 COBIT 5 DSS05.04, DSS05.10, DSS06.10 ISA 62443-2-1:2009 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 ISO/IEC 27001:2013 A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 NIST SP 800-53 Rev. 4 AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11

Standard, Framework, Legal

(Standard, Framework and Legal about Information security management system)

Information
Security
Management
Systems

ISO/IEC 27000 family



Act.



- พรบ.การรักษาความมั่นคงปลอดภัยใช้เบอร์ พ.ศ.2562
- พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550
- พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ฉบับที่ 2 พ.ศ. 2560



- ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการปลอดภัย พ.ศ. 2555
- หลักเกณฑ์การเก็บรักษาข้อมูลจากรายงานคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๖๔
- พรบ. ลิขสิทธิ์ ฉบับที่ 5 พ.ศ. 2565
- พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

Cybersecurity Act.



พระราชบัญญัติ
การรักษาความมั่นคงปลอดภัยไซเบอร์
พ.ศ. ๒๕๖๗

Cybersecurity Act.

“ไซเบอร์” หมายความรวมถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรศัมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป

“การรักษาความมั่นคงปลอดภัยไซเบอร์” หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศอันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ

“ภัยคุกคามทางไซเบอร์” หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภัยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

Cybersecurity Act.

“โครงสร้างพื้นฐานสำคัญทางสารสนเทศ” หมายความว่า คอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งหน่วยงานของรัฐหรือหน่วยงานเอกชนใช้ในการข้อมูลที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ

“หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ” หมายความว่า หน่วยงานของรัฐหรือหน่วยงานเอกชน ซึ่งมีการกิจกรรมให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ



- มาตรา ๔๙ ให้คณะกรรมการมีอำนาจประกาศกำหนดลักษณะหน่วยงานที่มีการกิจกรรมให้บริการในด้านดังต่อไปนี้ เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
- (๑) ด้านความมั่นคงของรัฐ
 - (๒) ด้านบริการภาครัฐที่สำคัญ
 - (๓) ด้านการเงินการธนาคาร
 - (๔) ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม
 - (๕) ด้านการขนส่งและโลจิสติกส์
 - (๖) ด้านพลังงานและสาธารณูปโภค
 - (๗) ด้านสาธารณสุข
 - (๘) ด้านอื่นตามที่คณะกรรมการประกาศกำหนดเพิ่มเติม

Cybersecurity Act.

- นโยบายและแผน
- การบริหารจัดการ
- การรับมือกับภัยคุกคามทางไซเบอร์

ตรวจสอบ

ตรวจสอบข้อมูลที่เกี่ยวข้อง
ข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์
ของหน่วยงานนั้น รวมถึงพฤติกรรม
แผลล้มของตน

ประเมินการเกิด

ประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้น
หรือไม่

ป้องกัน รับมือ ลดความเสี่ยง

ให้ดำเนินการป้องกัน รับมือ และลดความ
เสี่ยงจากภัยคุกคามทางไซเบอร์ตาม
ประมาณแนวทางปฏิบัติและกรอบมาตรฐาน
ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
ของหน่วยงานนั้น



แจ้งไปยังสำนักงาน

แจ้งไปยังสำนักงานและหน่วยงาน ควบคุม
หรือกำกับ



CIS Controls

CIS Critical Security Controls[®]

<https://learn.cisecurity.org/cis-controls-download>

CIS implementation group



IG3 (Includes IG1 and IG2)

An IG3 enterprise employs security experts that specialize in the different facets of cybersecurity (e.g., risk management, penetration testing, application security). IG3 assets and data contain sensitive information or functions that are subject to regulatory and compliance oversight. An IG3 enterprise must address availability of services and the confidentiality and integrity of sensitive data. Successful attacks can cause significant harm to the public welfare.

Safeguards selected for IG3 must abate targeted attacks from a sophisticated adversary and reduce the impact of zero-day attacks.



IG1

An IG1 enterprise is small to medium-sized with limited IT and cybersecurity expertise to dedicate towards protecting IT assets and personnel. The principal concern of these enterprises is to keep the business operational, as they have a limited tolerance for downtime. The sensitivity of the data that they are trying to protect is low and principally surrounds employee and financial information.

Safeguards selected for IG1 should be implementable with limited cybersecurity expertise and aimed to thwart general, non-targeted attacks. These Safeguards will also typically be designed to work in conjunction with small or home office commercial off-the-shelf (COTS) hardware and software.



IG2 (Includes IG1)

An IG2 enterprise employs individuals responsible for managing and protecting IT infrastructure. These enterprises support multiple departments with differing risk profiles based on job function and mission. Small enterprise units may have regulatory compliance burdens. IG2 enterprises often store and process sensitive client or enterprise information and can withstand short interruptions of service. A major concern is loss of public confidence if a breach occurs.

Safeguards selected for IG2 help security teams cope with increased operational complexity. Some Safeguards will depend on enterprise-grade technology and specialized expertise to properly install and configure.

ຮັກສູດ ວຽກງານນັ້ນຄອງປລອດກັຍ Security Engineer

ກາຍໄດ້ໂຄຣການເລັກທາງສູ່ວຽກງານນັ້ນຄອງປລອດກັຍ ສໍາເຮັບນັກສຶກບໍາຈົບໃໝ່ສູ່ການກຳຈານໃນການອຸດສາຫກຮຽນ

CIS Controls

CIS Critical Security Controls

Control 01 Inventory and Control of Enterprise Assets

Why is this Control critical?
Procedures and tools
Safeguards

Control 02 Inventory and Control of Software Assets

Why is this Control critical?
Procedures and tools
Safeguards

Control 03 Data Protection

Why is this Control critical?
Procedures and tools
Safeguards

Control 04 Secure Configuration of Enterprise Assets and Software

Why is this Control critical?
Procedures and tools
Safeguards

Control 05 Account Management

Why is this Control critical?
Procedures and tools
Safeguards

Control 06 Access Control Management

Why is this Control critical?
Procedures and tools
Safeguards

Control 07 Continuous Vulnerability Management

Why is this Control critical?
Procedures and tools
Safeguards

Control 08 Audit Log Management

Why is this Control critical?
Procedures and tools
Safeguards

Control 09 Email and Web Browser Protections

Why is this Control critical?
Procedures and tools
Safeguards

Control 10 Malware Defenses

Why is this Control critical?
Procedures and tools
Safeguards

Control 11 Data Recovery

Why is this Control critical?
Procedures and tools
Safeguards

Control 12 Network Infrastructure Management

Why is this Control critical?
Procedures and tools
Safeguards

Control 13 Network Monitoring and Defense

Why is this Control critical?
Procedures and tools
Safeguards

Control 14 Security Awareness and Skills Training

Why is this Control critical?
Procedures and tools
Safeguards

Control 15 Service Provider Management

Why is this Control critical?
Procedures and tools
Safeguards

Control 16 Application Software Security

Why is this Control critical?
Procedures and tools
Safeguards

Control 17 Incident Response Management

Why is this Control critical?
Procedures and tools
Safeguards

Control 18 Penetration Testing

Why is this Control critical?
Procedures and tools
Safeguards

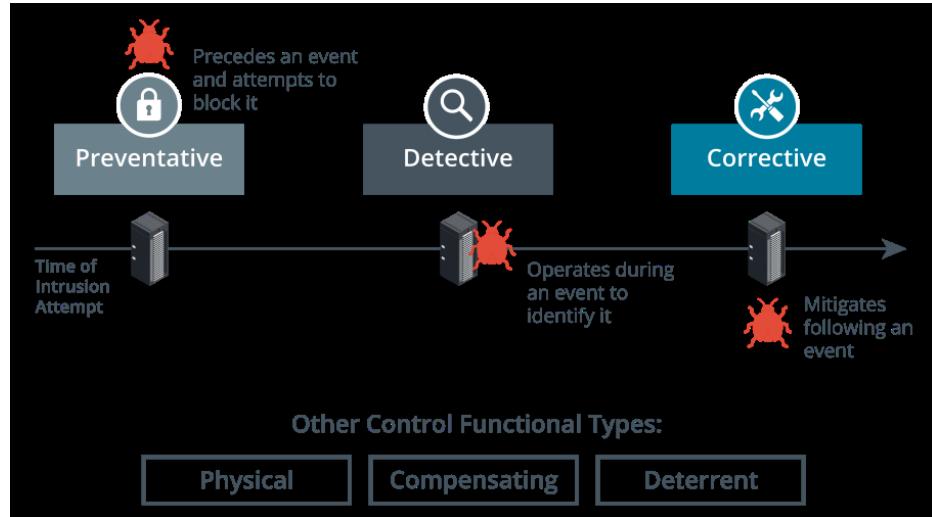
หลักสูตร วิศวกรความมั่นคงปลอดภัย Security Engineer

ภายใต้โครงการเส้นทางสู่วิศวกรความมั่นคงปลอดภัย สำหรับบัณฑิตจบใหม่สู่การทำงานในภาคอุตสาหกรรม

Risk Management & Security Controls



Security Control Functional Types



Preventive

- Physically or logically restricts unauthorized access
- Operates before an attack

Detective

- May not prevent or deter access, but it will identify and record any attempted or successful intrusion
- Operates during an attack

Corrective

- Responds to and fixes an incident and may also prevent its reoccurrence
- Operates after an attack

Physical

Controls such as alarms, gateways, and locks that deter access to premises and hardware

Deterrent

May not physically or logically prevent access, but psychologically discourages an attacker from attempting an intrusion

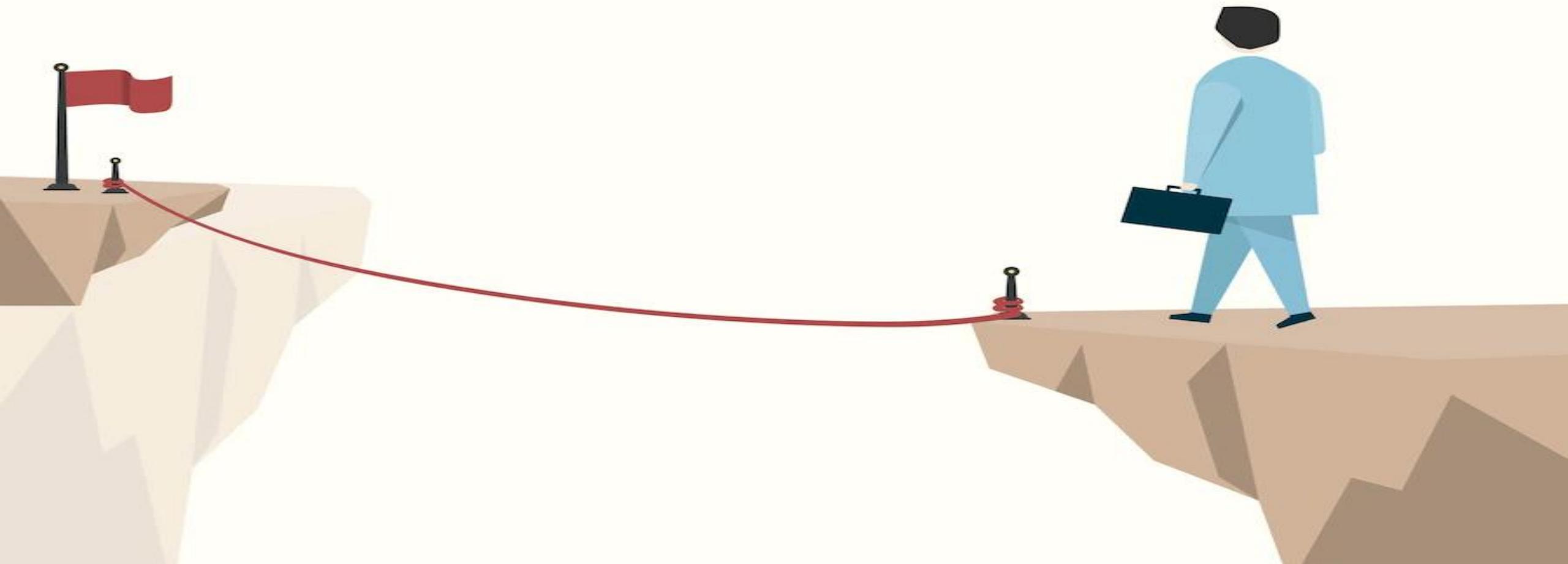
Compensating

Substitutes for a principal control

អត្ថបទ ធមធានគម្រោងសំខាន់សំខាន់របស់អ្នក

ការណាន់ការងារដែលត្រូវការគម្រោងសំខាន់សំខាន់របស់អ្នក ដើម្បីរួមចិត្តរបស់អ្នកទៅការងាររបស់អ្នក

Risk



หลักสูตร วิศวกรความมั่นคงปลอดภัย Security Engineer

ภายใต้โครงการเส้นทางสู่วิศวกรความมั่นคงปลอดภัย สำหรับบัณฑิตจบใหม่สู่การทำงานในภาคอุตสาหกรรม

Risk



What's Risk

Introduction

Organization of all types and sizes face internal and external factors and influences that make it uncertain whether and when they will achieve their objectives. the effect this uncertainty has on an organization's objectives is "risk"

- ✓ Involves uncertainty
- ✓ Something **BAD** Happening
- ✓ Given the **Opportunities**

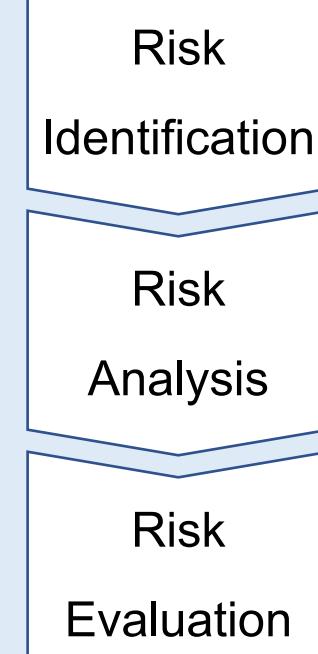


Risk process



Communication & Consultation

Scope, Context, Criteria



Risk Treatment

Monitoring & Review

Recording & Reporting

หลักสูตร วิศวกรความมั่นคงปลอดภัย Security Engineer

ภายใต้โครงการเส้นทางสู่วิศวกรความมั่นคงปลอดภัย สำหรับบัณฑิตจบใหม่สู่การทำงานในภาคอุตสาหกรรม

Risk Matrix

Business Impact Criteria
เกณฑ์สำหรับใช้ประเมินผลกระทบต่อธุรกิจขององค์กร

01

likelihood
โอกาสเกิดขึ้นเหตุการณ์ที่มีผลกระทบต่อธุรกิจ

02

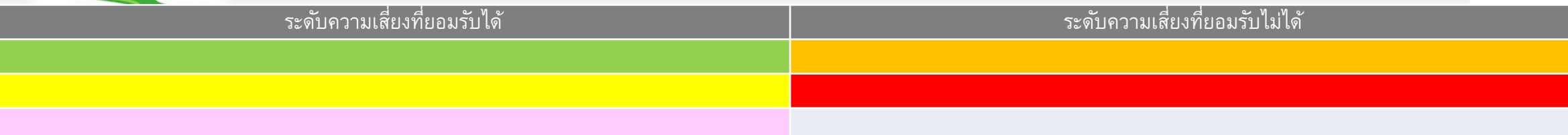


Risk Matrix	1 - Low	2 - Medium	3 - High	4 - Very High	5 - Extremely High
5 - Extremely Likely	5	10	15	20	25
4 - High Likely	4	8	12	16	20
3 - Likely	3	6	9	12	15
2 – Possible	2	4	6	8	10
1 - Unlikely or Rarely	1	2	3	4	5



ระดับความเสี่ยงที่ยอมรับได้

ระดับความเสี่ยงที่ยอมรับไม่ได้



- พื้นที่สีเขียว สีเหลือง สีชมพู เป็นระดับความเสี่ยงที่ต้องมีมาตรการควบคุมและมีการเฝ้าติดตามอย่างสม่ำเสมอ
- ในพื้นที่สีส้มและสีแดง เป็นระดับความเสี่ยงที่ต้องมีแผนควบคุมความเสี่ยง (Risk Treatment Plan) เพื่อลดระดับ Impact หรือ Likelihood และ/หรือ ต้องมีแนวทางการบริหารจัดการโดยเร็ว

Identifying & Assessing Security Risks

Threat & Vulnerability

Threat & Vulnerability	ผลกระทบ			Likelihood	Risk level	แนวทางบริหารความเสี่ยง			
	Security principle impact	Business impact							
	C	I	A	F	O	R	L	P	Business impact consequence

- 1 ผู้บุกรุกสามารถเข้าถึงระบบเนื่องจากการใช้รหัสผ่านที่อ่อนแวง

2

3

4

..

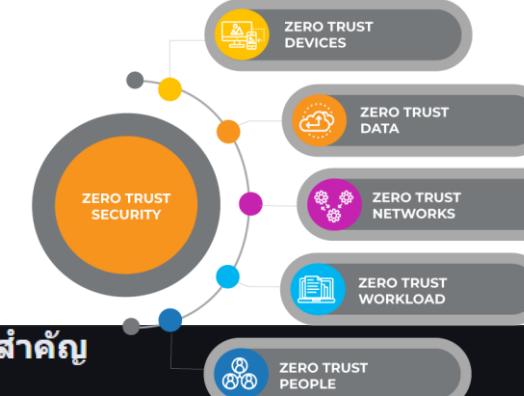
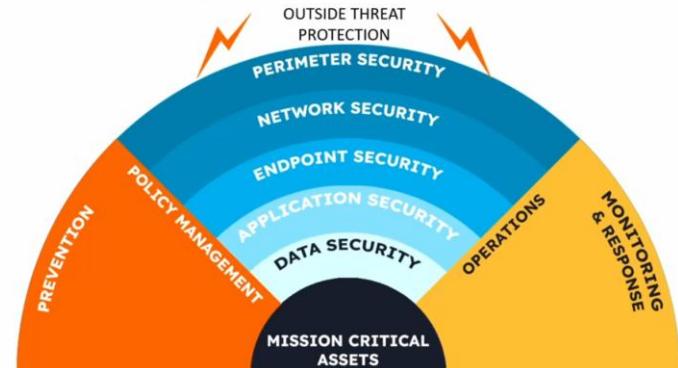


Defense in Depth (Layered Security) & Zero Trust Model

สรุปความแตกต่างและเหมือนกัน

คุณสมบัติ	การป้องกันเชิงลึก (Defense in Depth)	โมเดล Zero Trust
หลักการ	การรักษาความปลอดภัยหลายชั้น	การยืนยันทุกการเข้าถึง
สมมติฐานพื้นฐาน	มีการเชื่อมโยงในเครือข่าย และมีหลายด้านในการป้องกัน	ไม่มีผู้ใช้หรืออุปกรณ์ใดที่น่าเชื่อถือโดยอัตโนมัติ
การทำงาน	สร้างอุปสรรคป้องกันในหลายรูปแบบ	กำหนดสิทธิ์และยืนยันตัวตนอย่างเข้มงวดในทุกการเข้าถึง
ความสัมพันธ์	เป็นกลุ่มยุทธศาสตร์ที่ใช้แนวทางหลายอย่าง	เป็นแนวคิดที่ไม่เป็นหลักการในการกำหนดการรักษาความปลอดภัยให้ครอบคลุม

Defense in Depth/ Layered Defense Model



ความแตกต่างที่สำคัญ

คุณลักษณะ	Defense in Depth (DiD)	Zero Trust Model
แนวคิดหลัก	เน้นการสร้างการป้องกันหลายชั้น (เป็นชั้นๆ) เพื่อให้ผู้โจมตีต้องฝ่าหลายด่านก่อนจะเข้าถึงข้อมูลได้	เน้นหลักการ "ไม่ไว้ใจใคร" ทั้งจากภายในและภายนอกเครือข่าย โดยทุกการเข้าถึงต้องผ่านการตรวจสอบยืนยันเสมอ
พื้นที่ควบคุม	มุ่งเน้นไปที่การสร้าง "ป้อมปราการ" เพื่อป้องก็องเครือข่ายและระบบภายใน โดยเชื่อว่าเมื่อผ่านเข้ามาในเขตปลอดภัยได้แล้ว จะมีความน่าเชื่อถือในระดับหนึ่ง	ไม่สนใจขอบเขตเครือข่าย ทุกการเข้าถึงต้องเป็นความเสี่ยง ไม่ว่าผู้ใช้จะอยู่ภายในหรือภายนอก
การตรวจสอบ	การตรวจสอบจะเข้มงวดที่จุดทางเข้า (Perimeter) เช่น Firewall หลังจากนั้นการตรวจสอบจะลดลงเมื่ออยู่ภายในเครือข่ายแล้ว	ตรวจสอบยืนยันตัวตนและสิทธิ์การเข้าถึงอย่างต่อเนื่องในทุกๆ การร้องขอ และจะเป็นผู้ใช้ภายใน
การอนุญาตสิทธิ์	เมื่อผู้ใช้ได้รับอนุญาตให้เข้าสู่เครือข่ายแล้ว ว่าจะได้รับสิทธิ์ในการเข้าถึงทรัพยากรต่างๆ ภายในตามระดับที่กำหนด	ใช้หลักการลิมิชต์ชั้นต่ำสุด (Least Privilege) โดยให้สิทธิ์การเข้าถึงเท่าที่จำเป็นต่อการทำงานในแต่ละครั้งเท่านั้น
การมองภัยคุกคาม	มุ่งป้องกันการโจมตีจากภายนอกเป็นหลัก และจัดการภัยคุกคามจากภายนอกในกรณีที่จำเป็น	มุ่งป้องกันภัยคุกคามจากทุกทิศทาง ทั้งภายนอกและภายใน โดยเชื่อว่าภัยคุกคามสามารถมาจากทุกที่

Risk not equal a zero

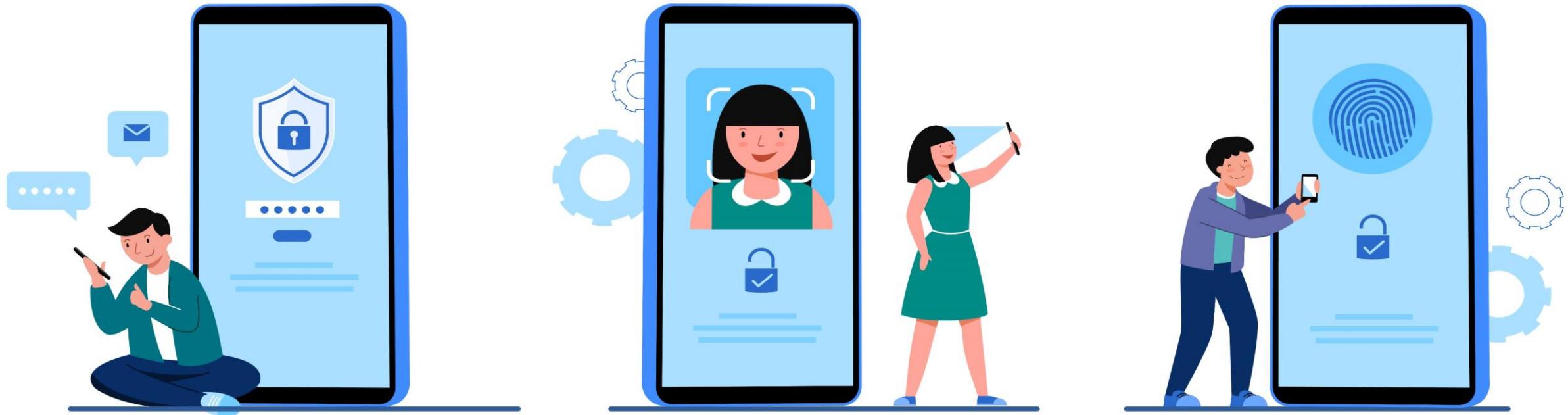
หลักสูตร วิศวกรความมั่นคงปลอดภัย Security Engineer

ภายใต้โครงการเส้นทางสู่วิศวกรความมั่นคงปลอดภัย สำหรับบัณฑิตจบใหม่สู่การทำงานในภาคอุตสาหกรรม



Identity & Access Management (IAM)

Authentication and Authorization concepts



Identity and Access Management



Identification

Associating a valid subject with a computer/network account

Authentication

Challenge to the subject to supply a credential to operate the account

Authorization

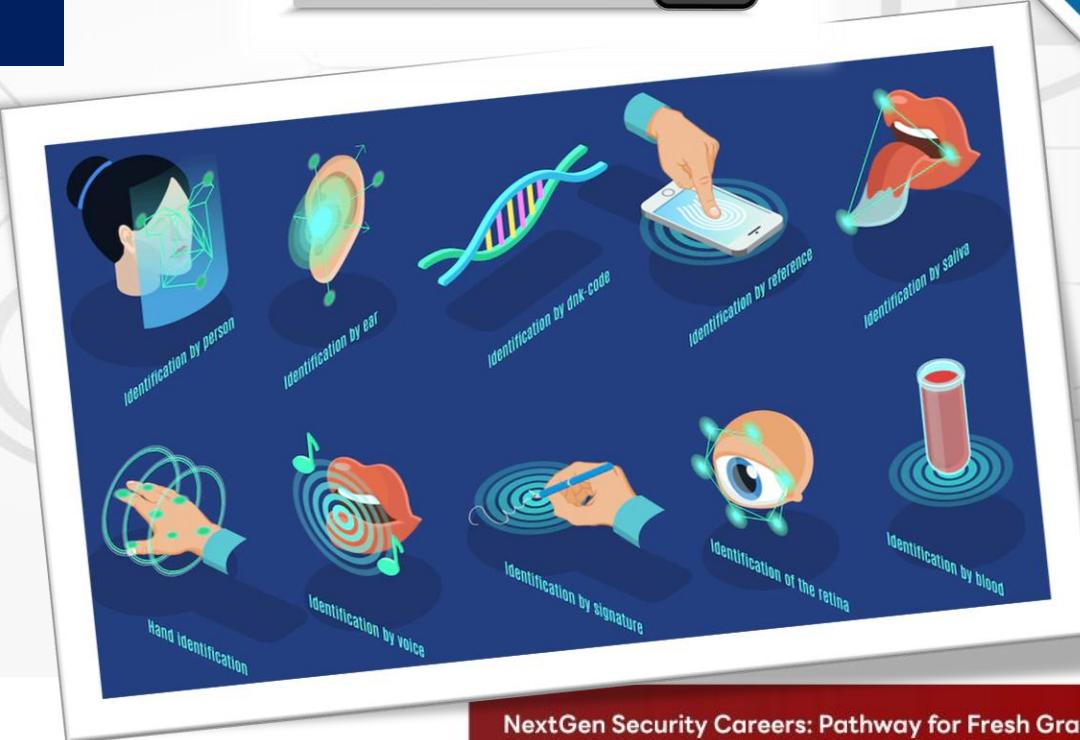
Rights, permissions, or privileges assigned to the account

Accounting

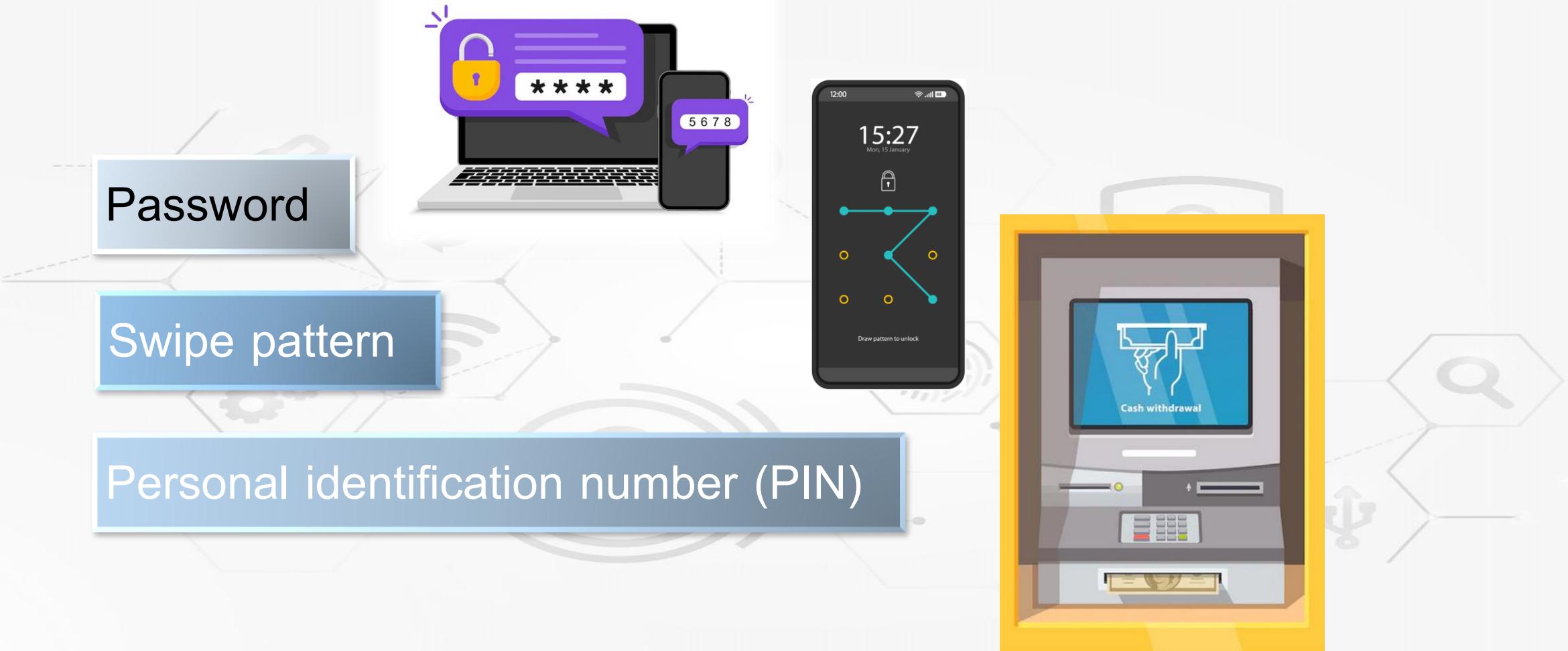
Auditing use of the account

Authentication Factors

Something you know
Something you have
Something you are



Something you know



Something you have

Hardware tokens and fobs



Something you are

Biometric factor

Fingerprint



Facial recognition

Enrollment can be relatively slow

Privacy issues

Prone to relatively high false acceptance/rejection rates/spoofing

Retinal scan

Pattern of blood vessels

Scanning relatively intrusive and complex

Iris scan

Pattern of eye surface

Easier to scan

More vulnerable to spoofing



អត្ថបទ ធមធានរបាយការមំបងគ្រប់គ្រងយោង Security Engineer

រាយការណ៍វិទ្យាសាស្ត្ររបាយការមំបងគ្រប់គ្រងយោង សំខាន់បានកើតបានដូចតាមការការពារនៃការងាររបាយការនេះ

Something you do

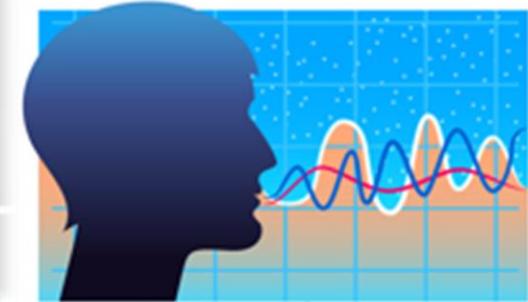
Signature recognition



Gait analysis



Voice recognition



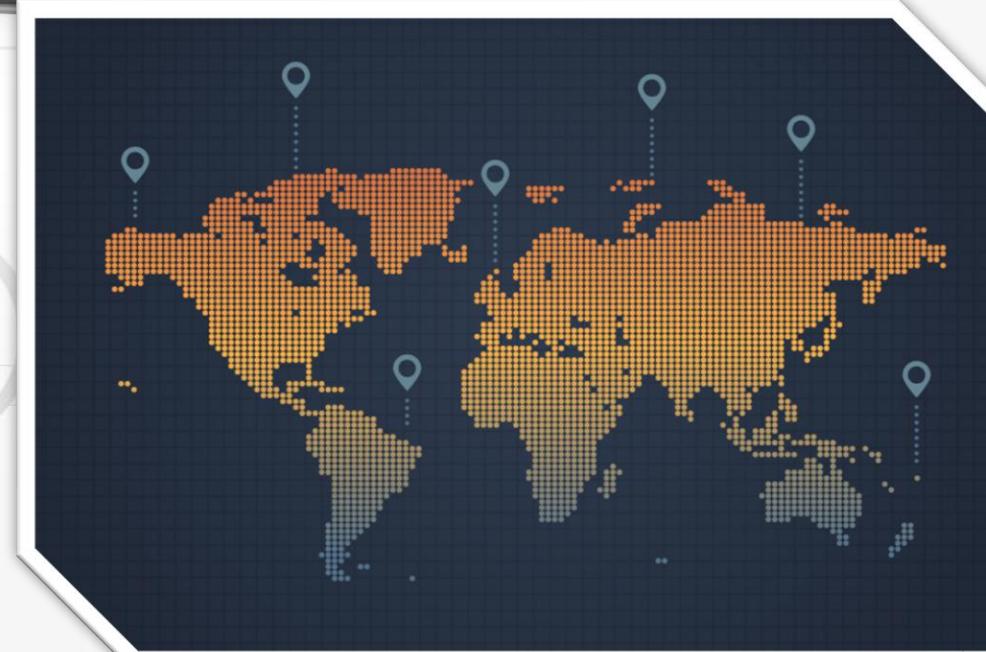
Somewhere you are

Switch port, virtual LAN (VLAN), or wireless network name



Geolocation via location services

IP location



Multifactor Authentication (MFA)

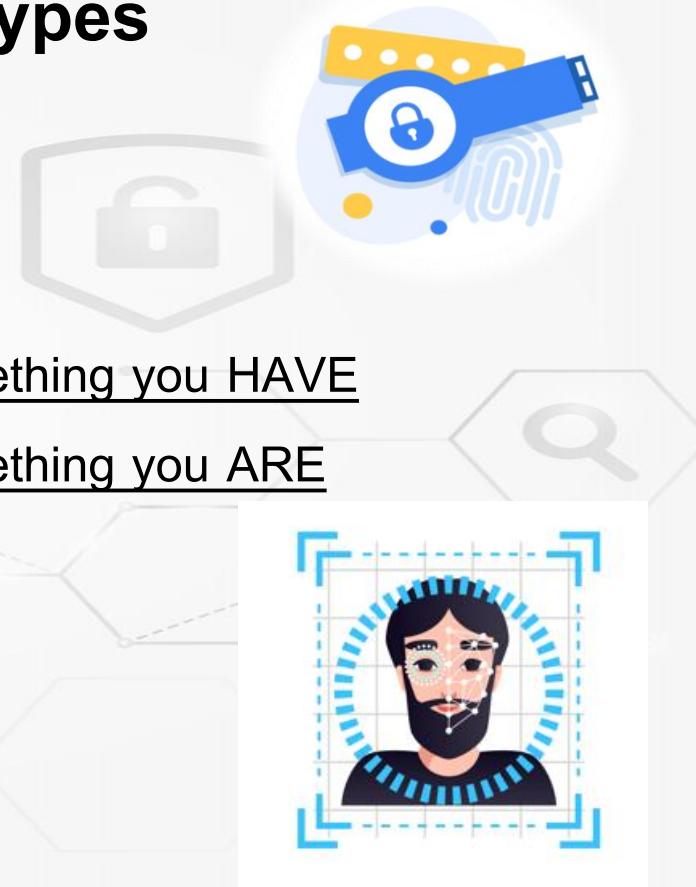
Strong authentication requires two (or three) types

Multifactor authentication Two-factor authentication (2FA)



Something you KNOW and something you HAVE
Something you KNOW and something you ARE

NOT something you KNOW and something else you KNOW



Access Control model

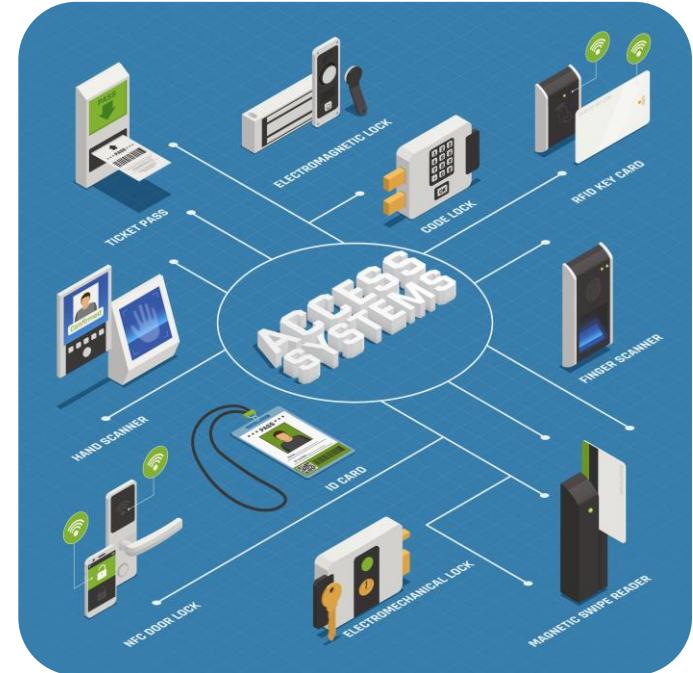
Access control model determines how users receive permissions/rights

Discretionary Access Control (DAC)

- Based on resource ownership
- Access Control Lists (ACLs)
- Vulnerable to compromised privileged user accounts

Role-Based Access Control (RBAC)

- Non-discretionary and more centralized control
- Based on defining roles then allocating users to roles
- Users should only inherit role permissions to perform particular tasks



Least Privilege Principle

forces code to run with the lowest privilege/permission level possible



&

Need to know

the aim is to make it difficult for unauthorized access to occur, without inconveniencing legitimate access.



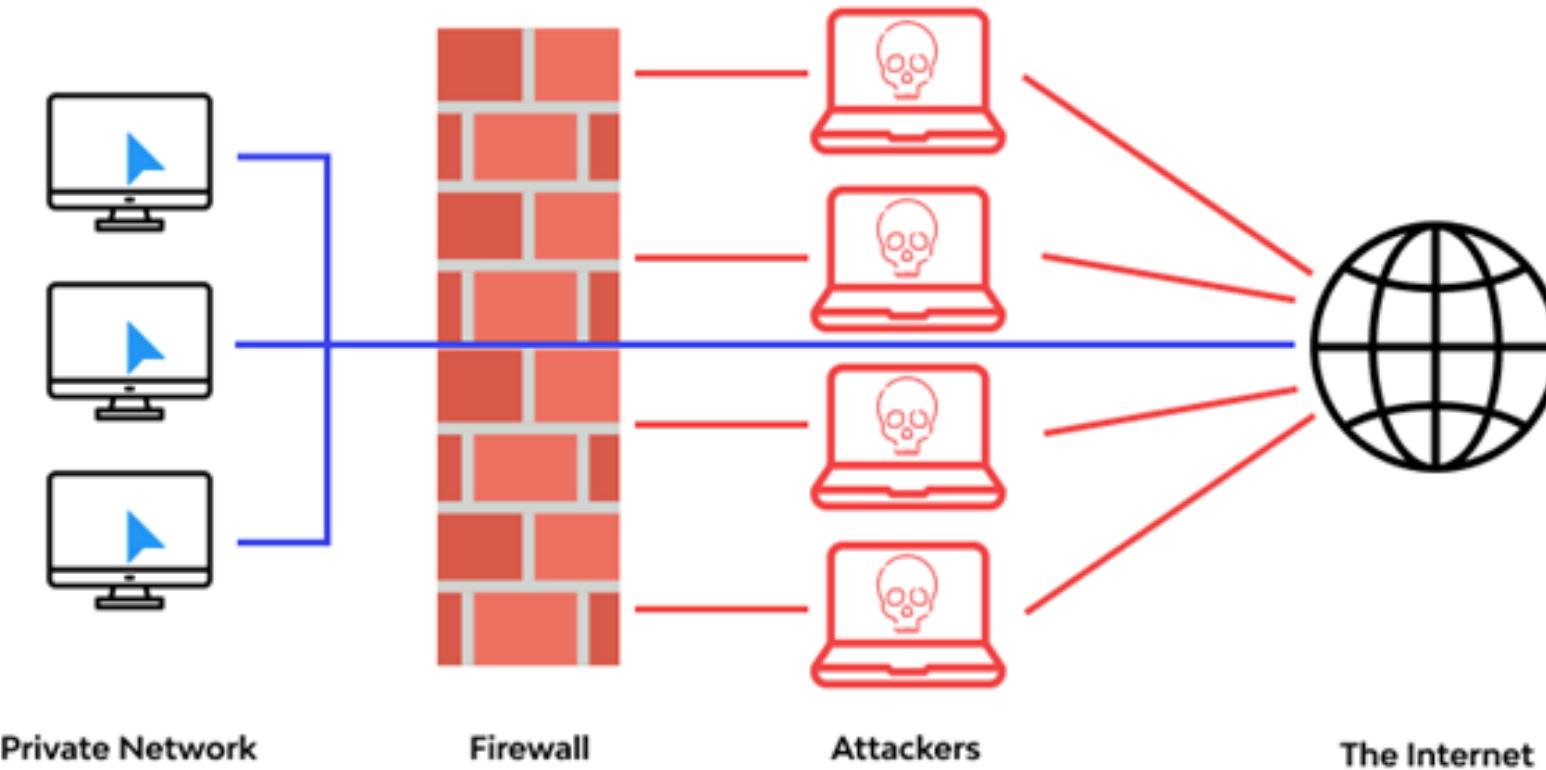
หลักสูตร วิศวกรความมั่นคงปลอดภัย Security Engineer

ภายใต้โครงการเส้นทางสู่วิศวกรความมั่นคงปลอดภัย สำหรับบัณฑิตจบใหม่สู่การทำงานในภาคอุตสาหกรรม

Network & Endpoint Security



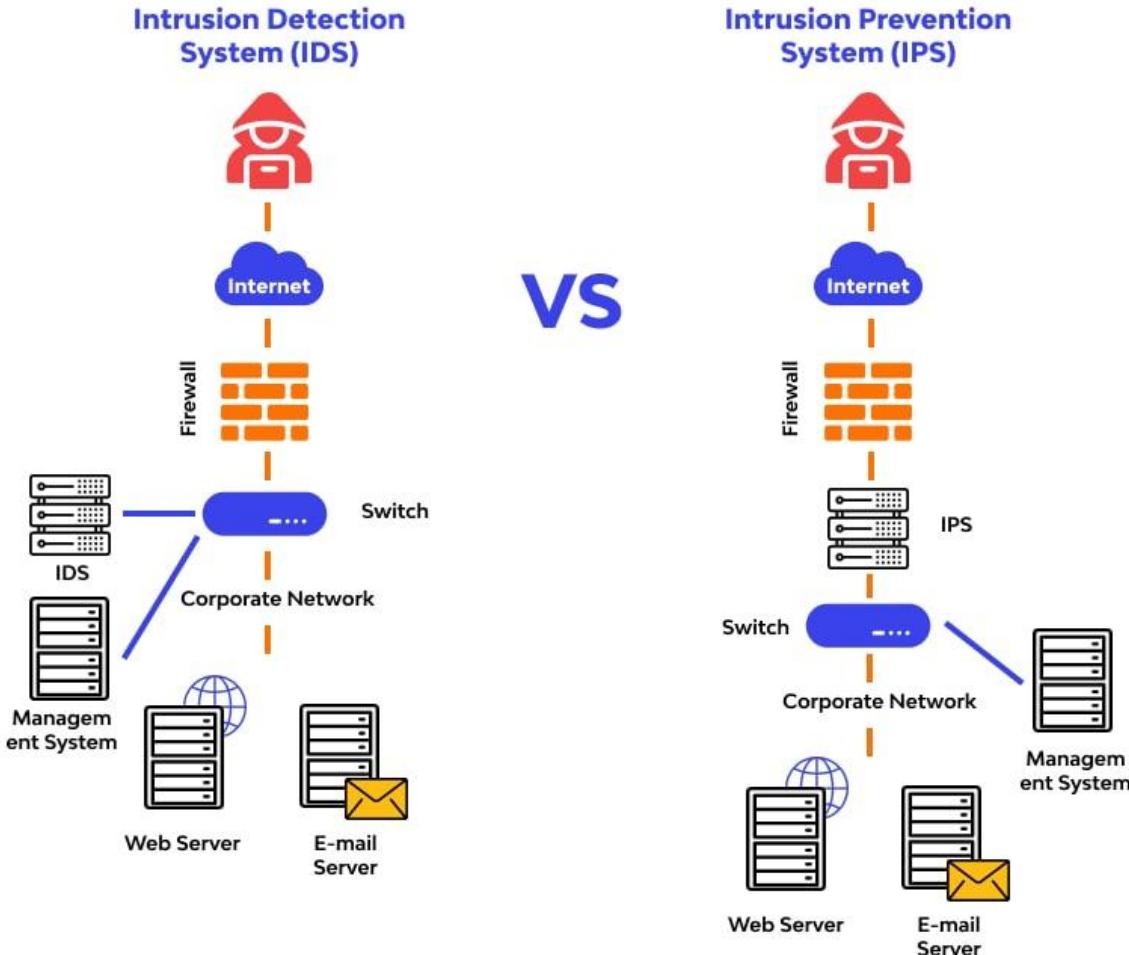
Firewall



ຮັກສູດ ວິສວຍຄວາມນັ້ນຄອງປລອດກໍຍ Security Engineer

ກາຍໃຊ້ໂຄຣກເຮັດກາງສູ່ວິສວຍຄວາມນັ້ນຄອງປລອດກໍຍ ສໍາເຫຼັບນັກສຶກທີ່ກາຈົບໃໝ່ສູ່ກາງກຳຈານໃນກາຄອດສາທະກຣນ

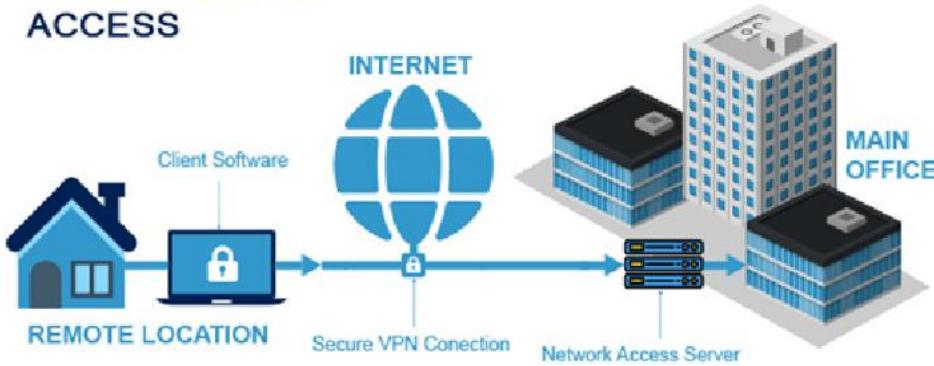
IPS/IDS



Feature	IDS	IPS
Action	Detects and Alerts	Detects and Blocks
Deployment	Out of band	In-line
Traffic latency	No impact	May introduce slight delay
Risk of false positives	Low risk (no block)	Higher risk (may block legitimate traffic)
Use case	Visibility, Threat hunting, Compliance	Real-time protection, threat mitigation

VPN

VPN & REMOTE ACCESS



Type	Compatible	Highlights
Remote Access VPN	บุคคลทั่วไป, พนักงานที่ทำงานจากที่บ้าน	ใช้งานง่าย ปลอดภัย เข้ารหัสข้อมูล
Site-to-Site VPN	องค์กรที่มีสาขา	เชื่อมต่อเครือข่ายสำนักงานโดยตรง
SSL VPN	พนักงานที่ต้องการเข้าถึงระบบจากระยะไกล	ไม่ต้องติดตั้งซอฟต์แวร์ ใช้งานผ่านเบราว์เซอร์
IPSec VPN	ธุรกิจที่ต้องการความปลอดภัยสูง	รองรับการเข้ารหัสที่แข็งแกร่ง
MPLS VPN	บริษัทขนาดใหญ่	เครือข่ายเสถียรและปลอดภัยสูง
Cloud VPN	ธุรกิจที่ใช้ Cloud Computing	ใช้งานง่าย เชื่อมต่อกับ Cloud ได้สะดวก

Endpoint Security

ANTIVIRUS

VS.

EDR

VS.

XDR

- **Database-based:** a set of signatures (characteristics files must match).
- **Human managed.**
- **Pitfalls:**
 1. Malwares now have changing characteristics.
 2. Increasing number of malwares.

- **Behavior-based** (unexpected, unusual, and unwanted), no need for threats to be precisely defined.
- **Automatic**, no need of human intervention.
- **Detects an infection and initiate a response.**
- **One security layer:** focuses on collecting data from the endpoint.

- **Behavior-based.**
- **Automatic**, no need of human intervention.
- **Detects an infection and initiate a response.**
- **Multiple security layers:** endpoints, cloud infrastructure, mobile devices etc.
- **Single solution:** simplifies an organization's security architecture.

Windows Hardening



CIS Microsoft Windows Server 2016 RTM (Release 1607) Benchmark

v1.1.0 - 10-31-2018

1 Account Policies	39
1.1 Password Policy.....	39
1.1.1 (L1) Ensure 'Enforce password history' is set to '24 or more password(s)' (Scored)	39
1.1.2 (L1) Ensure 'Maximum password age' is set to '60 or fewer days, but not 0' (Scored)	42
1.1.3 (L1) Ensure 'Minimum password age' is set to '1 or more day(s)' (Scored)	44
1.1.4 (L1) Ensure 'Minimum password length' is set to '14 or more character(s)' (Scored)	46
1.1.5 (L1) Ensure 'Password must meet complexity requirements' is set to 'Enabled' (Scored)	48
1.1.6 (L1) Ensure 'Store passwords using reversible encryption' is set to 'Disabled' (Scored)	51
1.2 Account Lockout Policy.....	53
1.2.1 (L1) Ensure 'Account lockout duration' is set to '15 or more minute(s)' (Scored)	53
1.2.2 (L1) Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0' (Scored)	55
1.2.3 (L1) Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)' (Scored)	57
2 Local Policies	59
19.7.33 Tablet PC	870
19.7.34 Task Scheduler	870
19.7.35 Windows Calendar	871
19.7.36 Windows Color System	871
19.7.37 Windows Defender SmartScreen	871
19.7.38 Windows Error Reporting	871
19.7.39 Windows Hello for Business (formerly Microsoft Passport for Work)	872
19.7.40 Windows Installer	873
19.7.40.1 (L1) Ensure 'Always install with elevated privileges' is set to 'Disabled' (Scored)	873
19.7.41 Windows Logon Options	875
19.7.42 Windows Mail	875
19.7.43 Windows Media Center	875
19.7.44 Windows Media Player	876
19.7.44.2.1 (L2) Ensure 'Prevent Codec Download' is set to 'Enabled' (Scored)	876

Password policy Hardening

1 Account Policies

This section contains recommendations for account policies.

1.1 Password Policy

This section contains recommendations for password policy.

1.1.1 (L1) Ensure 'Enforce password history' is set to '24 or more password(s)' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines the number of renewed, unique passwords that have to be associated with a user account before you can reuse an old password. The value for this policy setting must be between 0 and 24 passwords. The default value for Windows Vista is 0 passwords, but the default setting in a domain is 24 passwords. To maintain the effectiveness of this policy setting, use the Minimum password age setting to prevent users from repeatedly changing their password.

The recommended state for this setting is: 24 or more password(s).

Rationale:

The longer a user uses the same password, the greater the chance that an attacker can determine the password through brute force attacks. Also, any accounts that may have been compromised will remain exploitable for as long as the password is left unchanged. If password changes are required but password reuse is not prevented, or if users continually reuse a small number of passwords, the effectiveness of a good password policy is greatly reduced.

If you specify a low number for this policy setting, users will be able to use the same small number of passwords repeatedly. If you do not also configure the Minimum password age setting, users might repeatedly change their passwords until they can reuse their original password.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to 24 or more password(s):

```
Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Enforce password history
```

Impact:

The major impact of this configuration is that users must create a new password every time they are required to change their old one. If users are required to change their passwords to new unique values, there is an increased risk of users who write their passwords somewhere so that they do not forget them. Another risk is that users may create passwords that change incrementally (for example, password01, password02, and so on) to facilitate memorization but make them easier to guess. Also, an excessively low value for the Minimum password age setting will likely increase administrative overhead, because users who forget their passwords might ask the help desk to reset them frequently.

Default Value:

24 passwords remembered on domain members. 0 passwords remembered on stand-alone servers.

Linux Hardening



CIS Ubuntu Linux 18.04 LTS Benchmark

v1.0.0 - 08-13-2018



1 Initial Setup.....	20
1.1 Filesystem Configuration	20
1.1.1.1 Ensure mounting of cramfs filesystems is disabled (Scored)	21
1.1.1.2 Ensure mounting of freevxs filesystems is disabled (Scored)	23
1.1.1.3 Ensure mounting of jffs2 filesystems is disabled (Scored)	25
1.1.1.4 Ensure mounting of hfs filesystems is disabled (Scored)	27
1.1.1.5 Ensure mounting of hfsplus filesystems is disabled (Scored)	29
1.1.1.6 Ensure mounting of udf filesystems is disabled (Scored)	31
1.1.2 Ensure separate partition exists for /tmp (Scored).....	33
1.1.3 Ensure nodev option set on /tmp partition (Scored)	35
1.1.4 Ensure nosuid option set on /tmp partition (Scored).....	36
1.1.5 Ensure separate partition exists for /var (Scored)	37
1.1.6 Ensure separate partition exists for /var/tmp (Scored)	38
1.1.7 Ensure nodev option set on /var/tmp partition (Scored)	40
1.1.8 Ensure nosuid option set on /var/tmp partition (Scored)	41
1.1.9 Ensure noexec option set on /var/tmp partition (Scored)	42
6.2 User and Group Settings.....	369
6.2.1 Ensure password fields are not empty (Scored)	369
6.2.2 Ensure no legacy "+" entries exist in /etc/passwd (Scored)	371
6.2.3 Ensure no legacy "+" entries exist in /etc/shadow (Scored).....	372
6.2.4 Ensure no legacy "+" entries exist in /etc/group (Scored)	373
6.2.5 Ensure root is the only UID 0 account (Scored).....	374
6.2.6 Ensure root PATH Integrity (Scored)	375
6.2.7 Ensure all users' home directories exist (Scored)	377
6.2.8 Ensure users' home directories permissions are 750 or more restrictive (Scored)	378
6.2.9 Ensure users own their home directories (Scored)	380
6.2.10 Ensure users' dot files are not group or world writable (Scored)	382
6.2.11 Ensure no users have .forward files (Scored)	384
6.2.12 Ensure no users have .netrc files (Scored)	386
6.2.13 Ensure users' .netrc Files are not group or world accessible (Scored)	388
6.2.14 Ensure no users have .rhosts files (Scored)	391
6.2.15 Ensure all groups in /etc/passwd exist in /etc/group (Scored)	393
6.2.16 Ensure no duplicate UIDs exist (Scored)	394
6.2.17 Ensure no duplicate GIDs exist (Scored)	395
6.2.18 Ensure no duplicate user names exist (Scored)	397
6.2.19 Ensure no duplicate group names exist (Scored)	398
6.2.20 Ensure shadow group is empty (Scored)	400

Disable unused filesystems

1 Initial Setup

Items in this section are advised for all systems, but may be difficult or require extensive preparation after the initial setup of the system.

1.1 Filesystem Configuration

Directories that are used for system-wide functions can be further protected by placing them on separate partitions. This provides protection for resource exhaustion and enables the use of mounting options that are applicable to the directory's intended use. Users' data can be stored on separate partitions and have stricter mount options. A user partition is a filesystem that has been established for use by the users and does not contain software for system operations.

The recommendations in this installation. If the system is already installed, perform a full system repartitioning before repartitioning.

Note: If you are repartitioning, make sure that the data has been copied over to the new partition. If the data was in the old partition, it will be lost. If the new partition that will be masked, it must be mounted in single-user mode with no root password. If the data is in the /tmp directory, this data will be lost. If the data is mounted unless it is removed, it will be lost.

Audit:

Run the following commands and verify the output is as indicated:

```
# modprobe -n -v cramfs
install /bin/true
# lsmod | grep cramfs
<No output>
```

Remediation:

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf

Example: vim /etc/modprobe.d/cramfs.conf

and add the following line:

```
install cramfs /bin/true
```

Run the following command to unload the cramfs module:

```
# rmmod cramfs
```

1.1.1 Disable unused filesystems

A number of uncommon filesystem types are supported under Linux. Removing support for unneeded filesystem types reduces the local attack surface of the system. If a filesystem type is not needed it should be disabled. Native Linux file systems are designed to ensure that built-in security controls function as expected. Non-native filesystems can lead to unexpected consequences to both the security and functionality of the system and should be used with caution. Many filesystems are created for niche use cases and are not maintained and supported as the operating systems are updated and patched. Users of non-native filesystems should ensure that there is attention and ongoing support for them, especially in light of frequent operating system changes.

Standard network connectivity and Internet access to cloud storage may make the use of non-standard filesystem formats to directly attach heterogeneous devices much less attractive.

Note: This should not be considered a comprehensive list of filesystems. You may wish to consider additions to those listed here for your environment.

1.1.1.1 Ensure mounting of cramfs filesystems is disabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

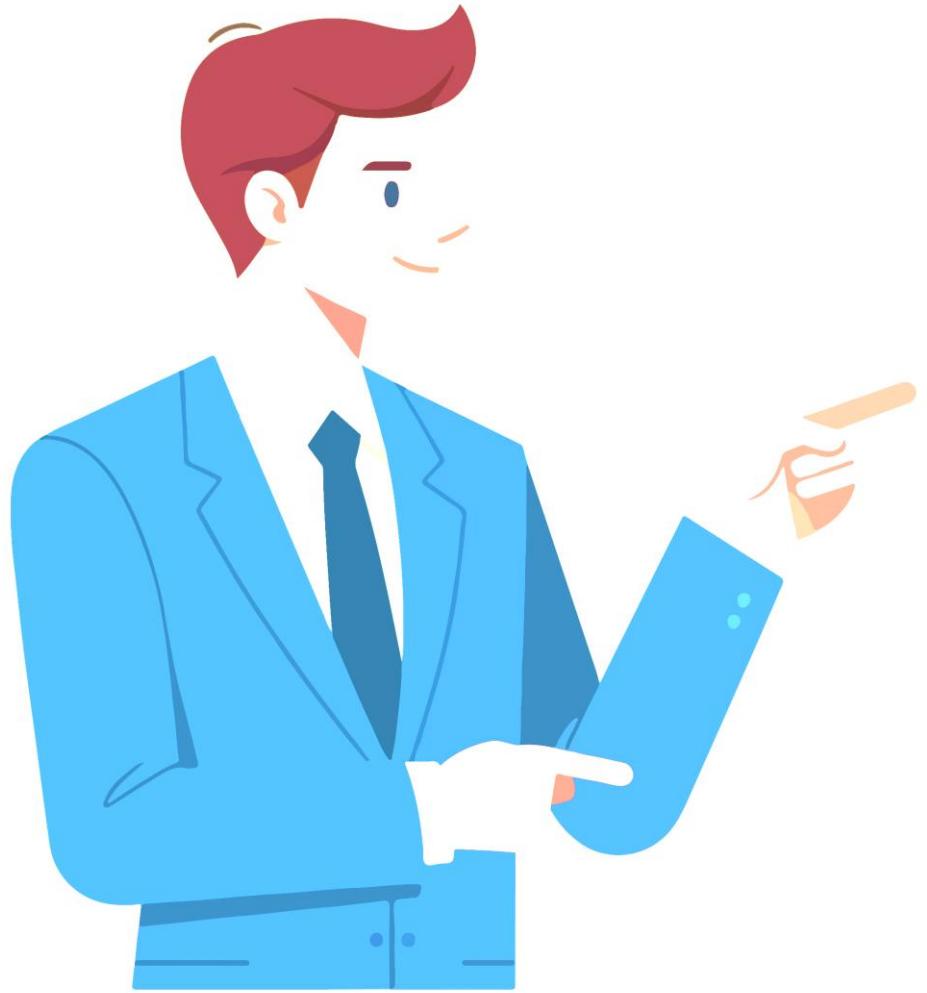
The cramfs filesystem type is a compressed read-only Linux filesystem embedded in small footprint systems. A cramfs image can be used without having to first decompress the image.

Rationale:

Removing support for unneeded filesystem types reduces the local attack surface of the server. If this filesystem type is not needed, disable it.

หลักสูตร วิศวกรความมั่นคงปลอดภัย Security Engineer

ภายใต้โครงการเส้นทางสู่วิศวกรความมั่นคงปลอดภัย สำหรับบัณฑิตจบใหม่สู่การทำงานในภาคอุตสาหกรรม



Security Awareness & Incident Response

Awareness



□ Topics for security awareness

- Overview of security policies
- Incident response procedures
- Site security procedures
- Data handling
- Password and account management
- Awareness of social engineering and malware threats
- Secure use of software such as browsers and email clients

Malware



Phishing



หลักสูตร วิศวกรความมั่นคงปลอดภัย Security Engineer

ภายใต้โครงการเส้นทางสู่วิศวกรความมั่นคงปลอดภัย สำหรับบัณฑิตจบใหม่สู่การทำงานในภาคอุตสาหกรรม

**THINK
before
you click.**





Hints that this is not a legitimate e-mail from Bellevue College

-----Original Message-----

From: Webmaster [mailto:logon@instructor.net]

Sent: Friday, September 23, 2011 8:40 AM

To: [REDACTED]

Subject: Final Notification :

1

อีเมลผู้ส่งไม่ใช่ที่อยู่ของสถาบัน

2

ขึ้นต้นด้วยคำก้าวๆไป

This is a follow-up to the previous email that was sent to you from our secure server through the admin officer to verify your informations. Due to the congestion of email users, the Admin unit would be shutting down all unused Accounts, You will have to re-confirm your E-mail account by filling out your Login Information below.

* Your Login Username:
* Your Login Password:
* Your Date of Birth:
* Your Country Or Territory:
* Send to ; webmail_accountlogin@instructor.net

3

ขอพาสวีร์ดและข้อมูลส่วนตัว

After following the instructions in the above, your email account will not be interrupted and will continue as normal. We thank you for your prompt attention to this matter.

Please understand that this is a security measure intended to help protect your account. We apologise for any inconvenience.

Failure to verify and re-confirm your email account membership details within three days, your email online account will be SUSPENDED!

4

ให้รับตอบกลับอย่างรวดเร็ว

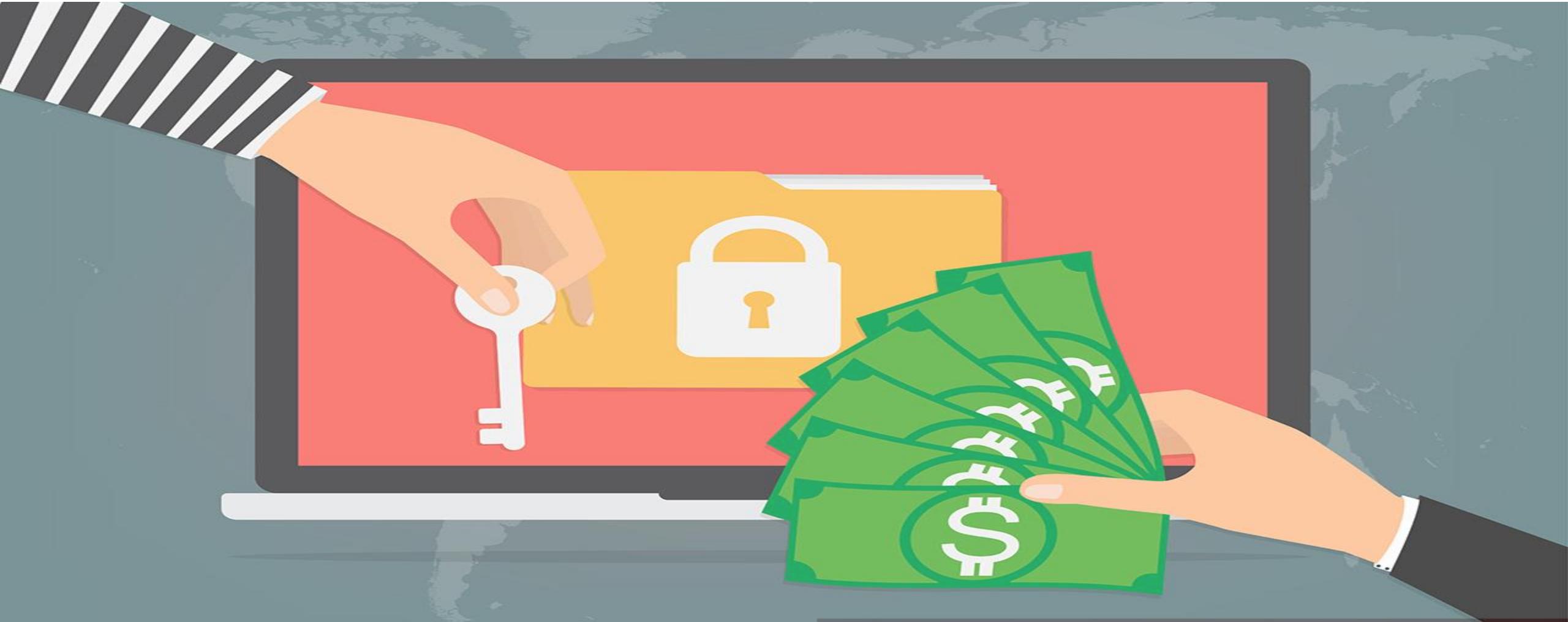
Warning Code:VX2G99AAJ

Thank you for using !

The Admin Team

Dear Email User:-

Ransomware



Ransomware



The screenshot shows a ransomware message box with a red background. At the top left is a large white padlock icon on a red gradient background. To its right, the text "Ooops, your files have been encrypted!" is displayed in white. In the top right corner, there is a language selection dropdown set to "English". Below the main title, the heading "What Happened to My Computer?" is shown in bold black text. The message explains that important files are encrypted and inaccessible. It urges the user not to waste time looking for recovery methods, stating that nobody can recover files without their decryption service. A yellow box on the left side displays a warning: "Payment will be raised on 5/16/2017 00:47:55" above a progress bar, followed by "Time Left 02: 23: 57: 37". Another yellow box below it shows "Your files will be lost on 5/20/2017 00:47:55" above a progress bar, also with "Time Left 06: 23: 57: 37". The bottom section contains the heading "Can I Recover My Files?", followed by text assuring the user they can recover files safely if they pay. It details the payment process, mentioning Bitcoin acceptance, current price checks, and specific payment instructions. The text ends with a note about free events for users who can't afford to pay.

Ooops, your files have been encrypted!

English

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am CEST.

Payment will be raised on
5/16/2017 00:47:55

Time Left
02: 23: 57: 37

Your files will be lost on
5/20/2017 00:47:55

Time Left
06: 23: 57: 37

How to protect yourself?

1



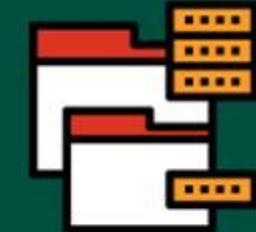
Do not open
suspicious
e-mail
attachments or
downloaded files

2



Update your
operating system
and software
promptly

3



Regularly make
backups of all
important files

หลักสูตร วิศวกรรมความมั่นคงปลอดภัย Security Engineer

ภายใต้โครงการเส้นทางสู่วิศวกรความมั่นคงปลอดภัย สำหรับบัณฑิตจบใหม่สู่การทำงานในภาคอุตสาหกรรม

Social Engineering



หลักสูตร วิศวกรความมั่นคงปลอดภัย Security Engineer

ภายใต้โครงการเส้นทางสู่วิศวกรความมั่นคงปลอดภัย สำหรับบุคคลที่สนใจเรียนรู้การทำงานในภาคอุตสาหกรรม

Social Engineering



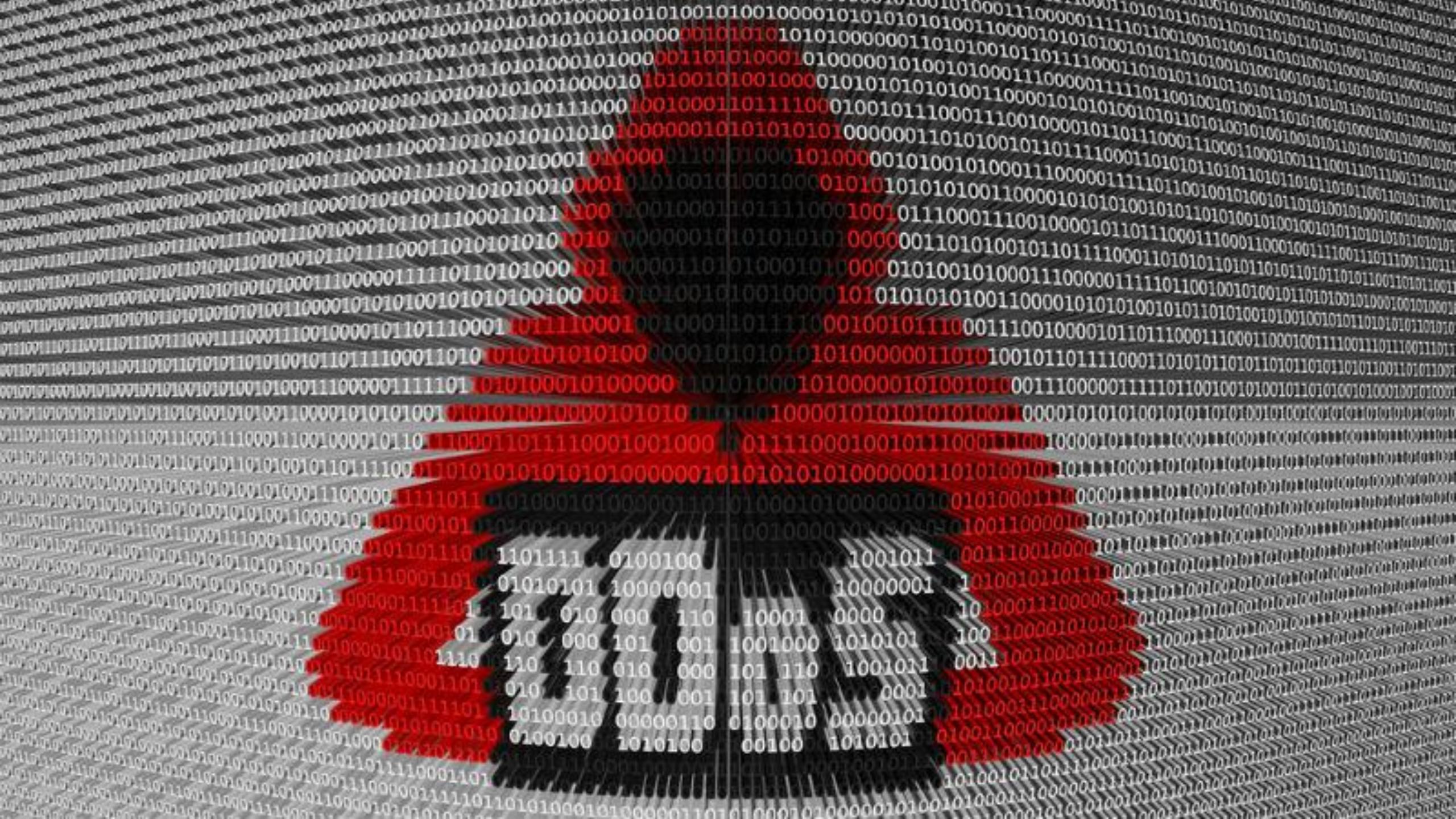
แจก พรี ไม่เสียเงิน เจพารคนเกิด กรกฎาคม
พิมพ์ “วันเกิด” ให้โพสต์
รับจี้พญาครุฑรับทรัพย์ ด่วน มีติดตัวแล้วดี

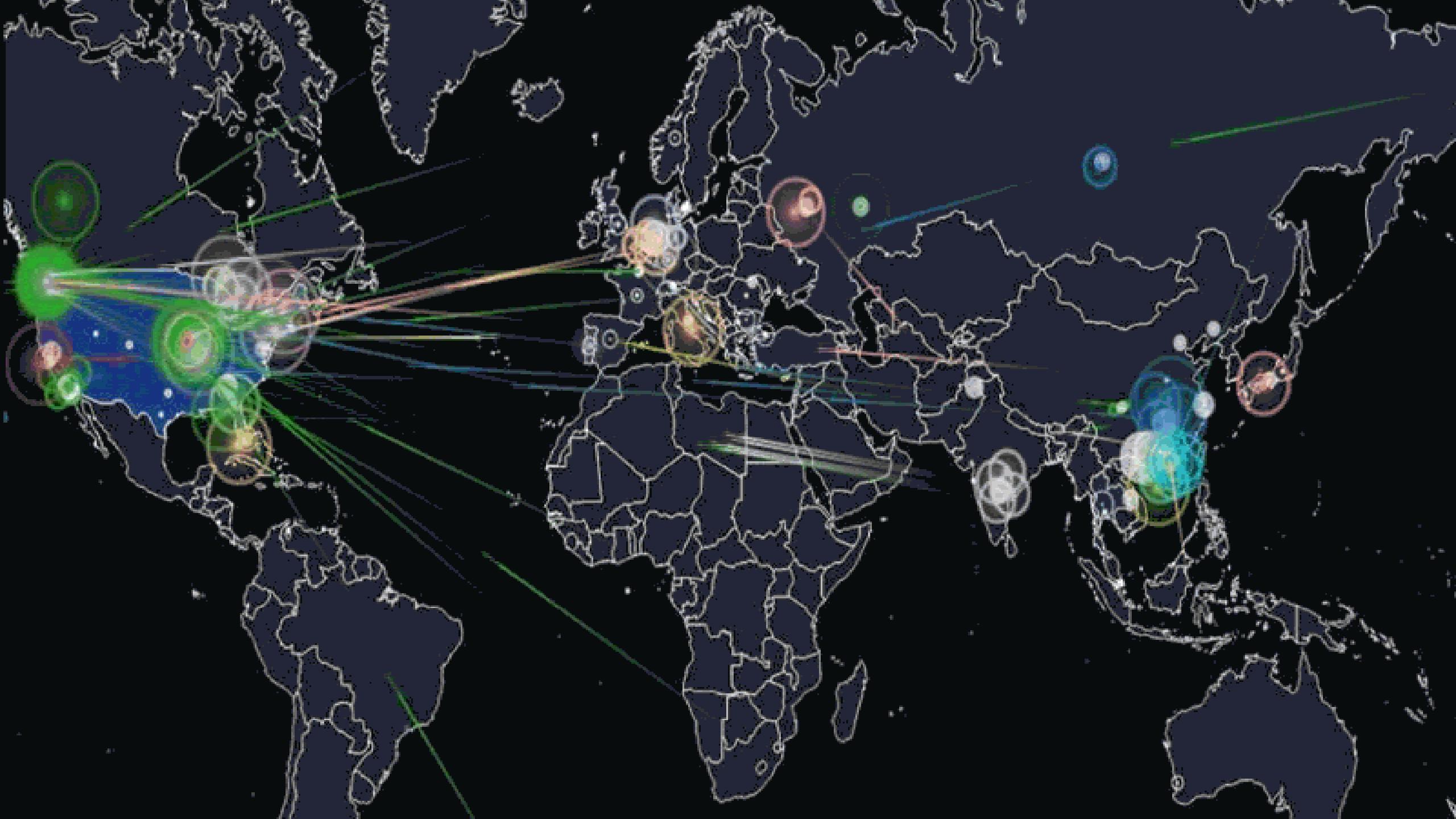
MESSENGER

รับจี้ เจพารคน กด>>

Send Message

- เกิดวันที่ 30 กรกฎาคม วันอาทิตย์
Like · Reply · 6d
- ศกศ ที่ 10 กรกฎาคม 2524 ค
Like · Reply · 1d
- เกิดวันจันทร์ที่ 19 กรกฎาคม 2519 ค
Like · Reply · 1w
- สวัสดีค่ะเกิด 24 กรกฎาคม 2508 ค
Like · Reply · 5d
- วันที่ 5 กรกฎาคม 2521
Like · Reply · 4d
- วันอาทิตย์ที่ 29 กรกฎาคม 2527
Like · Reply · 1d
- อาทิตย์ 4 กรกฎาคม 2536 ค
Like · Reply · 2w
- สวัสดีค่ะเกิดวันที่ 29 กรกฎาคม 2491
Like · Reply · 5d
- สวัสดีค่ะ เกิดวันจันทร์ที่ 22 กค 2511 ค. พอมีห
เจ็บค้าบ้มยังค
Like · Reply · 2w
- 12 กรกฎาคม 2520 ค
Like · Reply · 21h
- 31 กรกฎาคม 2536
- รับสติ๊กเก็ตวันที่ 12 กค 2517 วันศุกร์
Like · Reply · 2d
- 20 กรกฎาคม วันอาทิตย์
Like · Reply · 5d
- พธที่ 14 กรกฎาคม 2508
Like · Reply · 1w
- 11 กรกฎาคม วันเสาร์
Like · Reply · 3d
- 21 กค. 2496 วันอังคาร
Like · Reply · 4d
- 24 กรกฎาคม 2518
Like · Reply · 1w
- วันเสาร์ที่ 2 กรกฎาคม 2531
Like · Reply · 2d
- วันที่ 27 กรกฎาคม 2525
Like · Reply · 3d
- กิตวันอังคารที่ 8 กรกฎาคม
Like · Reply · 3d
- 7 กรกฎาคม
สงมาเลย 159 น. 3 ต.
ลง อ. อุบลราชธานี 080-
Like · Reply · 2w
- View more comments





អាសយដ្ឋាន ធម្មតាគម្រោងកសិករម្យ Security Engineer

ការណាន់កម្រិតជាអនុវត្តន៍ការងារសៀវភៅគម្រោងកសិករម្យ សំខាន់បានកើតការងារក្នុងការងារកសិករម្យ



Best Practices

Implementing Security Policies & Governance



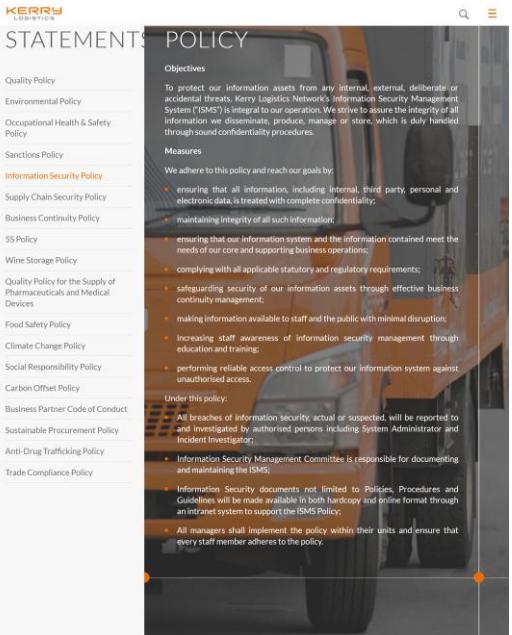
Contents		Page
Foreword		iv
Introduction		v
1 Scope		1
2 Normative references		1
3 Terms and definitions		1
4 Context of the organization		1
4.1 Understanding the organization and its context		1
4.2 Understanding the needs and expectations of interested parties		1
4.3 Determining the scope of the information security management system		2
4.4 Information security management system		2
5 Leadership		2
5.1 Leadership and commitment		2
5.2 Policy		3
5.3 Organizational roles, responsibilities and authorities		3
6 Planning		3
6.1 Actions to address risks and opportunities		3
6.1.1 General		3
6.1.2 Information security risk assessment		4
6.1.3 Information security risk treatment		4
6.2 Information security objectives and planning to achieve them		5
7 Support		6
7.1 Resources		6
7.2 Competence		6
7.3 Awareness		6
7.4 Communication		6
7.5 Documented information		6
7.5.1 General		6
7.5.2 Creating and updating		7
7.5.3 Control of documented information		7
8 Operation		7
8.1 Operational planning and control		7
8.2 Information security risk assessment		8
8.3 Information security risk treatment		8
9 Performance evaluation		8
9.1 Monitoring, measurement, analysis and evaluation		8
9.2 Internal audit		8
9.2.1 General		8
9.2.2 Internal audit programme		9
9.3 Management review		9
9.3.1 General		9
9.3.2 Management review inputs		9
9.3.3 Management review results		9
10 Improvement		10
10.1 Continual improvement		10
10.2 Nonconformity and corrective action		10
Annex A (normative) Information security controls reference		11
Bibliography		19

Annex A.5.1

Policies for information security

Control

Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.



Policies to organizational

- Personnel
- Third-party
- Data
- Credential policies
- Organizational



Personnal

- Acceptable use policy
- Job rotation
- Mandatory vacation
- Separation of duties
- Least privilege
- Clean desk space
- Background checks
- Non-disclosure agreement (NDA)
- Social media analysis
- Onboarding
- Offboarding
- User training



Third party

- Vendors
- Supply chain
- Business partners
- Service level agreement (SLA)
- Memorandum of understanding (MOU)
- Measurement systems analysis (MSA)
- Business partnership agreement (BPA)
- End of life (EOL)
- End of service life (EOSL)
- NDA



Data classification

Public (unclassified)

- No confidentiality, but integrity and availability are important

Confidential (secret)

- Subject to administrative and/or technical access controls

Critical (top secret)

Proprietary

- Owned information of commercial value

Private/personal data

- Data that can identify an individual

Sensitive

- Special categories of personal data, such as beliefs, ethnic origin, or sexual orientation

Credential

- Personnel
- Third-party
- Devices
- Service accounts
- Administrator/root accounts



Organizational [Asset Management]

- Inventory/asset management database**
- Asset identification and standard naming conventions**
 - Barcodes and RFID tags
 - Standard naming conventions for asset IDs
 - Attribute fields and tags
- Internet protocol (IP) schema**
 - Static allocation versus DHCP ranges
 - IP address management (IPAM) software suites



Organizational [Configuration Management]

- Service assets**
- Configuration items (CIs)**
 - Assets that require configuration management
- Baseline configuration**
- Configuration management system (CMS)**
- Creating and updating diagrams**
 - Workflows
 - Physical and logical network topologies
 - Network rack layouts



Organizational [Change management]

❑ Change control

- Assess whether a change should be made
- Classifying change (reactive, proactive, risk)
- Request for Change (RFC)
- Change Advisory Board (CAB)

❑ Change management

- Ensure changes are applied with minimum disruption
- Rollback plan



Cyber Hygiene

หลักเกณฑ์ขั้นตอนที่จำเป็น

1. การตั้งค่าระบบให้มีความปลอดภัย

(Security Baseline and Hardening)
กำหนดและตั้งค่าให้สอดคล้องกับมาตรฐานสากลและภาพรวมด้าน IT

2. การป้องกันระบบจาก Malware

(Malware Protection)
ตรวจจับและป้องกัน malware ได้เท่าทันกับคุกคาม

3. การบริหารจัดการช่องโหว่

(Security Patch Management)
กำหนดกระบวนการบริหารจัดการ security patch

4. การจัดการสิทธิ์สูงของระบบ

(Privilege User ID Management)
ควบคุมและจำกัดการใช้บัญชีผู้ใช้สิทธิ์สูงอย่างเข้มงวด

5. การพิสูจน์ตัวตนอย่างปลอดภัย

(Multi - Factor Authentication)
มีการพิสูจน์ตัวตนแบบ MFA ในบัญชีผู้ใช้สิทธิ์สูง เช่นบัญชีผู้ใช้งานที่มีความเสี่ยง

6. การทดสอบหาช่องโหว่

(VA & Pentest)
ประเมินช่องโหว่และทดสอบเจาะระบบอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง

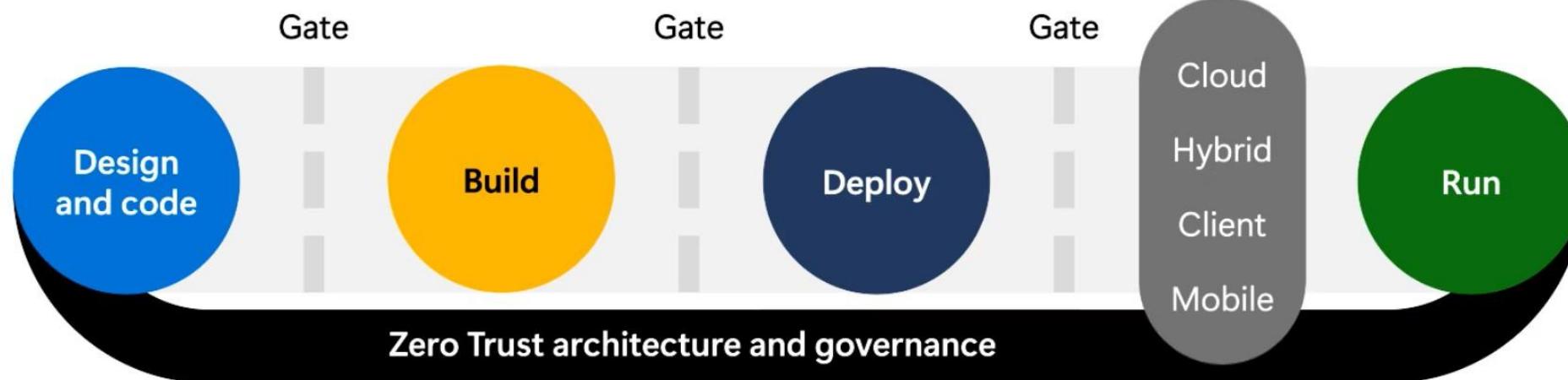
Secure Coding Practices



Code review

Statics Application Security Testing

Dynamic application security testing



The Future of Cybersecurity



អាណាសុទ្ធគិសនុវត្ថុរបាយការពេលដែលមិនមែនការងាររបាយការ

ការងារដែលមិនមែនការងាររបាយការ គឺជាការងារដែលមិនមែនការងាររបាយការ ត្រូវបានធ្វើឡើងដោយការងាររបាយការ

Ai Security



Automated Threat Intelligence

