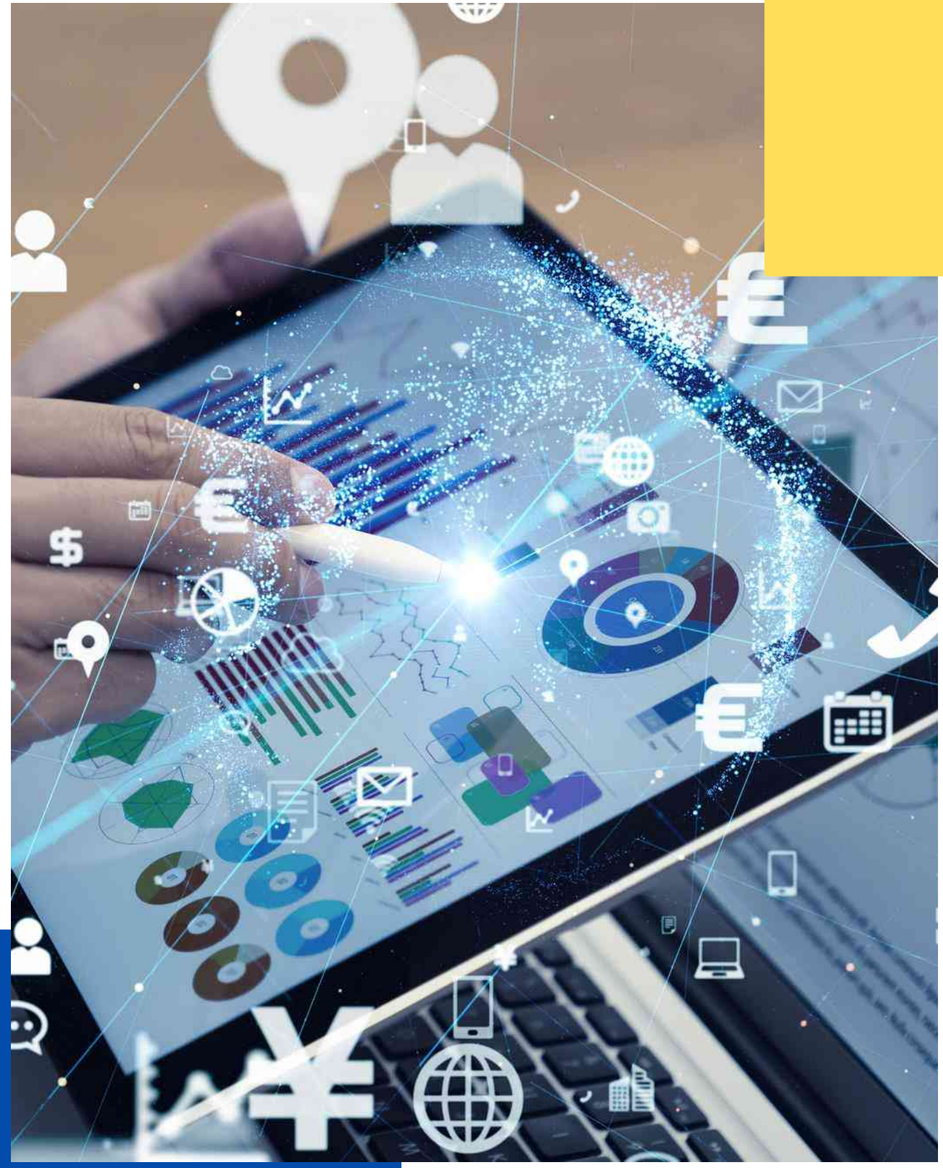
SERVICE PACKAGE
Cybersecurity Rating

TRISx

October 2022 (Ver. 14)



Benefits of Cybersecurity Management

ลดความเสี่ยงทางด้านความปลอดภัยทางไซเบอร์

- Cybersecurity Rating ทำหน้าที่ตรวจสอบและจัดการช่องโหว่ขององค์กรจากมุมมองการโจมตีไซเบอร์จากภายนอกองค์กร (Outside-in)
- ติดตามการปรับปรุงระบบอย่างต่อเนื่อง

เข้าใจถึงความเสี่ยงที่อาจเกิดขึ้นได้จากบุคคลภายนอกตลอด Supply chain

- Cybersecurity Rating ให้ข้อมูลเชิงลึก องค์กรนำข้อมูลที่ได้รับเพื่อใช้วางแผนและจัดสรรงบประมาณในการลงทุนด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์อย่างเหมาะสม
- ข้อมูลอย่างรอบด้านที่ได้รับจะช่วยให้องค์กรทราบถึงมูลค่าผลกระทบทางธุรกิจ หากเกิดเหตุโจมตีทางไซเบอร์และข้อมูลสำคัญขององค์กร

ลดค่าใช้จ่ายด้านทรัพยากรบุคคล/ประหยัดเวลา

- ลดต้นทุนการจ้างพนักงานที่ทำหน้าที่เฝ้าระวังและประเมินความเสี่ยงอย่างต่อเนื่องให้กับองค์กร

PACKAGE 1

เฝ้าระวังและออกรายงานผลอย่างต่อเนื่อง
(Continuous Risk Monitoring)

DELIVERABLE

รายงานระดับคะแนนความปลอดภัยทางไซเบอร์ขององค์กรภาพรวม (Cybersecurity Rating Report) รายเดือน ครอบคลุมความเสี่ยงหลัก 10 ด้าน อาทิ

- ความเสี่ยงจากการขึ้นบัญชีดำค่าไอพีสาธารณะขององค์กรที่ปรากฏภายนอก (IP Reputation)
- เว็บไซต์ และโดเมนขององค์กรที่ปรากฏภายนอกสาธารณะที่มีความเสี่ยง และมีผลกระทบต่อการถูกโจมตีทางไซเบอร์ (Website, Domain and Sub domain Assessment)
- ตรวจความปลอดภัยของ Endpoint Security ที่มองเห็นจากภายนอก เช่น อุปกรณ์ IoT, กล้องวงจรปิด และอุปกรณ์อื่นที่สามารถติดต่อจากภายนอกและทราบว่าเป็นขององค์กรของท่าน

SERVICE PRICE (ไม่รวมVat)

35,000 บาท/เดือน
ต่อเนื่องเป็นระยะเวลา 1 ปี
420,000 บาทต่อปี

DELIVERABLE

รายงานระดับคะแนนความปลอดภัยทางไซเบอร์ขององค์กรภาพรวม (Cybersecurity Rating Report) รายเดือน ครอบคลุมความเสี่ยงหลัก 10 ด้าน ** ประกอบด้วย

1. Application Security

การตรวจจับช่องโหว่ (Detecting common website application vulnerabilities)

2. Cubit Score

การตรวจสอบค่าความเสี่ยงจากฐานข้อมูลภัยคุกคามทางไซเบอร์ (Threat Intelligence)

3. DNS Health

การตรวจจับการกำหนดค่า DNS (Detecting DNS insecure configurations and vulnerabilities)

4. Endpoint Security

การวัดระดับความปลอดภัยพื้นที่ทำงานของพนักงาน (Measuring security level of employee workstations)

5. Hacker Chatter

การตรวจสอบฝั่งแฮกเกอร์ (Monitoring hacker sites for chatter about your company)

6. IP Reputation

การตรวจจับกิจกรรมที่น่าสงสัย (Detecting suspicious activity, such as malware or spam, within your company network)

7. Information Leak

ข้อมูลความลับรั่วไหลโดยไม่ตั้งใจ (Potentially confidential company information that may have been inadvertently leaked)

8. Network Security

การตรวจจับการตั้งค่าเครือข่ายที่ไม่ปลอดภัย (Detecting insecure network settings)

9. Patching Cadence

ทรัพย์สินล้าสมัยที่อาจมีช่องโหว่ (Out of date company assets which may contain vulnerabilities or risks)

10. Social Engineering

การวัดความตระหนักขององค์กรต่อภัยไซเบอร์ (Measuring company awareness to a social engineering or phishing attack)

Source: ** https://securityscorecard.com/blog/securityscorecard-10-risk-factors-explained

PACKAGE 1

Dashboard ตัวอย่างหน้าแสดงผล

ระดับคะแนนความปลอดภัยทางไซเบอร์ขององค์กร (Cybersecurity Rating Report) รายวันต่อเนื่อง

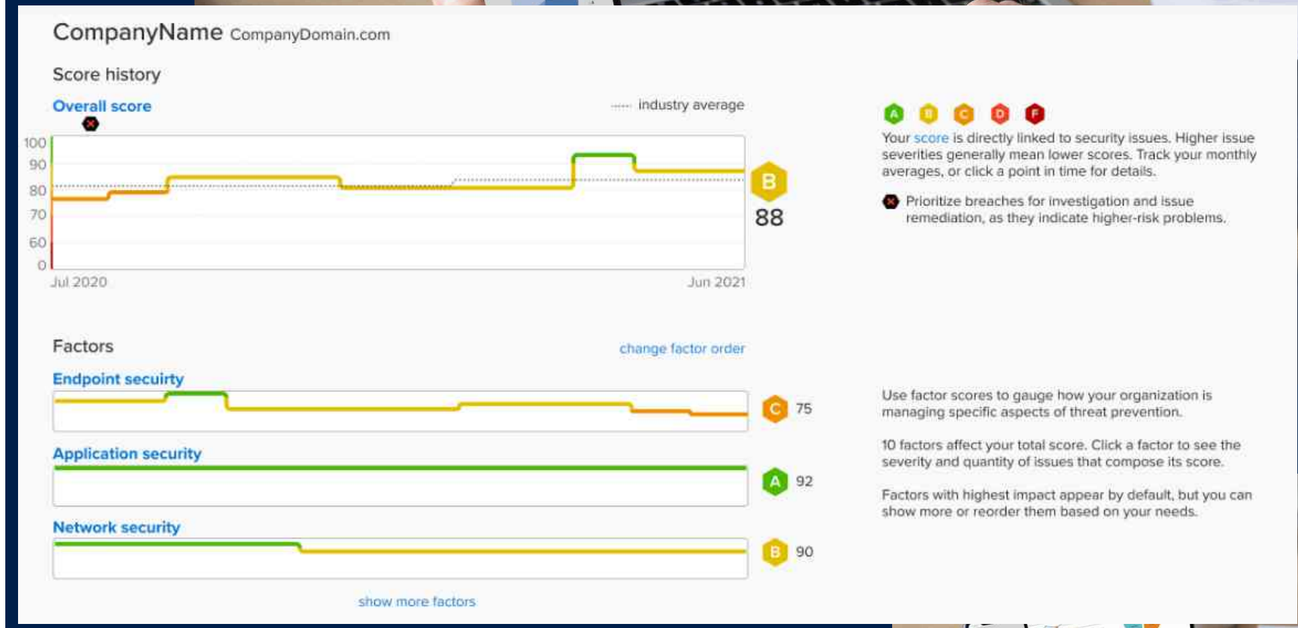
External Security Posture Report for Your Organization

Powered by SecurityScorecard | Updated daily

A 94

Your security posture is good for your industry. Your security posture score is based on your grades across ten major security categories.

B 84	Application Security Issues Found: 87	A 94	Cubit Score Issues Found: 50
A 96	Endpoint Security Issues Found: 15	B 84	DNS Health Issues Found: 87
B 84	Hacker Chatter Issues Found: 87	A 95	IP Reputation Issues Found: 87
A 95	Leaked Information Issues Found: 87	A 95	Network Security Issues Found: 87
A 95	Patching Cadence Issues Found: 10	A 95	Social Engineering Issues Found: 87



PACKAGE 1

เฝ้าระวังและออกรายงานผลอย่างต่อเนื่อง
(Continuous Risk Monitoring)

ขั้นตอนหลัก และกรอบระยะเวลา

หมายเหตุ: บริการอาจมีการปรับปรุงเปลี่ยนแปลงตามความเหมาะสม เพื่อให้เกิดประสิทธิภาพสูงสุดกับแต่ละองค์กร

Timeframe depend on:

- สำหรับขั้นตอนวางแผน เมื่อเปิดใบสั่งซื้อแล้ว จะสามารถใช้ระบบได้ ภายในระยะเวลา ไม่เกิน 7 วันทำการ

Key Informant:

- ผู้บริหารสายงานด้านเทคโนโลยีสารสนเทศและดิจิทัล
- ผู้รับผิดชอบด้านการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

PACKAGE 2

ติดตามและทบทวนความเสี่ยง แจ้งเตือน
เมื่อเกิดเหตุการณ์ที่สร้างผลกระทบต่อองค์กร
(Continuous High Risk Alert)

DELIVERABLE

รายงานการแจ้งเตือนผ่านอีเมล และแชทไลน์กลุ่ม

- แจ้งเตือนเมื่อพบโอกาสถูก Ransomware ซอฟต์แวร์เรียกค่าไถ่
- แจ้งเตือนเมื่อพบ CVE Score ระดับความเสี่ยงสูง เช่น พบ Log4j ที่อยู่ในระบบ
- แจ้งเตือนเมื่อพบว่าปรับปรุงระบบแล้ว แต่ไม่ครบถ้วนตามมาตรฐานสากล เช่น ISO27001, PCI/DSS และ GDPR/PDPA เป็นต้น

ขอบเขตของเหตุการณ์ที่แจ้งเดือน ประกอบด้วย
เว็บไซต์, อุปกรณ์ IoT, ไอพีแอดเดรส แอพลลิเคชั่น เครื่องแม่ข่าย
ขององค์กรที่ติดต่อในโลกอินเทอร์เน็ตและเข้าถึงได้ในสาธารณะ
และคู่ค้าที่ทำงานกับระบบซอฟต์แวร์ที่มีการเชื่อมกับองค์กรของท่าน

SERVICE PRICE (ไม่รวมVat)

120,000 บาท/เดือน
ต่อเนื่องเป็นระยะเวลา 1 ปี
1,440,000 บาทต่อปี (ไม่รวมVat)

PACKAGE 2

View each issue

ตัวอย่างหน้าแสดงผล

ตัวอย่างความเสี่ยงแต่ละด้าน ที่ควรได้รับการตั้งค่าแจ้งเตือนเพื่อป้องกันก่อนเกิดเหตุการณ์ที่สร้างผลกระทบต่อองค์กร

F
30
SECURITY SCORE

In 5 portfolios | 2 custom scorecards | Technology | 81 followers

Contact Company
Generate Report

Scorecard | History | Issues 53 | Compliance | Breaches & Incidents 5 | Digital Footprint → | Hierarchy (beta)

← VIEW ALL ISSUES

CUBIT SCORE

Ransomware-Susceptible Remote Access Services Exposed

INFORMATIONAL SIGNAL
Informational signals do not affect the company sc

DESCRIPTION

Services that allow remote access to a company's internal network, such as Remote Desktop Protocol (RDP), Samba (SMB), Virtual Network Computing (VNC), and X11 have long been hacker targets. Increasingly, these are the principal targets for ransomware groups and cybercrime affiliates. They enable access to an internal network through devices that often have unpatched vulnerabilities. Once an adversary achieves remote access to an internal network device, they may pivot from machine to machine, install malware and ransomware, and exfiltrate sensitive data. This is the case with most modern ransomware infections employing "double extortion" where the adversary encrypts devices on the network and exfiltrates sensitive data, threatening to release it if the ransom is not paid. Often, even when the ransom is paid, the data is sold on the Dark Web and is detected as another issue type, Domain Advertised as Ransomware Victim. Remote access devices should be placed behind a secure VPN service that is regularly patched, with firewalls on the border of the enterprise network or ISP. Use the principle of least privilege, where only certain users are given access and the passwords that have sufficient strength and randomness so that they cannot be guessed, brute-forced, or found in third-party credential leaks

RISK

We observed exposed RDP, VNC, and other remote access services, ransomware compromise.

RECOMMENDATION

Determine the business need of exposing these services to the publi them behind a secure, patched VPN service or firewall with appropria users. If they must be exposed, keep the services patched and updat under constant observation with logging and security monitoring.

IMPROVE YOUR SCORE

There is **1 finding** you can investigate right now. Resolving findings can affect your rating.

Resolve Findings Learn more

Need more context on this issue?

C
79
SECURITY SCORE

In 1 portfolio | Create Custom Scorecard + | Retail | 16 followers

Invite Company
Generate Report

Scorecard | History | Issues 14 | Compliance | Digital Footprint → | Hierarchy (beta) | Company Profile

← VIEW ALL ISSUES

HACKER CHATTER

Domain Advertised as Ransomware Victim

INFORMATIONAL SIGNAL
Informational signals do not affect the company score

DESCRIPTION

We observed your domain advertised as a breached victim on a ransomware group's Dark Web site, where victims and their data are disclosed. Ransomware attacks have become more complex. Attackers no longer rely on simply encrypting files and waiting for victims to pay for decryption keys. Now, to increase the likelihood of payment, attackers have begun to access multiple machines across the victim's network and systematically search for confidential files. The attackers load these files to a server they control prior to encrypting the victim-held data. If the victim does not pay the ransom, the attacker releases the stolen data to the public. These servers display public webpages to anyone who has access to the Dark Web through the Tor browser.

RISK

We observed this domain advertised on a ransomware site on the Dark Web, including the size of exfiltrated data and other information.

RECOMMENDATION

Perform a system audit to find how the attackers were able to gain entry. Then fix the issue. This may involve having to reset passwords or deploying other authentication methods. When you verify that no trace of the attacker remains, restore the data from most recent good backups if possible. Make sure to notify parties whose data may have been compromised.

IMPROVE YOUR SCORE

There is **1 finding** you can investigate right now. Resolving findings can affect your rating.

Resolve Findings Learn more

Need more context on this issue? Contact Company

COMPARISON TO SIMILAR COMPANIES

Score context analytics are not available for this issue type.

PACKAGE 2

ติดตามและทบทวนความเสี่ยง แจ้งเตือนเมื่อเกิดเหตุการณ์
ที่สร้างผลกระทบต่อองค์กร (Continuous High Risk Alert)*

ขั้นตอนหลัก และกรอบระยะเวลา

* ควรเริ่มต้นด้วยบริการ Package 1 ให้มีชุดข้อมูลด้านความเสี่ยงทั้งหมดก่อน

หมายเหตุ: บริการอาจมีการปรับปรุงเปลี่ยนแปลงตามความเหมาะสม เพื่อให้เกิดประสิทธิภาพสูงสุดกับแต่ละองค์กร

Timeframe depend on:

- สำหรับขั้นตอนวางแผน เมื่อเปิดใบสั่งซื้อแล้ว จะสามารถใช้ระบบได้ ภายในระยะเวลา ไม่เกิน 7 วันทำการ

Key Informant:

- ผู้บริหารสายงานด้านเทคโนโลยีสารสนเทศและดิจิทัล
- ผู้รับผิดชอบด้านการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

PACKAGE 2 Plus

บริการให้คำปรึกษาเพื่อปรับปรุงระดับคะแนนความปลอดภัยทางไซเบอร์ (Consulting Service for Improve Cybersecurity Rating)*

- ควรเริ่มต้นด้วยบริการ Package 1+2 ให้มีชุดข้อมูลด้านความเสี่ยงทั้งหมดตลอดนจนมีการติดตาม ทบทวนความเสี่ยง และแจ้งเตือน ก่อน

DELIVERABLE

รายงานสรุปแนวทางการปรับปรุงระดับคะแนนความปลอดภัยทางไซเบอร์ขององค์กร

- บริการให้คำปรึกษาโดยทำการปรับปรุงระดับคะแนน/เกรดที่ได้ให้ดีขึ้น
- อธิบายหลักเกณฑ์การพิจารณาระดับความซับซ้อน (ยาก-ง่าย) ของแต่ละประเด็นที่ได้จากการประเมินความเสี่ยงเพื่อเป็นแนวทางเสนอต่อองค์กรให้ดำเนินการปรับปรุง
- โดยระดับความเสี่ยงจะพิจารณาจากข้อมูลความเสี่ยงที่มีระดับความสำคัญ และผลกระทบต่อองค์กร รวมถึงจากแอพพลิเคชั่นของคู่ค้า หน่วยงานที่เกี่ยวข้องที่ต้องให้ความสำคัญเนื่องจากส่งผลต่อระดับคะแนนความปลอดภัยทางไซเบอร์ในองค์กร
- เสนอแผนกิจกรรมที่องค์กรต้องเร่งดำเนินการ

SERVICE PRICE (ไม่รวมVat)

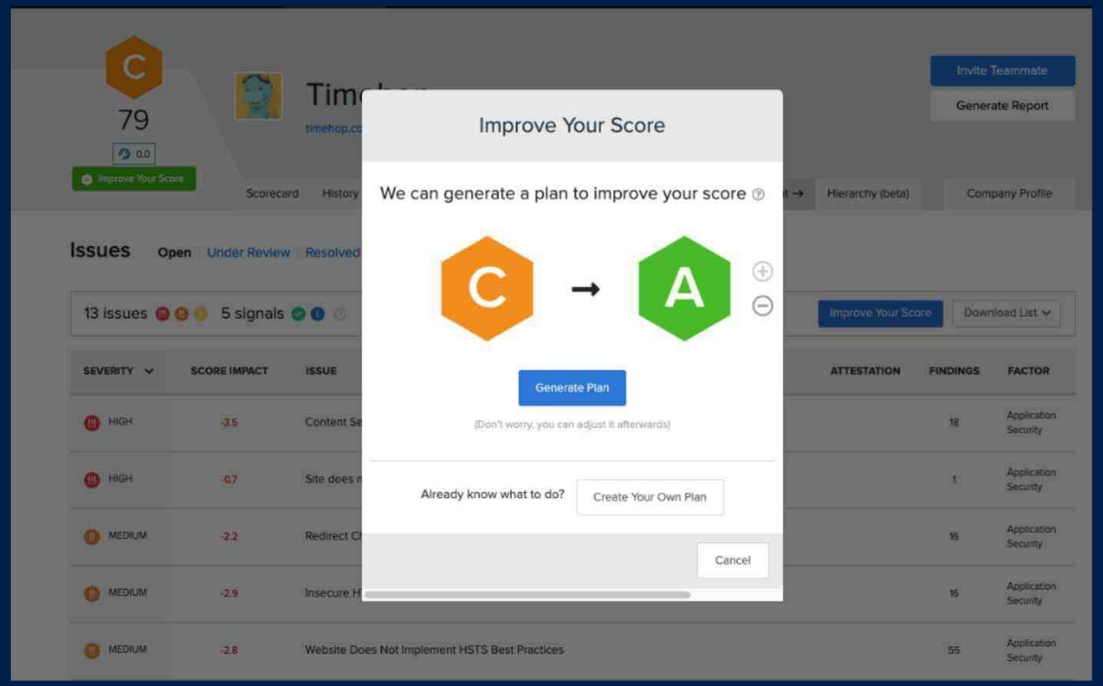
Package 2 Plus Consulting Service
120,000 บาท/เดือน
ต่อเนื่องเป็นระยะเวลา 1 ปี
1,440,000 ++ บาทต่อปี (ไม่รวมVat)

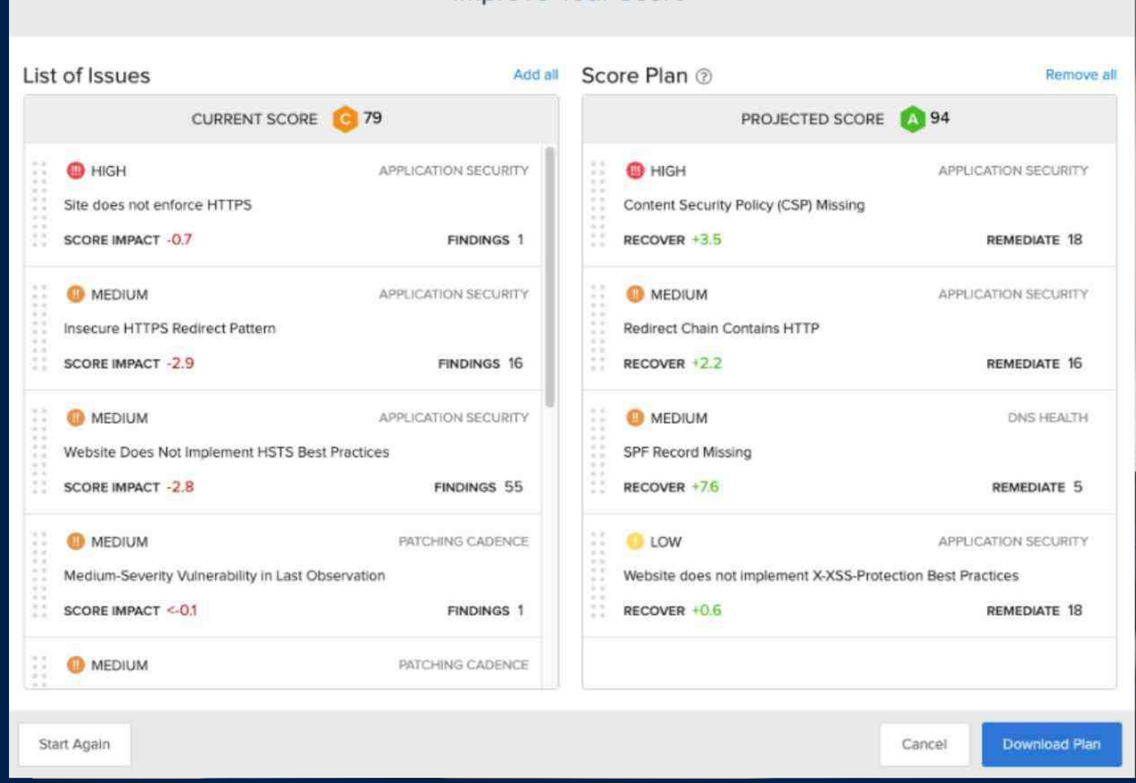
++การปรับปรุงระดับคะแนน/เกรด ขึ้นกับจำนวนและความซับซ้อนของ Issues ที่พบ ขั้นต่ำเริ่มต้นที่ 100,000 บาท

PACKAGE 2 Plus

บริการให้คำปรึกษาเพื่อปรับปรุงระดับคะแนนความปลอดภัยทางไซเบอร์ (Consulting Service for Improve Cybersecurity Rating)

ตัวอย่างหน้าแสดงผล





SERVICE PRICE (ไม่รวมVat)

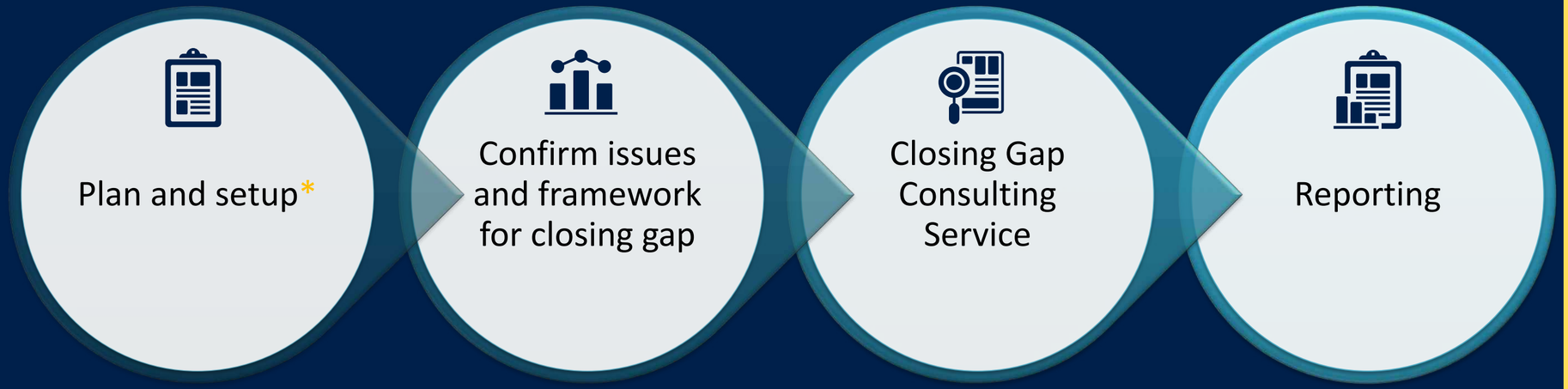
Package 2 Plus Consulting Service
120,000 บาท/เดือน
ต่อเนื่องเป็นระยะเวลา 1 ปี
1,440,000 ++ บาทต่อปี (ไม่รวมVat)

++การปรับปรุงระดับคะแนน/เกรด
ขึ้นกับจำนวนและความซับซ้อนของ Issues
ที่พบ ขั้นต่ำเริ่มต้นที่ 100,000 บาท

PACKAGE 2 Plus

บริการให้คำปรึกษาเพื่อปรับปรุงระดับคะแนนความปลอดภัยทางไซเบอร์
(Consulting Service for Improve Cybersecurity Rating)

ขั้นตอนหลัก และกรอบระยะเวลา



- ควรเริ่มต้นด้วยบริการ Package 1+2 ให้มีชุดข้อมูลด้านความเสี่ยงทั้งหมด ตลอดนจนมีการติดตาม ทบทวนความเสี่ยง และแจ้งเตือน ก่อน

หมายเหตุ: บริการอาจมีการปรับปรุงเปลี่ยนแปลงตามความเหมาะสม เพื่อให้เกิดประสิทธิภาพสูงสุดกับแต่ละองค์กร

Timeframe depend on:

- สำหรับขั้นตอนบริการให้คำปรึกษาเพื่อปรับปรุงระดับคะแนน/เกรด** ขึ้นอยู่กับจำนวน และความซับซ้อนของ Issues ที่พบ

Key Informant:

- ผู้บริหารสายงานด้านเทคโนโลยีสารสนเทศและดิจิทัล
- ผู้รับผิดชอบด้านการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

PACKAGE 3

การประเมินความเสี่ยงเพื่อหาช่องโหว่ภายในองค์กร (Vulnerability Assessment)

DELIVERABLE

รายงานตรวจสอบหาความผิดปกติการใช้งานระบบสารสนเทศภายในองค์กร

- จัดทำทรัพย์สินสารสนเทศ Inventory อุปกรณ์ Device ทั้งเครื่องคอมพิวเตอร์ เครื่องแม่ข่ายคอมพิวเตอร์ เครื่องปริ้นเอกสาร กล้องวงจรปิด อุปกรณ์ IoT ที่มีค่าไอพีแอดเดรสเป็นภายในองค์กร เพื่อตรวจสอบความผิดปกติและมีช่องโหว่ และยังไม่อัพเดทซอฟต์แวร์อันก่อให้เกิดภัยคุกคามทางไซเบอร์ได้
- ประเมินความเสี่ยงเพื่อหาช่องโหว่จากเครื่องแม่ข่ายที่สำคัญในองค์กรและออกรายงานผลตาม OWASP TOP 10
- ตรวจสอบการเข้าถึงระบบโดยมิชอบ Midnight login
- ตรวจสอบความเสี่ยงที่พบโอกาสการแพร่กระจายไวรัส Ransomware
- ตรวจสอบความเสี่ยงที่พบโอกาส Internal Hacking การโจรกรรมข้อมูลจากคนในองค์กร เช่น การเชื่อมต่อข้อมูลที่ไม่มีการเข้ารหัสไปยัง Server, ข้อมูลส่วนบุคคล PDPA และข้อมูลสำคัญมีโอกาสถูกละเมิด

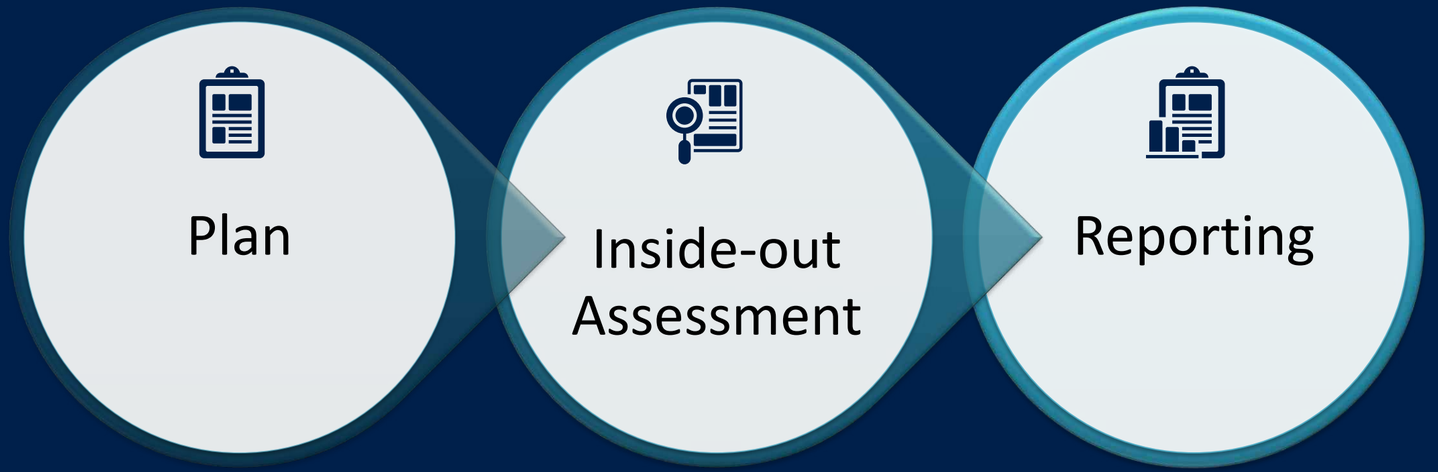
SERVICE PRICE (ไม่รวมVat)

450,000 บาท/ครั้ง

PACKAGE 3

การประเมินความเสี่ยงเพื่อหาช่องโหว่ภายในองค์กร
(Vulnerability Assessment: VA)

ขั้นตอนหลัก และกรอบระยะเวลา



45 วัน

หมายเหตุ: บริการอาจมีการปรับปรุงเปลี่ยนแปลงตามความเหมาะสม เพื่อให้เกิดประสิทธิภาพสูงสุดกับแต่ละองค์กร

Key Informant:

- ผู้บริหารสายงานด้านเทคโนโลยีสารสนเทศและดิจิทัล
- ผู้รับผิดชอบด้านการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

TRIS x TUNABLE PROJECT

THANK YOU

IN THE FUTURE TECHNOLOGY IS DEVELOPING VERY FAST

CONTACT CORPORATE

ติดต่อสอบถาม หรือปรึกษาเกี่ยวกับบริการของทริส

EMAIL ADDRESS
Tris@tris.co.th
Amornphan@tris.co.th

PHONE NUMBER
08-4648-5959

WEBSITE
www.tris.co.th