รายงานฉบับสมบูรณ์

โครงการขอรับการส่งเสริมและสนับสนุนจากเงินกองทุนวิจัยและพัฒนากิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม เพื่อประโยชน์สาธารณะ

โครงการระบบออนไลน์เพื่อพัฒนาผู้เชี่ยวชาญด้านความปลอดภัยไซเบอร์
(Cybersecurity Learning Platform)

บริษัท เทิร์นคีย์ คอมมูนิเคชั่น เซอร์วิส จำกัด (มหาชน)
กรกฎาคม ๒๕๖๕

ได้รับทุนอุดหนุนจาก
กองทุนวิจัยและพัฒนากิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม เพื่อประโยชน์สาธารณะ
(สำนักงาน กสทช.)

รายงานฉบับสมบูรณ์

ทุนส่งเสริมและสนับสนุนการวิจัยและพัฒนา
สัญญารับทุนเลขที่ A๖๒-๑-(๒)-๐๐๔

โครงการระบบออนไลน์เพื่อพัฒนาผู้เชี่ยวชาญด้านความปลอดภัยไซเบอร์ (Cybersecurity Learning Platform)

คณะผู้จัดทำ

๑.	ดร.ภาณุภัทร์ ภู่เจริญ	หัวหน้าโครงการ
๒.	พลโท ดร. ปรัชญา เฉลิมวัฒน์	ที่ปรึกษาโครงการ
๓.	นายมนตรี สายดาราสมุทร	ผู้จัดการโครงการ

ได้รับทุนอุดหนุนจาก
กองทุนวิจัยและพัฒนากิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม เพื่อประโยชน์สาธารณะ
(สำนักงาน กสทช.)

กรกฎาคม ๒๕๖๕

สารบัญ

บทที่ **หน้าที่**

บทที่ ๑ บทนำ

๑.๑ หลักการและเหตุผล

ปัจจุบันภัยคุกคามทางไซเบอร์มีจำนวนที่เพิ่มสูงขึ้น และทวีความรุนแรงขึ้นตามลำดับ ส่งผลกระทบ และสร้างความเสียหายทั้งต่อระดับปัจเจกชน และระดับประเทศ ในปี พ.ศ. ๒๕๖๔ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (Thailand Computer Emergency Response Team) ได้สรุปสถิติภัยคุกคามทางไซเบอร์ ดังตารางที่ ๑

ประเภทภัยคุกคาม ปี ๒๕๖๔	จำนวนครั้งการเกิด	สัดส่วน
Abusive content	๑๔	๐.๖๘%
Availability	๕	๐.๒๔%
Fraud	๒๑๒	๑๐.๒๕%
Information gathering	๒๔๘	๑๑.๙๙%
Information security	๓๐	๑.๔๕%
Intrusion Attempts	๒๒๔	๑๐.๘๓%
Intrusions	๑๘๓	๘.๘๔%
Malicious code	๔๗๙	๒๓.๑๕%
Vulnerability	๖๗๔	๓๒.๕๘%
Other	๐	๐%
รวม	๒๐๖๙	๑๐๐.๐๐%

ตารางที่ ๑ สถิติภัยคุกคามทางไซเบอร์ในปี พ.ศ. ๒๕๖๔ โดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย

ซึ่งนานาประเทศต่างให้ความสำคัญในการดำเนินงานเพื่อรับมือกับปัญหาภัยคุกคามดังกล่าวอย่างมาก ดังนั้นการตระหนักถึงความปลอดภัยของระบบไซเบอร์นั้นจะช่วยสร้างความเข้าใจพื้นฐานเกี่ยวกับภัยคุกคามและความเสี่ยงในโลกไซเบอร์ การทำกิจกรรมต่าง ๆ ในโลกไซเบอร์และการเผชิญกับความเสี่ยงต่าง ๆ ซึ่งประเทศไทยควรที่จะส่งเสริมการเรียนรู้ เพื่อเพิ่มความตระหนักถึงภัยในโลกไซเบอร์ อาทิ นักเรียน นักศึกษา หรือ ผู้สนใจในเรื่องการรักษาความปลอดภัยใน โลกไซเบอร์ ควรได้รับการพัฒนา ความรู้ ความเข้าใจ เกี่ยวกับเรื่องดังกล่าวอย่างต่อเนื่อง เพื่อที่จะสามารถรับมือกับภัยคุกคามที่เกี่ยวข้องกับไซเบอร์ที่มีพัฒนาการทางเทคโนโลยีและข้อมูลอยู่ตลอดเวลา

๑.๒ ความเชื่อมโยงและสอดคล้องกับแผนแม่บทและแผนยุทธศาสตร์ชาติ

จากการที่สำนักงาน กสทช. ได้มีการส่งเสริมและสนับสนุนการพัฒนาทรัพยากรสื่อสาร การวิจัย และพัฒนาด้าน กิจการกระจายเสียง กิจการโทรทัศน์ กิจการโทรคมนาคมและเทคโนโลยี สารสนเทศกรอบทิศทางในการวิจัยและพัฒนาเชิงนวัตกรรมเทคโนโลยีสารสนเทศและโทรคมนาคมด้านอุตสาหกรรม ๔.๐ (Industry ๔.๐) เพื่อรองรับกับสภาพแวดล้อมระบบนิเวศดิจิทัลที่เปลี่ยนแปลงอย่างรวดเร็วและเชื่อมโยงกันในทุกๆ ด้าน โดยมีเป้าหมายตามแผนแม่บทกิจการโทรคมนาคมกับการพัฒนาที่เชื่อมโยงกับยุทธศาสตร์ชาติ ๒๐ ปีตลอดจนนโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมทำให้มีความเชื่อมโยงที่เกี่ยวข้องกับกระทรวงและหน่วยงานต่างๆซึ่งมีแผนงานและนโยบายในเรื่องของความต้องการในการที่จะพัฒนาเพิ่มพูนทักษะของบุคคลากรในด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศให้มีเพิ่มมากยิ่งขึ้นไป

๑.๒.๑ สำนักงานสภาความมั่นคงแห่งชาติ สำนักนายกรัฐมนตรี

ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. ๒๕๖๐ – ๒๕๖๔

“๒.๑.๓ ความพร้อมทางด้านบุคลากร ความพร้อมทางด้านบุคลากรถือเป็นสิ่งที่สำคัญอย่างยิ่งทั้งในด้านความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ทั้งระดับนโยบายและปฏิบัติ และด้านความรู้ความเชี่ยวชาญเฉพาะทางซึ่งจากการสำรวจ พบว่ากว่าร้อยละ ๕๐ หน่วยงานรัฐและเอกชนยังไม่ได้ให้ความสำคัญกับการจัดทำแผนพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ และ ร้อยละ ๗๙ ของหน่วยงานจะมีข้อจำกัดในการสร้างแรงจูงใจให้บุคลากรเสริมศักยภาพให้กับตนเอง เช่น การสอบใบประกาศนียบัตรการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยเฉพาะใบประกาศนียบัตรที่ได้รับการยอมรับในระดับสากล ซึ่งประเทศไทยควรกำหนดทิศทางและให้ความสำคัญกับการส่งเสริมและสนับสนุนการพัฒนาบุคลากรที่มีความรู้ความเชี่ยวชาญในด้านความมั่นคงปลอดภัยไซเบอร์เพิ่มขึ้น เพื่อเตรียมการรับมือกับภัยคุกคาม ที่อาจเกิดขึ้นในรูปแบบต่าง ๆ ได้อย่างครอบคลุมและมีประสิทธิภาพยิ่งขึ้น”

“ประเด็นยุทธศาสตร์ที่ ๕ สร้างความตระหนักและส่งเสริมความร่วมมือภายในประเทศด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

เป้าหมาย

๑. ประชาชนทั่วไปทุกระดับทุกเพศและวัยที่เป็นผู้ใช้อินเทอร์เน็ต มีความตระหนักถึงภัยคุกคามทางไซเบอร์ และมีความรู้เรื่องการรักษาความปลอดภัยทางไซเบอร์

๒. รัฐ ภาคเอกชน และประชาสังคมร่วมมือกันในการรักษาความมั่นคงปลอดภัยไซเบอร์

๓. ช่องทาง/กลไกการสื่อสารแนวนโยบายสู่การปฏิบัติในภาคเอกชนและภาคประชาสังคม

ตัวชี้วัด

๑. การจัดทำคู่มือเผยแพร่ความรู้เกี่ยวกับด้านไซเบอร์และการประเมินผล

๒. จำนวนครั้งการประชาสัมพันธ์ผ่านสื่อประเภทต่าง ๆ /กลไกต่าง ๆ

๓. การจัดฝึกอบรมให้ความรู้แก่ประชาชนผู้ใช้อินเทอร์เน็ตและการประเมินผล”

“แนวทางการดำเนินการ

๕.๑ ส่งเสริมการเผยแพร่ข้อมูลข่าวสารแก่ทุกภาคส่วน โดยทั่วถึงกับผ่านสื่อและกลไกต่าง ๆ ของภาครัฐ ภาคเอกชน และภาควิชาการ เพื่อสร้างความตระหนักถึงภัยคุกคามทางไซเบอร์และความสำคัญของการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อการใช้เทคโนโลยีดิจิทัล และการดำเนินกิจกรรมทางไซเบอร์อย่างปลอดภัยและเกิดประโยชน์ และส่งเสริมความร่วมมือด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในรูปแบบการรวมกลุ่มทั้งในระดับบุคคลและองค์กร

๕.๒ ส่งเสริมความร่วมมือกับสถาบันวิจัยและสถานศึกษา เช่น มหาวิทยาลัยและสถาบันคลังสมองในด้านการแลกเปลี่ยนความรู้ การวิจัยร่วมกันและ/หรือการนำเสนองานวิจัยตลอดจบการจัดทำคู่มือเผยแพร่ความรู้เกี่ยวข้องกับด้านไซเบอร์

๕.๓ ส่งเสริมและพัฒนาหลักสูตรด้านการรักษาความมั่นคง ปลอดภัยไซเบอร์ในการศึกษาตามระบบตั้งแต่ขั้นพื้นฐานทั้งสายสามัญและอาชีวะโดยให้เนื้อหาของหลักสูตรมีความแตกต่างกับไปในแต่ละระดับการศึกษา

๕.๔ ส่งเสริมการให้ความรู้ด้านการรักษาความมั่นคงปลอดภัย ทางไซเบอร์แก่ประชาชนผู้ใช้อินเทอร์เน็ตทั่วไป ผู้สูงอายุ เด็ก สตรีและ เยาวชน ชุมชน ท้องถิ่น โดยร่วมมือกับสถานศึกษาองค์การบริหารส่วน ท้องถิ่นและหน่วยงานที่เกี่ยวข้องเพื่อเผยแพร่ความรู้และสร้างความตระหนักอย่างเป็นระบบและต่อเนื่อง

๕.๕ ส่งเสริมและประสานความร่วมมือระหว่างรัฐกับเอกชน และภาคประชาสังคมเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ในลักษณะองค์รวมที่มีความเข้มแข็งโดยจัดให้มีกลไกและช่องทางการสื่อสารระหว่างกันเพื่อประโยชน์ในการทำความเข้าใจในแนวนโยบายจากรัฐสู่เอกชนและภาคประชาสังคมสู่การปฏิบัติการมีส่วนร่วมของภาคเอกชนและภาคประชาสังคมในการสะท้อนปัญหาประเมินผลการดำเนิน นโยบายและการเสนอแนะนโยบาย ตลอดจนการสนับสนุนและการเป็นผู้ร่วมรักษาความมั่นคงปลอดภัยไซเบอร์”

๑.๒.๒ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

นโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม (พ.ศ. ๒๕๖๑ – ๒๕๘๐)

“๘) ภัยคุกคาม, ไซเบอร์

การจัดการกับภัยในรูปแบบใหม่ๆ รวมถึงภัยคุกคามจากสารสนเทศรูปแบบต่างๆ มีการพัฒนาและเปลี่ยนแปลงรูปแบบอย่างต่อเนื่องจึงต้องเตรียมความพร้อมเพื่อรับมือเพิ่มขีดความสามารถของบุคลากรในการรักษาความมั่นคงปลอดภัยและการพัฒนาทักษะความรู้เพื่อป้องกันตนเองและหน่วยงานลดความเสี่ยงจากการถูกโจมตีหรือภัยคุกคามและลดความท้าทายจากผลกระทบที่อาจเกิดขึ้น”

“๓.๓ การกำหนดมาตรการการเฝ้าระวังและรับมือภัยคุกคามไซเบอร์เหมาะสมและสอดคล้องตามมาตรฐานสากลโดยเฉพาะการปกป้องโครงสร้างพื้นฐานที่มีความจำเป็นอย่างยิ่งยวด (Critical Infrastructure) เช่น โครงสร้างพื้นฐานทางไฟฟ้า โครงสร้างพื้นฐานทางการเงิน เพื่อให้มีความมั่นคงปลอดภัยเพียงพอ ต่อการค้าและการลงทุน การสร้างเครือข่ายแลกเปลี่ยนข้อมูลภัยคุกคามไซเบอร์ พร้อมกำหนดหน่วยงาน รับแจ้งเหตุ และสร้างกลไกการบังคับใช้กฎหมายที่มีประสิทธิภาพในการป้องกันปราบปรามการกระทำความผิด ไม่ให้มีผลต่อระบบความมั่นคงปลอดภัยดิจิทัล ทั้งนี้การส่งเสริมให้เกิดความตระหนักและเท่าทันภัยคุกคามทางไซเบอร์เป็นสิ่งสำคัญที่ต้องดำเนินการอย่างต่อเนื่อง”

๑.๒.๓ กระทรวงกลาโหม

นโยบายเร่งด่วนของรัฐมนตรีว่าการกระทรวงกลาโหม ประจำปีงบประมาณ พ.ศ. ๒๕๖๒ (๑ ต.ค. ๖๑ - ๓๐ ก.ย. ๖๒)

“๒.๓ เสริมสร้างขีดความสามารถในการปฏิบัติการด้านไซเบอร์ทั้งเชิงรุกและเชิงรับอย่างต่อเนื่อง เพื่อรองรับภัยคุกคามด้านไซเบอร์ที่มีผลกระทบต่อความมั่นคงของชาติตลอดจนให้การสนับสนุนการดำเนินการด้านไซเบอร์ระดับประเทศ รวมทั้งบูรณาการความร่วมมือกับทุกภาคส่วนทั้งภายในและต่างประเทศที่เกี่ยวข้องในการพัฒนาขีดความสามารถด้านกิจการอวกาศของกระทรวงกลาโหม เพื่อรองรับภัยคุกคามด้านอวกาศที่มีผลกระทบต่อความมั่นคงของชาติโดยเฉพาะการพัฒนา ด้านองค์ความรู้ และขีดความสามารถของกำลังพลจากระดับผู้ใช้งาน (User) สู่การเป็นผู้ควบคุมและบริหารสถานีดาวเทียม (Operator) ซึ่งจะนำไปสู่การพึ่งพาตนเองได้ในอนาคต”

ด้วยเหตุนี้จึงเล็งเห็นความสำคัญในเรื่องภัยคุกคามทางไซเบอร์การเข้าถึงเรื่องของความปลอดภัยของระบบไซเบอร์ความรู้ความเข้าใจในเรื่องดังกล่าวยังมีอยู่น้อยจึงมีแนวคิดที่จะจัดทำโครงการ Cyber Security Learning Platform เพื่อเป็นสื่อกลางในการศึกษารูปแบบการโจมตีทางไซเบอร์ (Cyber attack) กับการป้องกันอันตรายและการสร้างความปลอดภัยทางไซเบอร์ (Cyber Security) และการป้องกันภัยคุกคามจากการใช้เทคโนโลยีสารสนเทศและการสื่อสารขึ้นเพื่อให้กับเยาวชนและนักศึกษาเกิดการเรียนรู้เข้าใจและสามารถนำความรู้เกี่ยวกับความปลอดภัยทางไซเบอร์ไปพัฒนาในด้านต่างๆ ได้ทันกับเทคโนโลยีสารสนเทศและการสื่อสารที่เปลี่ยนแปลงอย่างรวดเร็ว

อย่างไรก็ตามในการพัฒนาบุคลากรด้านไซเบอร์มักประสบปัญหาด้านงบประมาณที่ใช้ในการอบรมการผ่านการสอบประกาศนียบัตรที่รับรองมาตรฐานซึ่งต้องใช้ทั้งงบประมาณที่สูง บุคลากรที่มีศักยภาพสูง อีกทั้งต้องใช้เงินลงทุนในเครื่องมือที่ราคาแพงและต้องใช้ระยะเวลาที่ยาวนานในการฝึกฝนกว่าที่จะสามารถพัฒนาบุคลากรไซเบอร์ให้สามารถปฏิบัติการได้อย่างมีประสิทธิภาพ

๑.๓ วัตถุประสงค์

๑.๓.๑ เพื่อลดเวลาในการเรียนรู้และลดเวลาในกระบวนการพัฒนาบุคลากรด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยเปิดโอกาสให้เยาวชน นักเรียน นักศึกษา สามารถเข้าถึง สามารถเรียนรู้เรื่องภัยคุกคามทางไซเบอร์การโจมตีทางไซเบอร์และวิธีป้องกันด้วยระบบที่สร้างขึ้นผ่านช่องทาง Internet Web based ซึ่งสามารถเข้าถึงได้ตลอดเวลาและไม่มีค่าใช้จ่ายในการใช้งานสำหรับบทเรียนพื้นฐาน

๑.๓.๒ เพื่อออกแบบและพัฒนาระบบ Online Game-Based Cybersecurity Learning Platform สำหรับการพัฒนาบุคคลากรด้านไซเบอร์ให้สามารถสร้างผู้เชี่ยวชาญให้มีทักษะความสามารถทางด้านความปลอดภัยทางไซเบอร์เพิ่มขึ้นจนสามารถพัฒนาต่อยอด สู่ความเป็นเลิศ ทำให้ประเทศไทยมีจำนวนผู้เชี่ยวชาญเพิ่มมากขึ้น

๑.๓.๓ ส่งเสริมและเร่งรัดการพัฒนาบุคลากรทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งด้านปริมาณ และคุณภาพเพื่อสร้างรากฐานการประกอบวิชาชีพด้านความมั่นคงปลอดภัยไซเบอร์ให้มีคุณภาพทัดเทียมมาตรฐานสากลและเป็นคลังสมองที่สำคัญของประเทศ

๑.๓.๔ พัฒนากลไกในการสื่อสารเพื่อเป็นศูนย์รวมและเป็นสื่อกลางในการแลกเปลี่ยนความรู้ เทคนิค เครื่องมือกระบวนการของเทคโนโลยีด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระหว่างผู้ที่มีความสนใจร่วมกันจากหน่วยงานต่างๆ ทั้งภาคประชาชน ภาครัฐและเอกชน

๑.๔ ผลที่คาดว่าจะได้รับ

๑.๔.๑ สามารถลดเวลาในการเรียนรู้และลดเวลาในกระบวนการพัฒนาบุคลากรด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ผ่านช่องทางระบบที่สร้างขึ้น

๑.๔.๒ สามารถใช้ระบบ Online Game-Based Cybersecurity Learning Platform เพื่อพัฒนาบุคคลากรด้านไซเบอร์ให้มีทักษะความสามารถทางด้านความปลอดภัยทางไซเบอร์เพิ่มขึ้น

๑.๔.๓ มีระบบต้นแบบ Online Game-Based Cybersecurity Learning Platform เพื่อพัฒนาต่อยอดไปสู่ระดับIntermediate และ Advance

๑.๔.๔ สามารถส่งเสริมและเร่งรัดการพัฒนาบุคลากรทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งด้านปริมาณและ คุณภาพทัดเทียมมาตรฐานสากล

๑.๔.๕ เป็นศูนย์กลางที่เป็นกลไกในการสื่อสาร รวมความรู้ กรณีศึกษาและโมดูลทดสอบด้านความปลอดภัยทางไซเบอร์จากผู้เชี่ยวชาญทั้งจากภาคการศึกษามหาวิทยาลัหน่วยงานภาครัฐและธุรกิจเอกชนที่มีส่วนเกี่ยวข้อง

๑.๔.๖ เป็นช่องทางเรียนรู้แบบ online Self Training พร้อมให้ Virtual certification ทางด้านความปลอดภัยทางไซเบอร์

๑.๕ ตัวชี้วัดความสำเร็จ

๑.๕.๑ มีการจัดสร้างระบบต้นแบบ Online Game-Based Cybersecurity Learning Platform จนสำเร็จ

๑.๕.๒ มีการจัดทำ MOU และเกิดการร่วมงานระหว่างหน่วยงานที่ได้ประสานไว้คือ หน่วยงานการศึกษาระดับมัธยมศึกษา, ระดับอุดมศึกษา และกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

๑.๕.๓ บุคลากรที่เข้าใช้ระบบ เกิดการฝึกฝน เกิดความเข้าใจ มีความรู้ทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพิ่มขึ้น และมีความพึงพอใจในการใช้งานระบบ

๑.๕.๔ มีการจัดการสัมนาเชิงวิชาการเพื่อนำเสนอระบบ

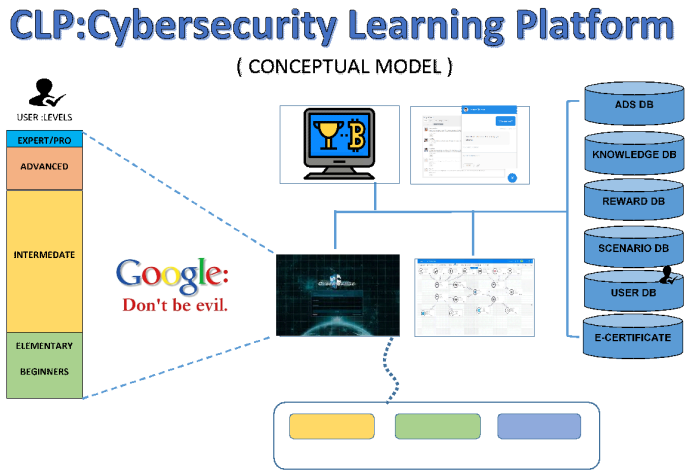
๑.๕.๕ เป็นแนวทางที่ชัดเจนเพื่อให้เยาวชนบุคคลที่มีความสนใจมีความตระหนักรู้ถึงภัยคุกคามและอาชญากรรมไซเบอร์และการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยที่เป็นรูปธรรม

บทที่ ๒. แผนการดำเนินงาน

๒.๑ รูปแบบลักษณะของโครงการ

โครงการนี้เป็นการจัดทำระบบ Cyber Security Learning Platform ระบบนี้ออกแบบมาเพื่อพัฒนาบุคลากรทางด้านไซเบอร์ ผ่านช่องทางอินเตอร์เน็ต (Internet Web based) ทั้งนี้ผู้ใช้สามารถเข้าถึงระบบการเรียนรู้นี้โดยไม่จำกัดสถานที่และเวลา ผู้เข้าใช้งานสามารถแยกประเภทได้เป็นหลายระดับในการเข้าใช้งานตามระดับความรู้ เช่น ระดับเริ่มต้น (Beginner) ระดับกลาง (Intermediate) และระดับสูง (Advance) หรือผู้เชี่ยวชาญ (expert) เป็นต้น เพื่อให้รูปแบบของระบบนี้ สามารถรองรับผู้ใช้งานได้หลายกลุ่มและอายุที่แตกต่างกัน โดยมีการออกแบบระบบเป็นลักษณะ Online Game-Based Cybersecurity Learning Platform ที่มีการแข่งขันระหว่างผู้ใช้อื่นๆ และมีระบบการให้คะแนน ทำให้ผู้ใช้งานได้รับความสนุกสนาน และดึงดูดความสนใจ และทำให้เกิด Self simulate competition

เนื้อหาที่นำมาใช้นั้นจะมีการนำเสนอเนื้อหาด้าน Cyber Security ตามความยากง่ายในรูปแบบของทั้งการให้ข้อมูล คำถาม ปัญหาเพื่อวิเคราะห์ และ แบบจำลอง (Scenario) เพื่อแก้ไขทั้งนี้ระบบได้นำเอาหลักการ พัฒนาเช่นเดียวกับ Cyber Range มาใช้ ทั้งนี้เนื้อหาที่นำมาใช้นั้นจะมีการทำ peer review หรือตรวจสอบกับหน่วยงานหรือสถาบันการศึกษาที่เป็นที่ยอมรับและเชื่อถือ โครงการนี้มีลักษณะรูปแบบโครงสร้าง (Conceptual Model) ดังแสดงในภาพที่ ๑



ภาพที่ ๑ โครงสร้างระบบ Cyber Security Learning Platform

จากรูปข้างต้น ระบบ Cyber Security Learning Platform ที่สร้างจะประกอบด้วยส่วนที่เป็นทั้งฮาร์ดแวร์และซอฟท์แวร์ ระบบฮาร์ดแวร์จะเป็นการนำเทคโนโลยี virtualization เข้ามาใช้กับระบบเซิร์ฟเวอร์เพื่อทำการสร้าง virtual machine สำหรับรันระบบปฏิบัติการและ แอปพลิเคชัน ตามรูปแบบการฝึกการเรียนรู้ที่กำหนดไว้ในฐานข้อมูล Scenario Database สำหรับระบบซอฟท์แวร์นั้น มีการออกแบบและพัฒนาให้เป็น Online Game-Based โดยมีจัดให้มีผู้ควบคุมระบบเพื่อทำหน้าที่บริหารจัดการการใช้งานต่าง ๆ เช่น มีการบันทึก

ประวัติการใช้งาน, มี Chat board, ระบบการ Reward เป็นต้น นอกจากนี้ ระบบ ซอฟท์แวร์จะประกอบด้วย ฐานข้อมูลของประวัติผู้เข้าใช้ (User Database) เพื่อติดตาม ความสัมฤทธิ์ผล, ฐานข้อมูลบทเรียน (Knowledge Database), สถานการณ์จำลอง (Scenario Database), ฐานข้อมูลอันดับผู้ชนะรางวัล (Reward Database) ทั้งนี้ในอนาคตยังสามารถจัดทำ e-certificate รับรองให้แก่ผู้เรียนที่สำเร็จได้อีกเช่นกัน

๒.๑.๑ มาตรฐานที่เกี่ยวข้องเพื่อใช้ในโครงการ

ในการจัดทำข้อมูลเนื้อหาเพื่อใช้ในระบบ Cyber Security Learning Platform นั้นจะมีการรวบรวมข้อมูลจากสถานบันการศึกษาที่ได้รับการรับรอง พร้อมทั้งจะมีการทบทวน (Peer review) ว่ามีความสอดคล้องกับมาตรฐานที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ อาทิ เช่น

๑. ISO/IEC JTC ๑/SC ๒๗ – IT Security Techniques
๒. ISO/IEC ๑๕๔๐๘ - Common Criteria
๓. ISO/IEC ๒๗๐๐๐ Series - ISMS Family of Standards
๔. ISO/IEC ๒๙๑๐๐:๒๐๑๑ Privacy Framework
๕. SAE J๓๐๖๑ Cybersecurity Guidebook for Cyber-Physical Vehicle Systems

๒.๒ ขอบเขตของงานโครงการ

ระบบ Cyber Security Learning Platform ที่นำเสนอกับกองทุนเพื่อทำวิจัยนั้นเป็นระยะเริ่มต้นของโครงการ โดยทำการพัฒนา Prototype และ โครงสร้างโดยรวมซึ่งมีขอบเขตดังนี้

๒.๒.๑ จัดทำต้นแบบระบบ Online Game-Based Cybersecurity Learning Platform ในส่วน Elementary and Basic Level

๒.๒.๒ จัดทำ Community chat room เพื่อให้ผู้ใช้งานสามารถสื่อสารใน Platform ที่สร้างขึ้น

๒.๒.๓ ออกแบบ และจัดทำเนื้อหา โจทย์ปัญหา และ scenarios สำหรับทดลองปฏิบัติ

๒.๒.๔ จัดประชุมหรือสัมนาร่วมกับสถาบันการศึกษา หรือองค์กรภาครัฐ/เอกชน รวมถึงบุคคลที่มีความสนใจเพื่อรับฟังข้อคิดเห็นหรือสร้างความร่วมมือและประชาสัมพันธ์การใช้งานระบบที่สร้างขึ้น

๒.๒.๕ ดำเนินการเก็บข้อมูลและรายงานสรุปผลการดำเนินงาน

๒.๓ แผนการดำเนินงานโครงการ

ระยะเวลาดำเนินการโครงการ ๑๘ เดือน โดยแบ่งเป็น

การศึกษาวิเคราะห์และออกแบบระบบ จัดซื้อและติดตั้งระบบ, จัดทำระบบ Front End, ระบบ Backend Elementary and Basic, ทดสอบระบบ, เริ่มใช้งานจริง, อบรม สัมนาเชิงปฏิบัติการร่วมกับสถาบันการศึกษาและองค์กร ภาครัฐ, ทำการรายงานผลการดำเนินการ

ตารางที่ ๒ แผนการดำเนินงานโครงการ

โครงการระบบออนไลน์เพื่อพัฒนาผู้เชี่ยวชาญด้านความปลอดภัยไซเบอร์

เริ่มสัปดาห์	Mar 25, 2019

สัปดาห์	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41
รายละเอียดการดำเนินงาน	Mar 25	Apr 1	Apr 8	Apr 15	Apr 22	Apr 29	May 6	May 13	May 20	May 27	Jun 3	Jun 10	Jun 17	Jun 24	Jul 1	Jul 8	Jul 15	Jul 22	Jul 29	Aug 5	Aug 12	Aug 19	Aug 26	Sep 2	Sep 9	Sep 16	Sep 23	Sep 30	Oct 7	Oct 14	Oct 21	Oct 28	Nov 4	Nov 11	Nov 18	Nov 25	Dec 2	Dec 9	Dec 16	Dec 23	Dec 30
เซ็นสัญญาโครงการ																																									
ทำการศึกษาวิเคราะห์ออกแบบระบบ																																									
จัดทำสรุปแผนการดำเนินงานโครงการ การวิเคราะห์ และออกแบบระบบ																																									
จัดหาระบบ Cloud Server และ software ที่เกี่ยวข้องในการทำงาน																																									
ออกแบบระบบหน้าบ้าน (Front-end)																																									
ออกแบบระบบหลังบ้าน (Back-end)																																									
พัฒนาระบบหน้าบ้าน (Front-end)																																									
พัฒนาระบบหลังบ้าน (Back-end)																																									
Stage 1 Game design																																									
Stage 1 Graphic																																									
Stage 1 Programming																																									
Stage 2 Game design																																									
Stage 2 Graphic																																									
Stage 2 Programming																																									
Stage 3 Game design																																									
Stage 3 Graphic																																									
Stage 3 Programming																																									
Stage 4 Game design																																									
Stage 4 Graphic																																									
Stage 4 Programming																																									
Stage 5 Game design																																									
Stage 5 Graphic																																									
Stage 5 Programming																																									
Stage 6 Game design																																									
Stage 6 Graphic																																									
Stage 6 Programming																																									
Stage 7 Game design																																									
Stage 7 Graphic																																									
Stage 7 Programming																																									
Stage 8 Game design																																									
Stage 8 Graphic																																									
Stage 8 Programming																																									
ปรับปรุงแก้ไข																																									
ทดสอบระบบ																																									
เริ่มใช้งานจริง																																									
อบรม สัมนาเชิงปฏิบัติการ ร่วมกับ สถาบันการศึกษา และองค์กรภาครัฐ/เอกชน																																									
การส่งมอบและรายงาน													1																		2										

โครงการระบบออนไลน์เพื่อพัฒนาผู้เชี่ยวชาญด้านความปลอดภัยไซเบอร์

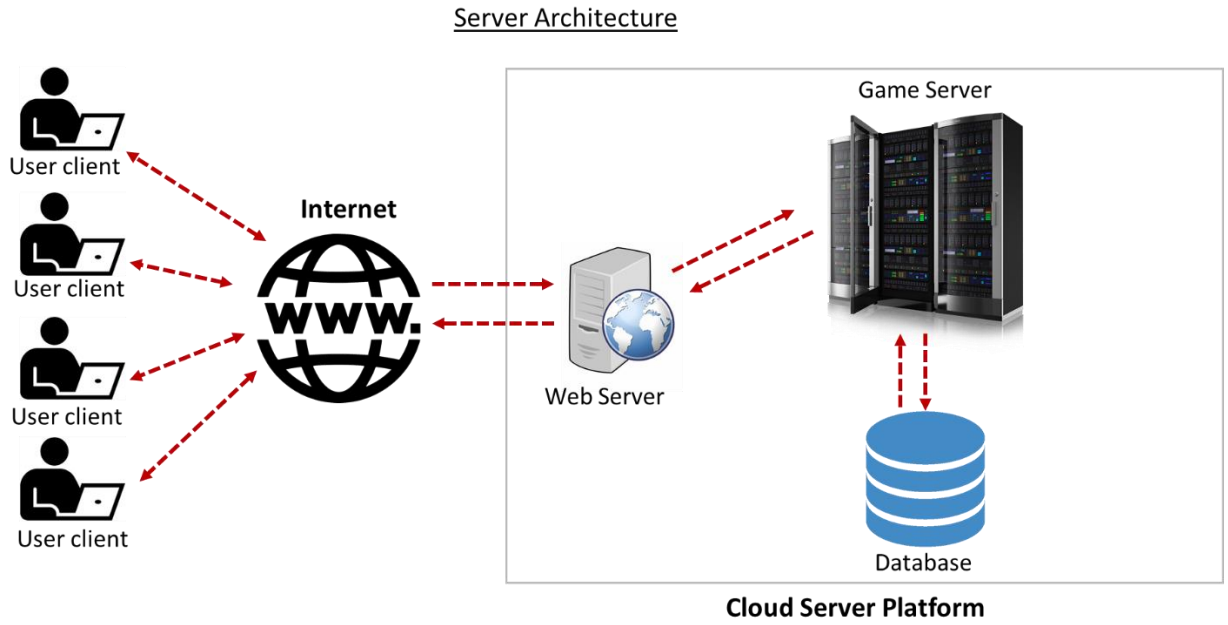
สัปดาห์	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81
รายละเอียดการดำเนินงาน	Jan 6	Jan 13	Jan 20	Jan 27	Feb 3	Feb 10	Feb 17	Feb 24	Mar 2	Mar 9	Mar 16	Mar 23	Mar 30	Apr 6	Apr 13	Apr 20	Apr 27	May 4	May 11	May 18	May 25	Jun 1	Jun 8	Jun 15	Jun 22	Jun 29	Jul 6	Jul 13	Jul 20	Jul 27	Aug 3	Aug 10	Aug 17	Aug 24	Aug 31	Sep 7	Sep 14	Sep 21	Sep 28	Oct 5
เซ็นสัญญาโครงการ																																								
ทำการศึกษาวิเคราะห์ออกแบบระบบ																																								
จัดทำสรุปแผนการดำเนินงานโครงการ การวิเคราะห์ และออกแบบระบบ																																								
จัดหาระบบ Cloud Server และ software ที่เกี่ยวข้องในการทำงาน																																								
ออกแบบระบบหน้าบ้าน (Front-end)																																								
ออกแบบระบบหลังบ้าน (Back-end)																																								
พัฒนาระบบหน้าบ้าน (Front-end)																																								
พัฒนาระบบหลังบ้าน (Back-end)																																								
Stage 1 Game design																																								
Stage 1 Graphic																																								
Stage 1 Programming																																								
Stage 2 Game design																																								
Stage 2 Graphic																																								
Stage 2 Programming																																								
Stage 3 Game design																																								
Stage 3 Graphic																																								
Stage 3 Programming																																								
Stage 4 Game design																																								
Stage 4 Graphic																																								
Stage 4 Programming																																								
Stage 5 Game design																																								
Stage 5 Graphic																																								
Stage 5 Programming																																								
Stage 6 Game design																																								
Stage 6 Graphic																																								
Stage 6 Programming																																								
Stage 7 Game design																																								
Stage 7 Graphic																																								
Stage 7 Programming																																								
Stage 8 Game design																																								
Stage 8 Graphic																																								
Stage 8 Programming																																								
ปรับปรุงแก้ไข																																								
ทดสอบระบบ																																								
เริ่มใช้งานจริง																																								
อบรม สัมนาเชิงปฏิบัติการ ร่วมกับ สถาบันการศึกษา และองค์กรภาครัฐ/เอกชน																																								
การส่งมอบและรายงาน											3																											4		

บทที่ ๓. วิธีการดำเนินโครงการ

๓.๑ การดำเนินการจัดหาระบบ Server เพื่อใช้กับระบบ

จากการประเมินเรื่องของการจัดซื้อ Hardware Server มาใช้ในโครงการนั้นต้องใช้เวลาในการจัดหาและเมื่อประเมินถึงประสิทธิภาพของการจัดการ การเข้าถึงระบบผ่านอินเทอร์เน็ตนั้น ทางโครงการจึงเลือกที่จะใช้วิธีเช่าใช้บริการระบบ Cloud Server จากทางผู้ให้บริการ โดยจะคิดค่าเช่าระบบตามปริมาณการใช้พื้นที่และปริมาณข้อมูล Traffic ที่ไหลเข้าออกของระบบ โดยในระยะแรกในระหว่างการพัฒนาระบบจะทำให้มีค่าใช้จ่ายที่ต่ำ ในแต่ละเดือนเมื่อระบบพร้อมให้บริการ คาดว่าจะมี Traffic User ที่ประมาณการไว้ที่ ๒๐๐ Concurrent User ซึ่งในช่วงนี้ก็จะทำให้มีค่าบริการรายเดือนที่เพิ่มสูงตามขนาด Traffic ที่มีการใช้งาน

System Architectures



ภาพที่ ๒ System Architectures

Google Cloud as a Service

https://firebase.google.com/

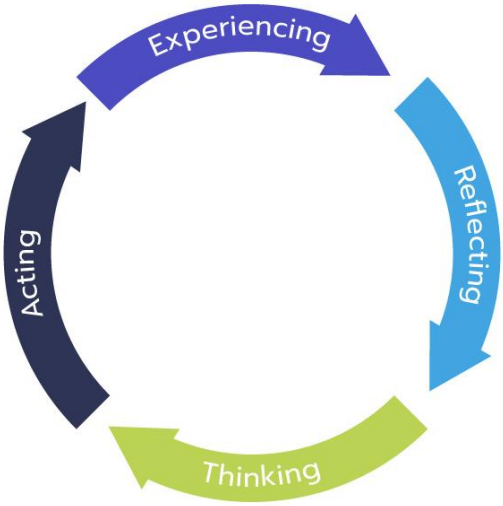
๓.๒ การออกแบบระบบ Cybersecurity Learning Platform

๓.๒.๑ ทฤษฎีการเรียนรู้ที่นำมาใช้ในการออกแบบ

[๑๖]

‘ทฤษฎีการเรียนรู้จากประสบการณ์’ หรือ Experiential Learning Theory (ELT) โดย ดร.เดวิด เอ. โคล์บ (Dr.David A. Kolb) นักทฤษฎีการศึกษา ซึ่งเป็นผู้ริเริ่มแนวคิดนี้

หลักการของ ELT มีอยู่ว่า คนเรามีรูปแบบการเรียนรู้อยู่ ๔ โหมดซึ่งหมุนเป็นวงจรสลับสับเปลี่ยนอย่างต่อเนื่องตลอดเวลาได้แก่ experiencing (มีประสบการณ์ ลงมือทำ) reflecting (ใคร่ครวญ) thinking (คิดวิเคราะห์ สังเคราะห์ความรู้ใหม่ด้วยตนเอง) และ acting (ลงมือทำซ้ำจากความรู้ ความเข้าใจที่พัฒนาขึ้น)



ภาพที่ ๓ วงจรของการเรียนรู้ผ่านประสบการณ์ (The Experiential Learning Cycle)

ด้วยเป้าหมายและหลักการที่สอดคล้องกับความต้องการที่แท้จริงของสังคมปัจจุบัน ELT จึงกลายเป็นแนวทางจัดการศึกษาที่ได้รับการยอมรับและถูกนำไปประยุกต์ใช้ในโรงเรียนและมหาวิทยาลัยทั่วโลกและถูกบรรจุในหลักสูตรการศึกษาภาคบังคับของนิวซีแลนด์และสิงคโปร์เลยทีเดียว

๑. การเรียนรู้เป็นวงจรต่อเนื่องไม่สิ้นสุด

วงจรการเรียนรู้ (learning cycle) เป็นกระบวนการของการแลกเปลี่ยนระหว่างโลกภายในของผู้เรียนกับสิ่งแวดล้อมภายนอก ซึ่งเกิดขึ้นต่อเนื่อง ไม่สิ้นสุด เหมือนการหายใจที่เป็นกระบวนการรับเข้า - ปล่อยออกที่ดำเนินไปตลอดชีวิต

สำหรับครูหรือผู้จัดการเรียนรู้การเรียนรู้จึงต้องให้ผู้เรียนได้ ‘รับเข้า’ และ ‘เอาออก’ คือให้ผู้เรียนรับความรู้ที่จำเป็นในการใช้ชีวิตและการทำงานในโลกปัจจุบันเข้ามาและให้เขาถ่ายทอดสิ่งที่ได้เรียนรู้นั้นออกมาเป็นช่วงการ ‘เอาออก’ ซึ่งเป็นกระบวนการที่ต้องใช้ทักษะขั้นสูง

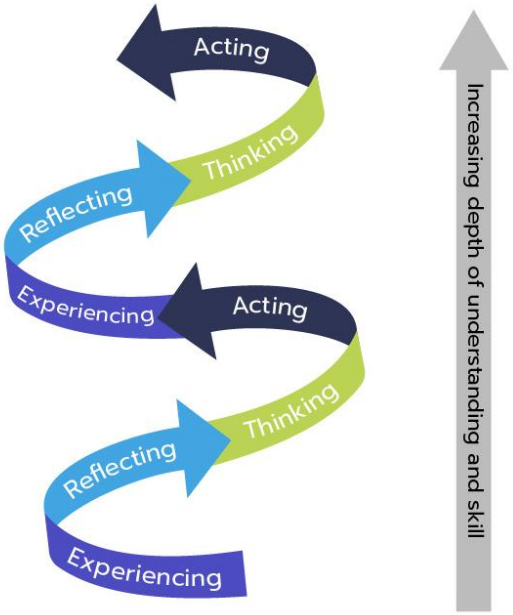
การเรียนรู้จึงไม่ใช่การส่งออกความรู้จากครูและผู้เรียนเป็นผู้รับแบบเป็นเส้นตรง (linear) แต่ในวงจรการเรียนรู้จะเริ่มจาก

๑) ผู้เรียนรับข้อมูลผ่านการมีประสบการณ์ ลงมือทำ (concrete experience)

๒) เปลี่ยนข้อมูลจากการมีประสบการณ์นั้นด้วยการใคร่ครวญ (reflection)

๓) คิดวิเคราะห์-สังเคราะห์ความรู้จากการได้มีประสบการณ์และคิดใคร่ครวญ (thinking) ทำให้ผู้เรียนมีข้อมูล ความรู้ และความเข้าใจแบบหนึ่ง

๔) ผู้เรียนจะเปลี่ยนความรู้และความเข้าใจนั้นอีกครั้งผ่านการลงมือทำซ้ำ (acting) เหล่านี้เป็นวงจรเรียนรู้ที่ผู้เรียนเป็นทั้งผู้รับและผู้สร้างความรู้



ภาพที่ ๔ เกลียวการเรียนรู้ผ่านประสบการณ์ (The Experiential Learning Spiral)

๒. ประสบการณ์จริง สิ่งที่ขาดไม่ได้ในการเรียนรู้

ในวงจรการเรียนรู้ ‘การมีประสบการณ์’ (experience) นั้นมีความสำคัญเป็นอย่างมาก ก่อนอื่นต้องทำความเข้าใจก่อนว่าทุกโหมดในวงจรการเรียนรู้คือประสบการณ์ทั้งหมด แต่เป็น ‘ประสบการณ์’ ที่เกิดขึ้นที่นี่ เดี๋ยวนี้ ที่นำไปสู่การเรียนรู้ บางประสบการณ์และพฤติกรรมที่เราเจอะเจอและทำมันทุกวันอาจเป็นสิ่งที่เราปฏิบัติสืบต่อกันมาและทำไปโดยอัตโนมัติเนื่องจากการเรียนรู้ก่อนหน้านั้นหล่อหลอมขึ้นเป็นนิสัยและวิถีประเพณีที่ติดตัวมาโดยตลอด ถึงประสบการณ์อาจจะดูเป็นสิ่งใหม่ที่เพิ่งประสบแต่แท้จริงมันคือสิ่งที่แฝงไว้ด้วยการตีความของคนรุ่นก่อนหน้าเรามาแล้วทั้งสิ้น

จอห์น ดิวอีย์ (John Dewey) นักจิตวิทยาและปฏิรูปการศึกษาชาวอเมริกันชี้ว่าการที่คนเราจะใคร่ครวญและเข้าใจวิถีทางของประสบการณ์ในลักษณะนี้ได้นั้นต้องเข้าไปสัมผัสประสบการณ์เหล่านั้นอย่างลึกซึ้งก่อน เช่น เมื่อเรา ‘ติดขัด’ กับปัญหา เกิดความยากลำบาก หรือ ‘ประหลาดใจ’ กับสิ่งที่แปลกใหม่ต่างจากประสบการณ์เดิมที่ผ่านมา วิลเลียม เจมส์ (William James-๑๙๙๗) นักจิตวิทยาชื่อดังเรียกประสบการณ์นี้ว่า ‘ประสบการณ์บริสุทธิ์’ (pure experience)

หลายคนมองว่าการใคร่ครวญถอดบทเรียนจากสิ่งที่เรียนรู้ในประสบการณ์เป็นสิ่งที่สำคัญที่สุดแต่ที่จริงแล้วขั้นตอนแรกสุดที่จะนำไปสู่การใคร่ครวญถอดบทเรียน คือการได้เข้าไปสัมผัสกับประสบการณ์ ‘บริสุทธิ์’ ที่ลบล้างวิธีคิดเก่า หรือเมื่อได้เผชิญกับสิ่งที่เหนือความคาดหมายเดิมต่างหาก แม้การเรียนรู้อาจเกิดขึ้นได้จากประสบการณ์ที่พบเจอได้ทุกวันก็ตามที แต่การเรียนรู้ที่ได้ก็มักให้คำตอบคล้ายเดิมหรืออาจช่วยเปลี่ยนความคิดและพฤติกรรมได้เพียงนิดเดียว

๓. การเรียนรู้จากโหมดตรงกันข้าม ช่วยกระตุ้นการเรียนรู้

อะไรขับเคลื่อนวงจรการเรียนรู้ของคนเราให้ดำเนินไป ? และ อะไรผลักดันให้เราเรียนรู้ ? คำตอบของคำถามนี้อยู่ที่การเรียนรู้ด้วยโหมดขั้วตรงข้ามซึ่งอยู่ในวงจรการเรียนรู้ (The Dialectic Poles of the Cycle) นั่นเอง

การมีประสบการณ์ตรง (concrete experience) กับ การสรุปความคิดในใจ (abstract thinking) คือสองวิธีพื้นฐานที่อยู่ขั้วตรงข้ามกัน ซึ่งมนุษย์ใช้สองขั้วตรงข้ามนี้ในการทำความเข้าใจประสบการณ์ วิลเลียม เจมส์ เรียกแทนสองขั้วนี้ว่า ‘percepts & concepts’ กล่าวคือ perception เป็นการรับรู้ประสบการณ์ที่เกิดขึ้น ณ ปัจจุบัน ส่วน conception เป็นความคิดที่ย้อนระลึกถึงประสบการณ์ในอดีตและสิ่งที่จะเกิดในอนาคต เปรียบสองสิ่งนี้เป็นใบมีดของกรรไกรที่เวลาใช้งานจะขาดใบมีดข้างใดข้างหนึ่งไปไม่ได้ เช่นเดียวกับที่เราต้องใช้ทั้ง ‘ประสบการณ์’ และ ‘ความคิด’ ในการทำความเข้าใจโลกรอบตัว

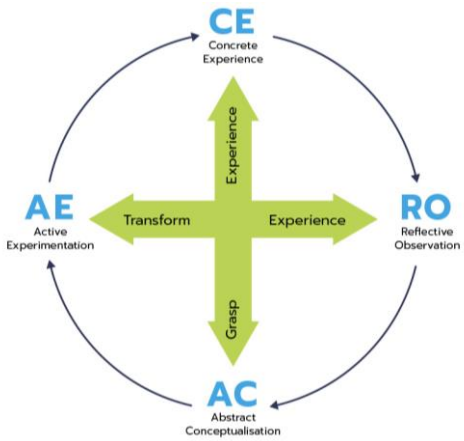
การใคร่ครวญ (reflecting) และ การลงมือทำ (acting)

ก็เช่นเดียวกัน สองโหมดนี้ต่างก็เป็นกระบวนการที่ใช้เรียนรู้และทำความเข้าใจ เปาโล เฟรรี (Paulo Freire) นักการศึกษาคนสำคัญของโลกยืนยันว่าการที่บุคคลเล่าถึงประสบการณ์ว่าตนทำอะไรมาบ้าง (practice) นั้นสำคัญมาก เพราะจะได้ใช้กระบวนการทำความเข้าใจด้วยขั้วตรงข้ามระหว่าง ‘ความคิดใคร่ครวญ’ กับ ‘การลงมือทำ’ นั่นเอง

อย่างไรก็ตามถ้าใช้ขั้วใดขั้วหนึ่งมากเกินไป เช่น action มากไป เอาแต่ลงมือทำอย่างเดียวโดยไม่มีการฉุกคิดไตร่ตรองในสิ่งที่ทำ หรือ reflection มากไป เอาแต่คิดใคร่ครวญโดยไม่ลงมือทำสักที ความเข้าใจก็จะไม่เกิดการทำความเข้าใจด้วยโหมดการเรียนรู้ขั้วตรงข้ามที่กล่าวมานี้ ช่วยให้ความคิดอ่านของเรามีลักษณะแบบ ‘เสียงสเตอริโอ’ คือเสียงที่ดังออกมาแยกจากกัน ซึ่งเสียงต่างขั้วเหล่านั้นเองที่ผลักดันให้เราเกิดการเรียนรู้ และถ้าขั้วใดทำงานมากเกินไปก็จะไม่เกิดการเรียนรู้ การมุ่งเน้นกิจกรรมจนเกินไปหรือมัวแต่ขบคิดใคร่ครวญล้วน ไม่ก่อประโยชน์ในการเรียนรู้

ความเชื่อบางอย่างแบบดันทุรังก็สามารถขัดขวางการเปิดประสบการณ์ใหม่ๆ ของเราได้เช่นกัน เช่นเดียวกับที่ความหมกมุ่นอยู่แต่กับประสบการณ์ก็อาจทำให้ความคิดไม่กระจ่างชัดมากพอ

อย่างไรก็ตามประสบการณ์ที่เข้มข้นสั่นสะเทือนระดับ ‘ช็อกจนตาค้าง’ (shock and awe) สามารถกระตุ้นให้บุคคลทบทวนความคิดความเชื่อเสียใหม่ ซึ่งส่งผลต่อการรับประสบการณ์ครั้งต่อๆไป การคิดใคร่ครวญสิ่งที่เกิดขึ้นหลังจากลงมือทำก็จะช่วยแก้ไขสิ่งผิดและปรับปรุงสิ่งที่จะลงมือทำในอนาคตให้ดีขึ้นได้ แต่ในทางกลับกันการลงมือพร้อมกับคิดใคร่ครวญไปด้วยกลับไม่ก่อให้เกิดผลดี



ภาพที่ ๕ แผนผังแสดงการเรียนรู้ด้วยโหมดขั้วตรงข้ามที่อยู่ในวงจรการเรียนรู้

๔. ผู้เรียนมีสไตล์การเรียนรู้หลากหลาย และเปลี่ยนรูปแบบไปเรื่อยๆ

แต่ละคนมี ‘สไตล์การเรียนรู้’ แตกต่างกัน แต่ละคนเรียนรู้ด้วยวิธีที่ไม่เหมือนกัน เมื่อผู้เรียนเข้าใจว่าตนเองมีวิธีการเรียนรู้อย่างไรครูหรือผู้จัดการเรียนรู้ก็จะสามารถจัดการเรียนการสอนหรือประสบการณ์ให้เหมาะสมได้

สไตล์การเรียนรู้ใน ELT หมายถึง จริตของผู้เรียนที่ชอบเรียนรู้ด้วยกระบวนการข้างใดข้างหนึ่งของ วงจรการเรียนรู้ (ข้างแรกคือ action and reflection กับอีกข้างคือ experience กับ thinking) สไตล์การเรียนรู้ของแต่ละคนถือเป็นนิสัยการเรียนรู้ที่ผู้เรียนมักใช้โหมดหนึ่งโหมดใดหรือหลายโหมดซ้ำๆ ในการเรียนรู้เป็น ประจำ หากมองเช่นนี้จะเข้าใจได้ว่าในการเรียนรู้ที่เกิดขึ้นนั้นจะไม่มีโหมดการเรียนรู้ใดเป็นแบบเดียว (stereotype) ตายตัว

การรู้ว่าตนเองมีสไตล์การเรียนรู้แบบไหนช่วยให้ผู้เรียนปรับการเรียนรู้ของตนให้ยืดหยุ่นกับเนื้อหาความรู้และความยากง่าย โดยสามารถเลือกใช้โหมดความรู้ได้แบบองค์รวมและปรับเปลี่ยนได้ตามสถานการณ์ ดร.โคล์บ และภรรยา ดร.เอลิซ โคล์บ (Dr. Alice Kolb) ร่วมกันคิดค้น The Kolb Learning Style Inventory (KLSI) หรือแบบวัดสไตล์การเรียนรู้ ซึ่งชี้ให้เห็นว่าสไตล์การเรียนรู้ของบุคคลถูกกำหนดโดยรูปแบบการเรียนรู้ที่ตนชอบที่สุดรวมกัน แผนผังของสไตล์การเรียนรู้มีหน้าตาเหมือน ‘ว่าว’ (ดูภาพที่ ๔) ซึ่งแผนผังรูปว่าวของแต่ละคนก็จะต่างกันเล็กน้อยตามแต่สไตล์ล่าสุดงานวิจัย KLSI ๔.๐ ได้ระบุรูปแบบการเรียนรู้เอาไว้ ๙ แบบคือ

๑) The Initiating Style – เริ่มเรียนรู้ด้วย ‘การลงมือทำ’ (action) ผ่านประสบการณ์หรือสถานการณ์

๒) The Experiential Style – เรียนรู้ด้วยการค้นหาความหมาย จากการ ‘เข้าไปมีประสบการณ์อย่างลึกซึ้ง’ (deep involvement in experience)

๓) The Imagining Style – เรียนรู้จากการจินตนาการความเป็นไปได้ ด้วยการสังเกต (observing) และถอดบทเรียนจากการร่วมประสบการณ์ (reflecting)

๔) The Reflecting Style – เรียนรู้โดยการเชื่อมโยงประสบการณ์กับไอเดีย ผ่านการคิดใคร่ครวญ

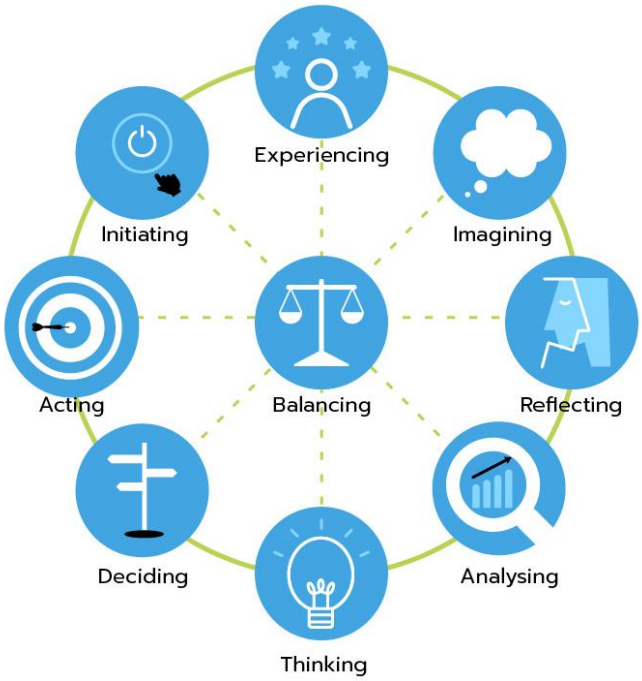
๕) The Analysing Style – เรียนรู้โดยการขมวดความคิดเป็นโมเดล หรือเป็นระบบจากการคิดใคร่ครวญ

๖) The Thinking Style – เรียนรู้ด้วยการคิดเชิงตรรกะ คิดเป็นเหตุเป็นผล

๗) The Deciding Style – ใช้ทฤษฎีหรือหลักการเพื่อตัดสินใจในการหาทางออกและลงมือทำบางอย่าง

๘) The Acting Style – มีแรงผลักดันที่จะทำบางอย่างให้บรรลุเป้าหมายโดยการจัดการคน (people) และงาน (tasks)

๙) The Balancing Style – ปรับตัวโดยชั่งน้ำหนักข้อดีข้อเสียระหว่างการลงมือทำกับการคิดใคร่ครวญ (acting vs reflecting) และ การสัมผัสประสบการณ์กับการคิด (experience vs thinking)



ภาพที่ ๖ สไตล์การเรียนรู้ ๙ แบบที่อยู่บนวงจรการเรียนรู้

๓.๒.๒ Game-Based Learning

การเรียนรู้ด้วยเกม (Game-Based Learning) เป็นการใช้งานระบบดิจิตอลเกมที่มีเป้าหมายที่มุ่งเน้น (เช่นวัตถุประสงค์ทางการศึกษา) เป็นเครื่องมือที่สนับสนุนการเรียนรู้ กระบวนการในวิธีที่สำคัญ เกมดิจิทัลเป็นเครื่องมือการเรียนรู้ ที่สามารถเพิ่มแรงจูงใจของนักเรียนเพื่อการเรียนรู้เพราะมีส่วนร่วมของผู้เล่นทำให้พวกเขามีส่วนร่วมและมีแรงจูงใจ ยิ่งไปกว่านั้นผู้เล่นยังสนุกไปกับการเล่นเกมเพราะพวกเขาต้องเรียนรู้ ซึ่งแน่นอน เมื่อการเล่นเกมดำเนินต่อไป ดังนั้นผู้เล่นต้องมีการพัฒนาทักษะและเรียนรู้กลยุทธ์ใหม่ ๆ จนกว่าเกมจะเสร็จสมบูรณ์ และอีกหนึ่งคุณสมบัติของเกมที่ สอดคล้องกับการเรียนรู้ที่ดีนั่นคือ เกมให้ความคิดเห็นสั้น ๆ สิ่งนี้ช่วยให้ ผู้เล่นสามารถ สำรวจสภาพแวดล้อมของเกม ลองสมมติฐานของพวกเขา เรียนรู้โดยทดลองและข้อผิดพลาดและรับข้อมูลทันที และพวกเขาสามารถใช้เพื่อกำหนดสมมติฐานที่ผิดพลาดอีกครั้ง ในสภาพแวดล้อมที่ถูกจำลองขึ้น ลักษณะนี้จะสอดคล้องกับข้อกำหนดการศึกษา ระบุว่าแนวทางการศึกษาส่วนใหญ่ ต้องการให้ผู้ให้การศึกษาแก่นักเรียน พร้อมข้อเสนอแนะเกี่ยวกับความสำเร็จของพวกเขา

ดังนั้นเกมจึงเป็นสื่อที่เหมาะสำหรับการส่งเสริมความเป็นจริง กระบวนการเรียนรู้และ“ เรียนรู้ด้วยการทำ” ประสบการณ์การเรียนรู้ของตัวเองในแง่นี้ดิจิตอล เกมสามารถให้ประสบการณ์การเรียนรู้ที่มีความหมายโดยจำลองสถานการณ์แบบโต้ตอบที่จะพบในโลกแห่งความจริง ปัญหาที่เกิดขึ้น ด้วยเหตุนี้เกมจึงเป็นตัวแทนของสื่อที่ดีเพื่อส่งเสริมการเรียนรู้อย่างและพัฒนาทักษะการแก้ปัญหาของนักเรียนการปฏิบัติตามและนำไปสู่ประสิทธิภาพที่สูงขึ้น

ขั้นตอนแรกสำหรับการออกแบบ Game-Based โดยกำหนดกิจกรรมการเรียนรู้คือการกำหนดองค์ประกอบที่มีลักษณะ การเรียนรู้จากเกมจากนั้นจึงทำการเชื่อมโยงองค์ประกอบเหล่านี้ทำให้เกิดกระบวนทัศน์ทางจิตวิทยาการสอน ในแบบ ProActive โดยจะพิจารณาได้ว่าเราไม่ได้เรียนรู้ เพียงวิธีเดียว แต่ในรูปแบบต่าง ๆ ที่ขึ้นอยู่กับเกี่ยวกับความถนัดส่วนตัวในสถานการณ์ สถานที่เรียนรู้เกิดขึ้นและเนื้อหา ที่จะเรียนรู้ มีรูปแบบ มีคำอธิบายของวิธีการที่แตกต่างกัน การเรียนรู้สำหรับคนต่าง ๆ จะขึ้นอยู่กับทฤษฎีการเรียนรู้อันแสดงถึงการเรียนรู้ที่ไม่ได้มีข้อจำกัดเฉพาะและในความเป็นจริงทุกคนสามารถมีการจัดการในเรื่องที่แตกต่างกันได้ตามสถานการณ์

๑. การรับข้อมูล คือการถ่ายโอนข้อมูลการเรียนรู้ วิธีการเรียนรู้เป็นการทำซ้ำและลอกเลียนแบบอยู่เสมอ ของความรู้ที่ได้รับหรือของกิจกรรมทางความคิดของแต่ละบุคคล
๒. การเลียนแบบ: คือการมุ่งเน้นในการสร้างแบบจำลองพฤติกรรมโดยการสังเกตผู้อื่น ปฏิกิริยาต่อเหตุการณ์ แนวคิดหลักคือ ประสบการณ์การเรียนรู้ที่เป็นตัวแทนสามารถช่วยได้
๓. การทดลอง: คือ กระบวนการ“ เรียนรู้ด้วยการทำ” มันจะถูกนำไปใช้กับการเรียนรู้กิจกรรมเฉพาะที่ซับซ้อน หรืองานที่ต้อง ค้นคว้า ทดสอบ การใช้งาน และกระบวนการเรียนรู้ตามบริบทส่วนใหญ่จะเกี่ยวข้องกับกิจกรรมการปฏิบัติและทักษะ โดยทั่วไปจะใช้กับงานปฏิบัติการต่างๆ

ประสบการณ์ GBL นอกจากความคิดเกี่ยวกับที่ต้องการใช้เป็นวิธีใหม่จากการเรียนรู้แบบดั้งเดิมรูปแบบและรวมถึงนวัตกรรมและความคิดสร้างสรรค์ โดยขึ้นอยู่กับคุณสมบัติเหล่านี้

๑. วัตถุประสงค์การเรียนรู้ที่เข้าใจ ข้อความที่ชัดเจนและเฉพาะเจาะจงของสิ่งที่ผู้เรียนรู้จะสามารถดำเนินการได้ในตอนท้าย ของกิจกรรม
๒. บทบาทของการสอนที่ซึ่งแตกต่างจากแบบดั้งเดิม การสอนแบบ ProActive เกิดการทดลองเรียนรู้ รูปแบบ ความสงสัย และเกิดการศึกษาเพิ่มเติม
๓. บทบาทของผู้เรียนที่เปลี่ยนไป Fun to learn ในการโต้ตอบและการใช้งาน
๔. สภาพแวดล้อมของเกม โลกที่จำลองขึ้น กลศาสตร์ของเกมที่ใช้ และส่วนอื่นอีก (เช่นการสนทนาระหว่างเพื่อน chat, การสืบค้นข้อมูลเพิ่มเติม)
๕. กลยุทธ์การเรียนรู้ ซึ่งถือเป็นเส้นทางในการส่งเสริมการเรียนรู้ที่มีประสิทธิภาพ กระบวนการ. จุดเด่นการเล่นเกม ที่หมายถึง การเล่นเกมในด้านที่ต้องการ หรือความเหมาะสมกับมุมมองการเรียนรู้ในแต่ละแบบ
๖. การส่งเสริมการเรียนรู้ที่จะมาจากกลไกของเกมที่สามารถส่งเสริมการเรียนรู้ให้พัฒนาขึ้นไปได้
๗. ลักษณะของงาน จุดเด่นในเกม ผู้เล่นมีความอิสระที่จะกำกับตนเอง การใช้ประสบการณ์ตัวเองในการกำหนดวิธีการต่าง ๆ

๓.๓ Cyber Security Knowledge for Game-Based Learning Design

Cyber Security Knowledge Base for Elementary and Basic Level

เนื้อหาความรู้ที่นำมาอยู่ใน Game จะเป็นความรู้จาก Ethical Hacking Course ซึ่งประกอบไปด้วย [๑๗]

๑. What is Hacking?
๒. Potential Security Threats To Your Computer Systems
๓. Skills Required to Become a Ethical Hacker
๔. Top ๒๐ Ethical Hacking Tools
๕. How to hack using Social Engineering
๖. How to make your data safe using Cryptography
๗. How to crack password of an Application
๘. Learn everything about Trojans, Viruses, and Worms
๙. Learn ARP Poisoning with Example
๑๐. Wireshark Tutorial: Network & Passwords Sniffer
๑๑. How to hack wireless networks

๑๒. Ultimate guide to DoS(Denial of Service) Attacks

๑๓. BEST DDoS Attack Tools

๑๔. How to Hack a Web Server

๑๕. How to Hack a Website

๑๖. Learn SQL Injection with practical example

๑๗. Hacking Linux Systems

๑๘. What is Digital Forensics? History, Process, Types, Challenges

๑๙. What is Cybercrime? Types, Tools, Example

ตัวอย่างเช่น (Example)

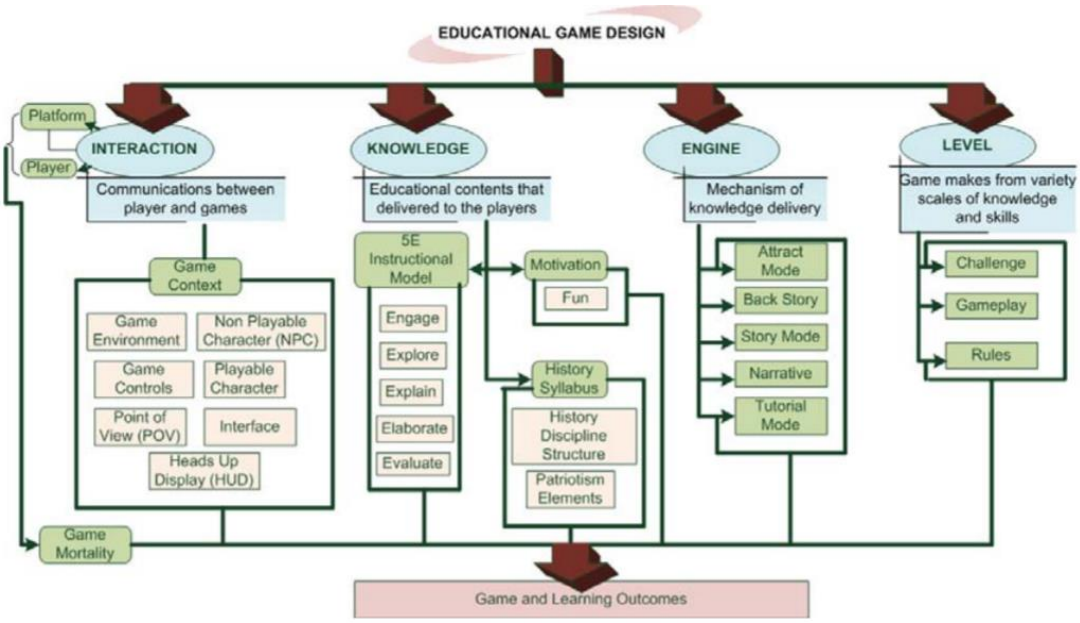
“What are some of the common Cyberattacks?”

Following are some common cyber attacks that could adversely affect your system.

ภาพที่ ๗ Cyber Security Knowledge Base for Elementary and Basic Level

๓.๔ Game Design Scenario and Flow

[๑๘]



ภาพที่ ๘ Game Design Scenario

ในการออกแบบเกมทางด้าน Mechanic จะนำกลยุทธ์การใช้วิธีการ ทาง Cyber Security มากระทำเพื่อไปสู่เป้าหมายของเกม โดยสอดแทรก action ทางด้าน cyber security เช่น การใช้ Social engineering หลอกล่อให้เหยื่อในเกมหลงกล โดยผู้เล่นจะต้องใช้เครื่องมือต่างๆ ในการเจาะระบบ เช่น Network Scanning, Phishing , Malware , Trojan, Encryption, Password crack, etc.

ในเกมจะมี Action ให้เลือกโดยจำกัด ตามเงื่อนไขของแต่ละด่าน และต้องแข่งกับเวลา ซึ่ง Scoring จะสัมพันธ์กับการใช้เวลาในเกม โดยในการดำเนินเรื่องของเกม จะมีจุด Action ที่เมื่อผู้เล่นเลือกวิธีการนี้จะทำให้ถูกหักแต้มอยู่ในด่านด้วย

ลักษณะเกมจะแทรกความรู้ ระหว่างเล่น และเมื่อเล่นจบในแต่ละด่าน จะมีสรุป อธิบายรายละเอียดรวมถึงผลกระทบ และยังบอกวิธีการป้องกัน และ จะเป็นคำแนะนำ เพื่อให้เกิดความตระหนักรู้ และการค้นคว้าหาข้อมูลต่อในเรื่องของความปลอดภัยทางไซเบอร์มากขึ้น

๓.๕ Game Design Level/Scenario Mockup

๑. ด่าน ๑ ประเทศไทย, การ Hack ระบบอาคารสำนักงาน เพื่อก่อกวนระบบควบคุมการจราจร

๒. ด่าน ๒ ประเทศฝรั่งเศส, เจาะระบบจากตึกสำนักงานที่ควบคุม หอไอเฟล เพื่อไปเข้าควบคุมระบบ เช่น ปิดระบบ เข้าออก ปิดไฟทั้งตึก การสร้างความปั่นป่วน

๓. ด่าน ๓ ประเทศอียิปต์, เป็นการ Hack เข้าระบบในพิรามิดใต้ฐานพีรามิดมีห้องควบคุมระบบภายใน

๔. ด่าน ๔ ประเทศอิหร่าน, เข้าไปเจาะระบบ คลังเก็บน้ำมัน (ลักษณะ เป็นห้องควบคุมแหล่งผลิตน้ำมัน)

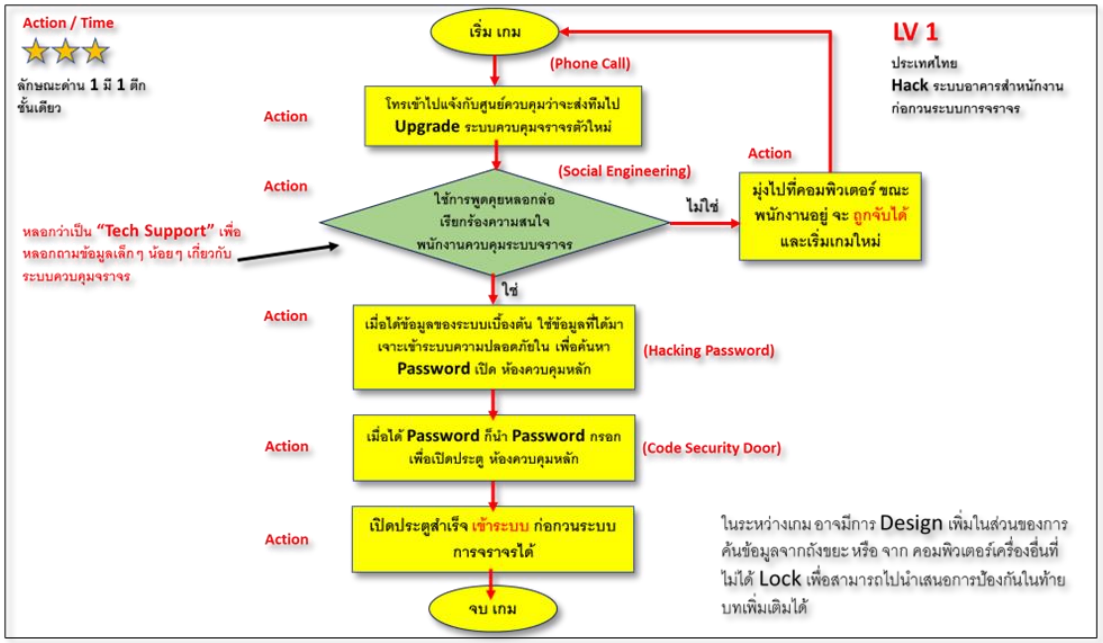
๕. ด่าน ๕ ประเทศอังกฤษ, เข้าไปเจาะระบบเพื่อไปแก้ไข เวลาของหอนาฬิกาบิกเบน (ห้องควบคุม ระบบของนาฬิกา)

๖. ด่าน ๖ ประเทศรัสเซีย, โจรกรรมเพชร ในพิพิธภัณฑ์ห้องเซฟเก็บเพชร

๗. ด่าน ๗ ประเทศจีน, เป็นการ Hack เข้าระบบ เพื่อไปสกัดกั้น ระบบขนการส่งสินค้า

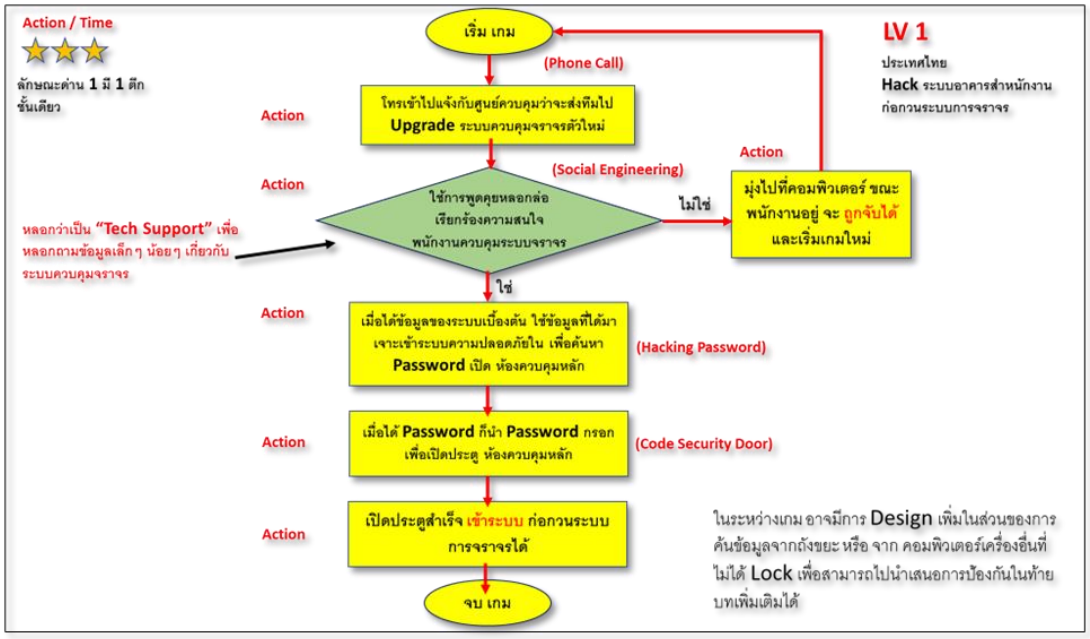
๘. ด่าน ๘ ประเทศอเมริกา, Hack ระบบปล่อยกระสวยอวกาศ ระบบการสื่อสาร การปล่อยดาวเทียม (เสริมในเรื่องของเวลาปล่อยกระสวย แข่งกับเวลา)

๑st Stage



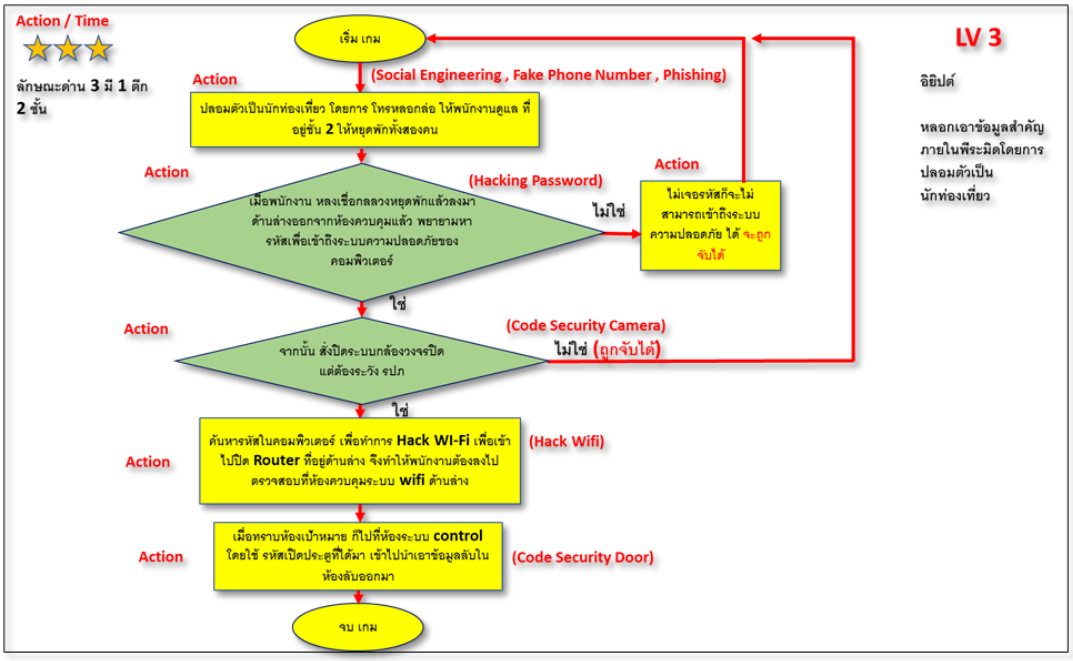
ภาพที่ ๙ การออกแบบ Scenario ด่านที่ ๑

๒nd Stage



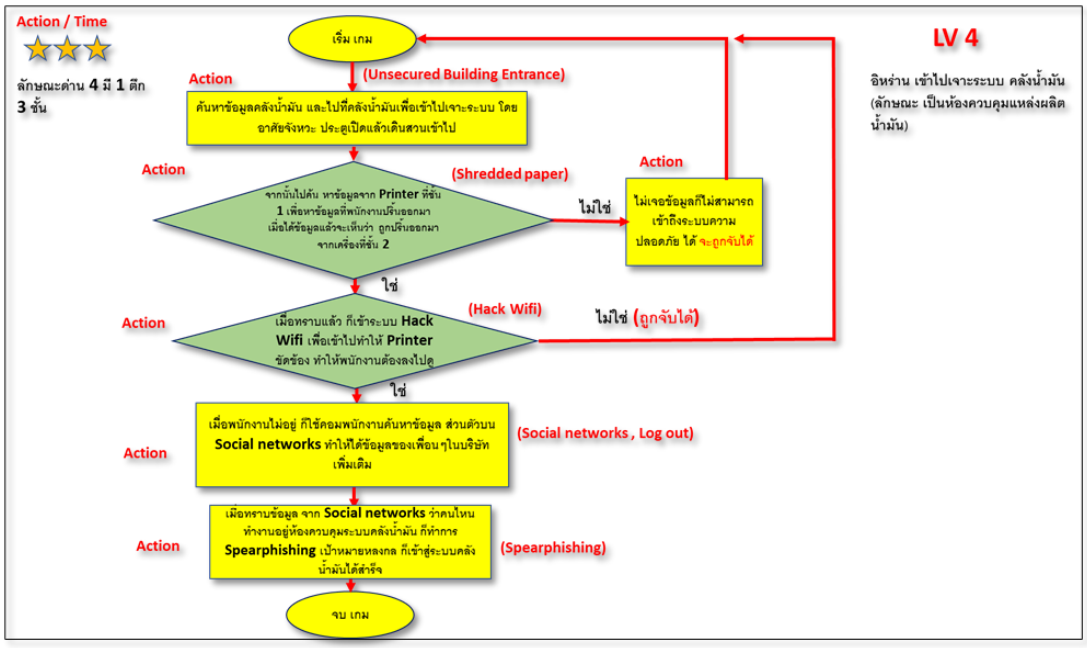
ภาพที่ ๑๐ การออกแบบ Scenario ด่านที่ ๒

๓rd Stage



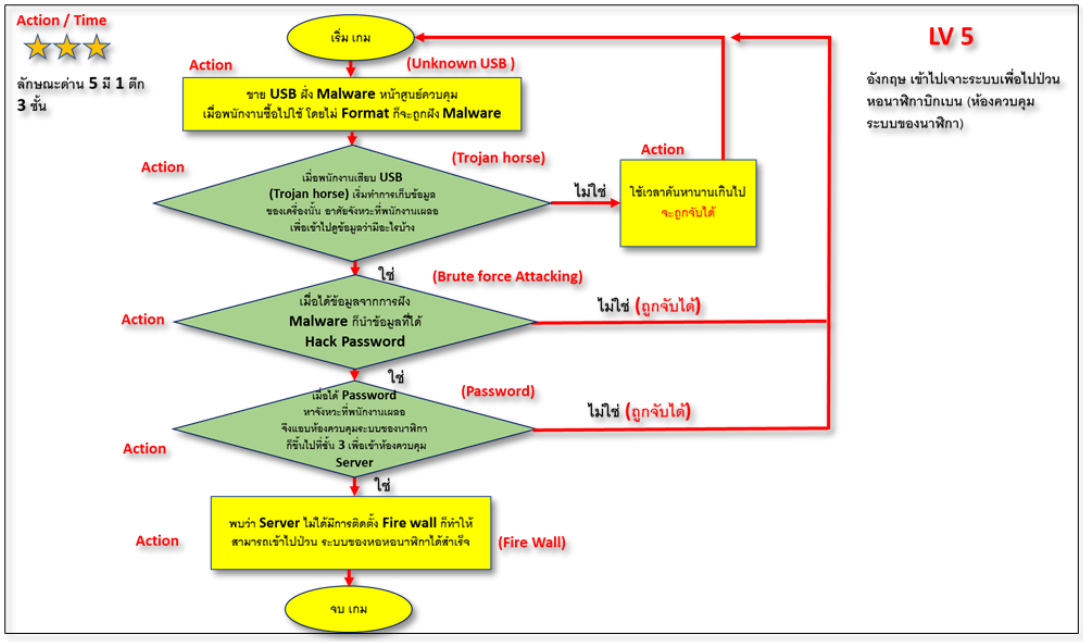
ภาพที่ ๑๑ การออกแบบ Scenario ด่านที่ ๓

๔th Stage



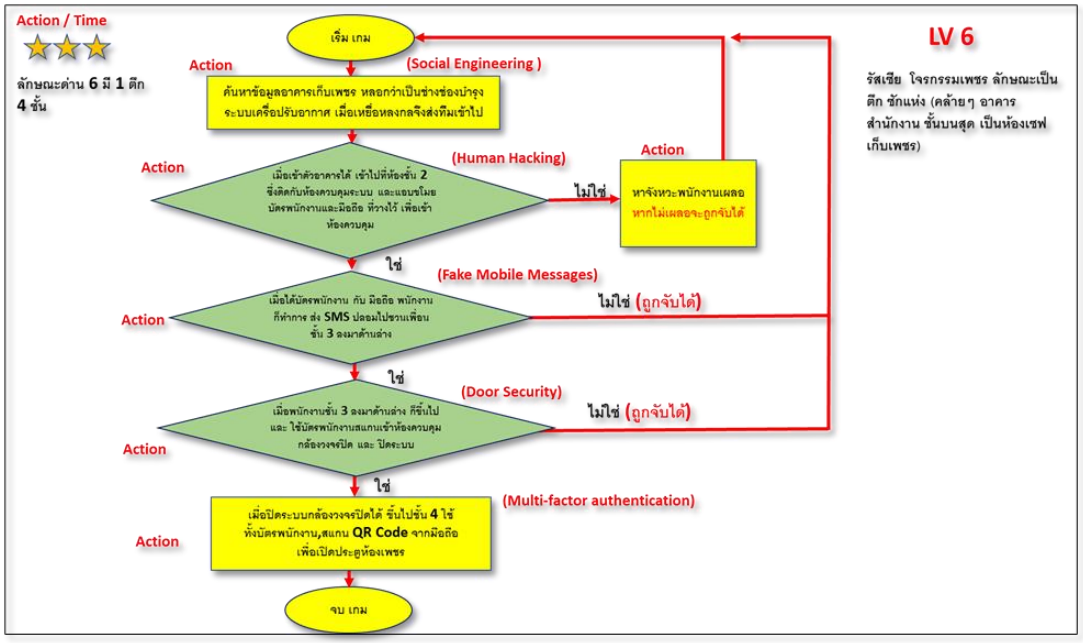
ภาพที่ ๑๒ การออกแบบ Scenario ด่านที่ ๔

๕th Stage



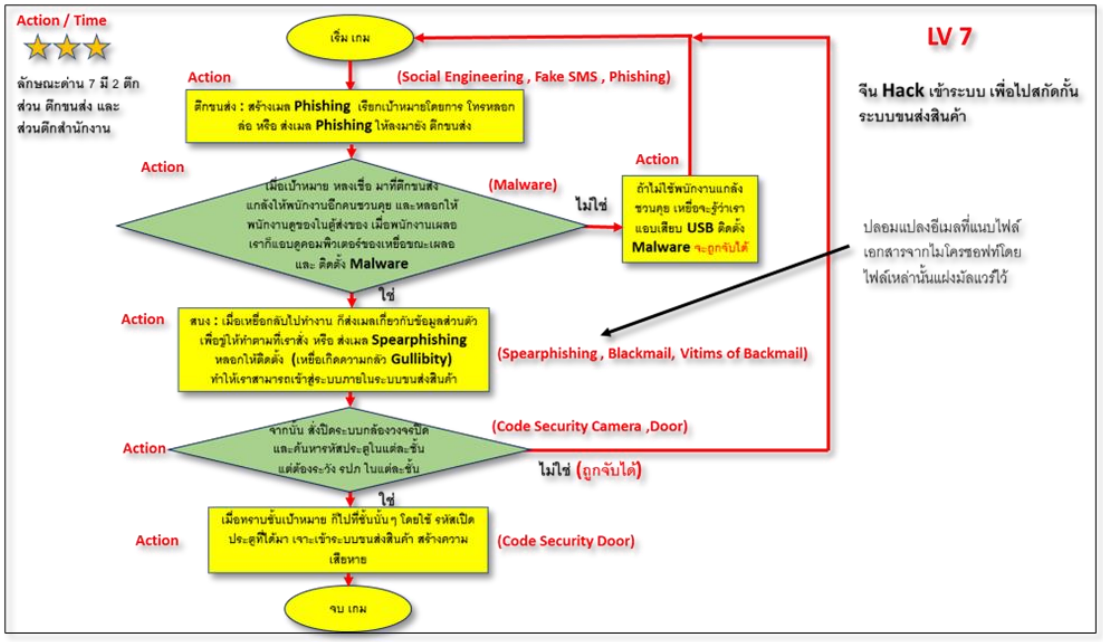
ภาพที่ ๑๓ การออกแบบ Scenario ด่านที่ ๕

๖th Stage



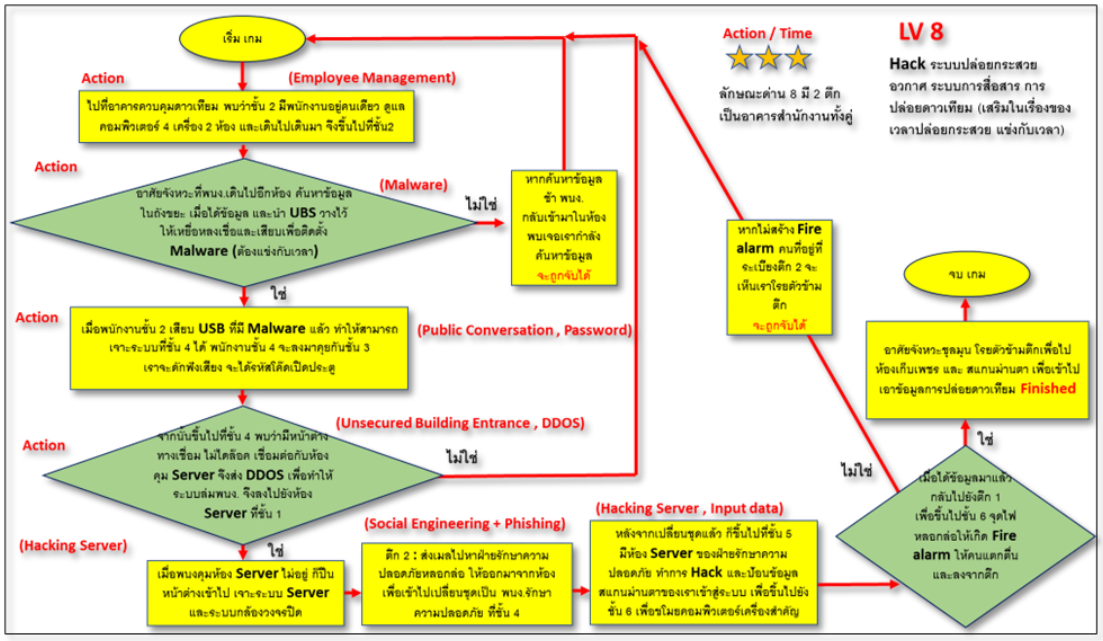
ภาพที่ ๑๔ การออกแบบ Scenario ด่านที่ ๖

๗th Stage



ภาพที่ ๑๕ การออกแบบ Scenario ด่านที่ ๗

๘th Stage



ภาพที่ ๑๖ การออกแบบ Scenario ด่านที่ ๘

๓.๖ Web UI Design Mockup

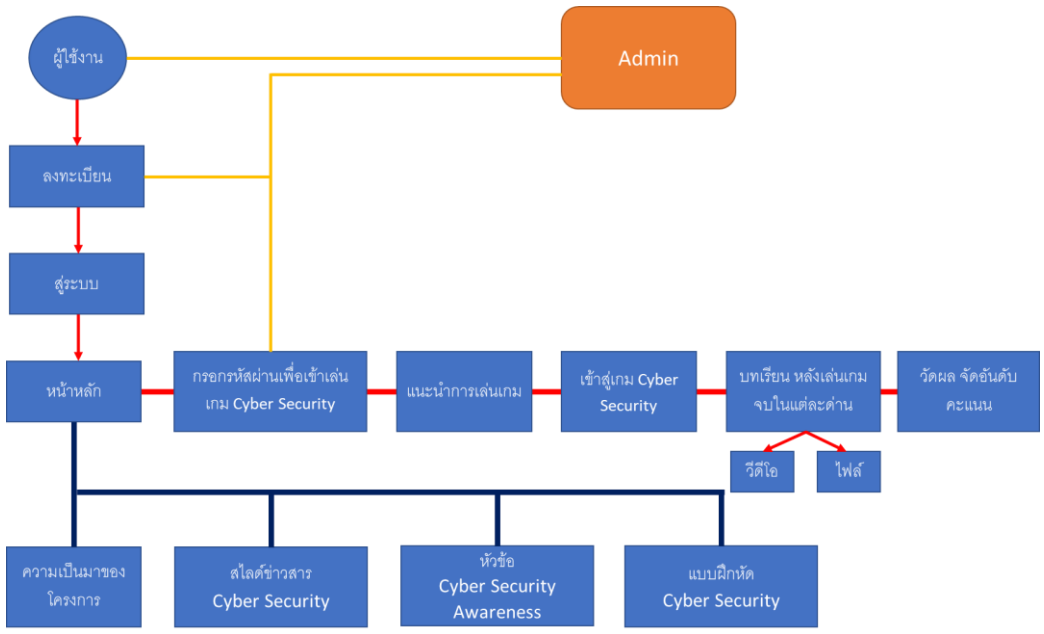
ในการ Design ออกแบบหน้า website เบื้องต้น จะออกแบบ Dashboard ที่มีความง่ายในการใช้งานไม่ซับซ้อน โดยจะมีการนำ ข่าวสารเกี่ยวกับ IT , Technology , Cybersecurity Knowledge, Video Link Knowledge มาอยู่บนหน้า Web โดยในหน้าของเวบไซท์ จะมีให้ผู้ใช้ Log in , Register ไม่ว่าจะเป็น ผ่าน Social network (Facebook, Twitter) & Email (Google Account)

มีหัวข้อให้ความรู้เกี่ยวกับความปลอดภัยทางไซเบอร์ เพื่อให้เกิดความตระหนักในการใช้งานบนโลกออนไลน์ ผู้ใช้สามารถเข้าไปทำความเข้าใจและศึกษาข้อมูลได้ตาม หัวข้อต่างๆ และจะมีแบบฝึกหัดให้ทำท้ายบท

ในส่วนของเกม จะเป็นเกมที่มีความสนุก และ สอดแทรกความรู้เข้าไป เบื้องต้นมีทั้งหมด ๘ ด่าน โดยไล่ระดับความยากขึ้นไป ในแต่ละด่านจะมี Action ให้ทำ โดยคะแนนจะมาจากเวลา และ ความถูกต้องของผู้เล่น และยังมีการจัดลำดับผู้เล่นอีกด้วย

ส่วนหนึ่งของหน้าเวบ จะมีเป็น ห้องตั้งกระทู้ , Chat bord ให้ทางผู้ใช้งานสามารถพูดคุยเกี่ยวกับเรื่องความปลอดภัยทางไซเบอร์ สอบถามปัญหา แบ่งปันข้อมูลกันได้

๓.๗ ขั้นตอนการทำงาน Web User Interface



ภาพที่ ๑๗ ขั้นตอนการทำงาน Web User Interface

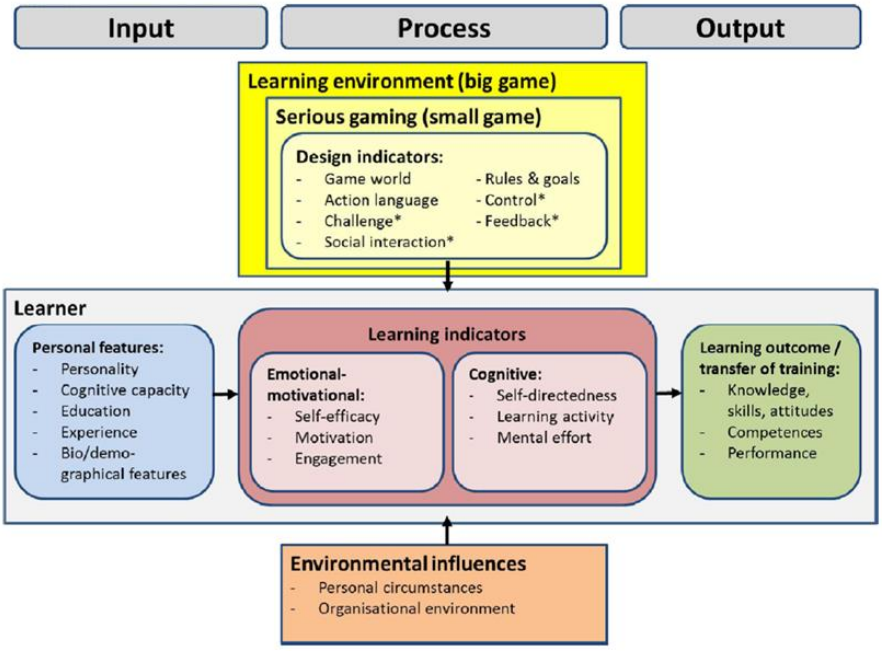
ภาพที่ ๑๘ ตัวอย่าง Web User Interface (๑)

ภาพที่ ๑๙ ตัวอย่าง Web User Interface (๒)

ภาพที่ ๒๐ ตัวอย่าง Web User Interface (๓)

๓.๘ Game-Based Learning Evaluation

[๑๙]



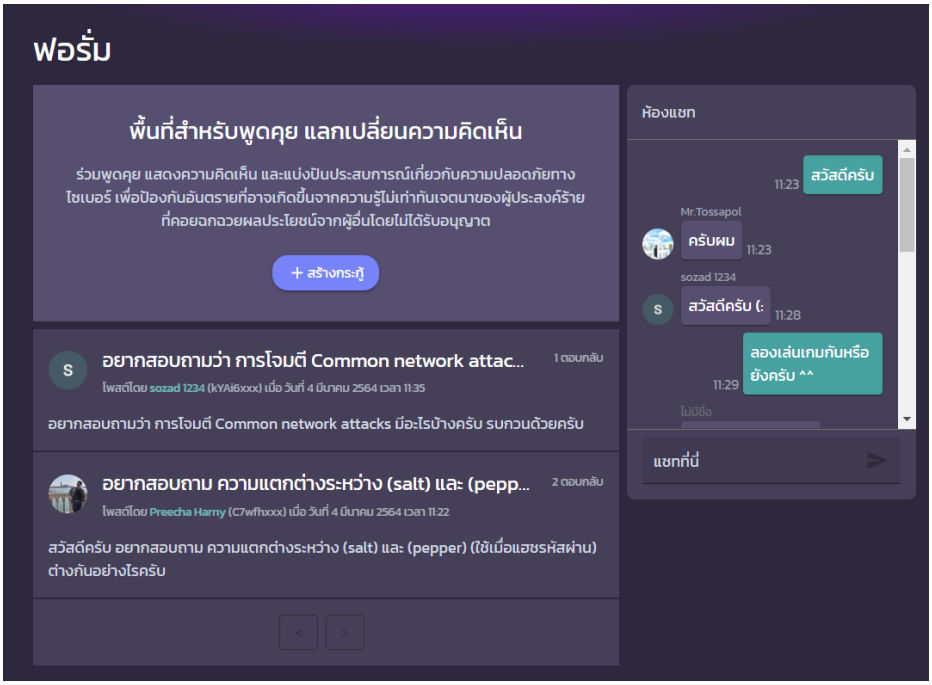
ภาพที่ ๒๑ Game-Based Learning Evaluation

Game-Based Learning Evaluation Model จะบ่งชี้ประเภทของตัวชี้วัดที่ใช้ในการวัด การตรวจวัดจะมีความเกี่ยวเนื่องกัน โดยมีแนวคิดคือ ผลลัพธ์จากการเรียนรู้ จะเป็นตัวบ่งชี้ถึงรูปแบบและการเรียนรู้ตามคุณลักษณะของแต่ละบุคคล กับอิทธิพลของสภาพแวดล้อมต่างในการเรียนรู้

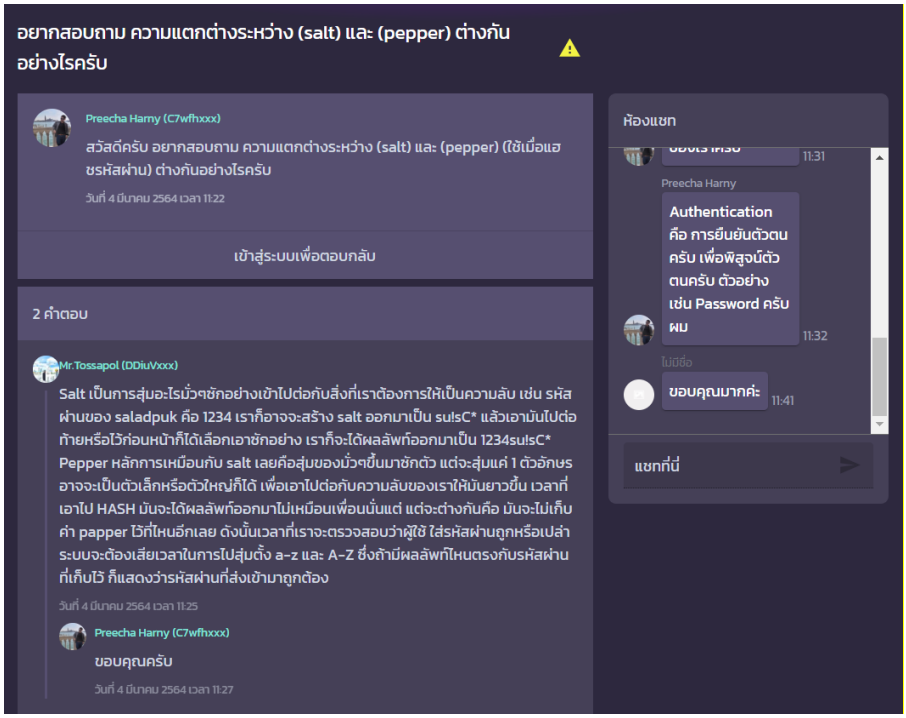
๑. การวัดความสำเร็จ (เช่น คะแนน)
๒. การเรียนรู้ข้อมูลที่เกี่ยวข้อง คำแนะนำต่างๆ กับความคืบหน้าสู่เป้าหมายของเกม
๓. สามารถเข้าใจถึงผลกระทบโดยตรงต่อการกระทำต่างๆที่อยู่เกม
๔. การค้นหาข้อมูลความรู้ต่างๆ ที่มีอยู่ใน Internet เพื่อนำมาใช้สนับสนุนการเรียนรู้การแก้ปัญหาในเกม
๕. ความ Challenge หมายถึงเนื้อหาจริงของเกมปัญหาที่ผู้เล่นต้องเผชิญ ปัญหาที่ต้องแก้ไขความคืบหน้าของการเล่น จะเป็นการวัดประสิทธิภาพของผู้เล่น

๓.๙ การจัดทำ Community Chat Room

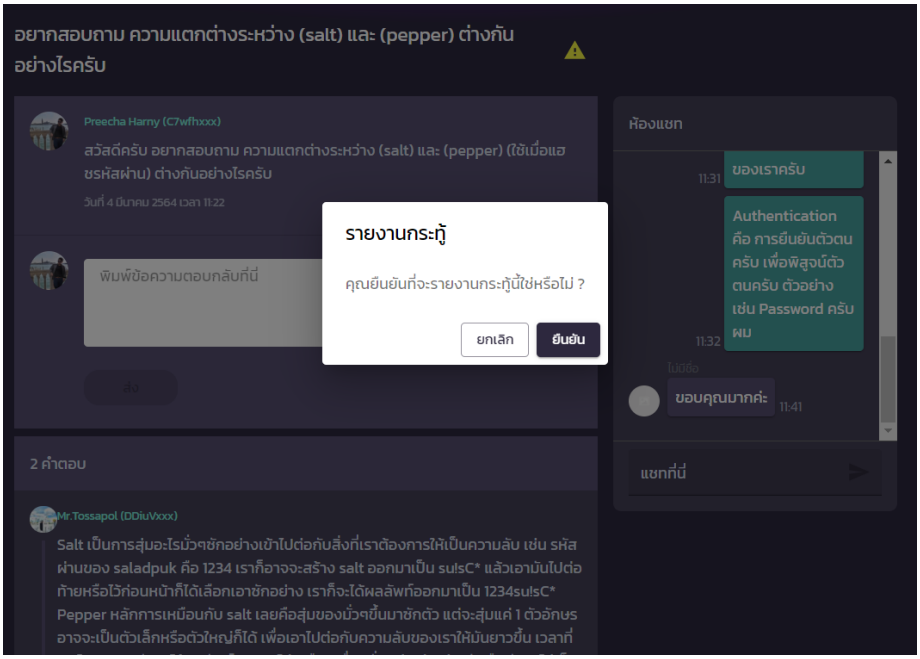
รายงานผลการจัดทำ Community Chat Room เบื้องต้นได้มีการทดสอบในส่วนของ ฟอรั่ม และ ห้องแชท โดยผู้ที่สามารถใช้พื้นที่ฟอรั่ม และห้องแชทได้จะต้องเป็นผู้ที่ลงทะเบียนเท่านั้น โดย Community Chat Room สามารถตั้งกระทู้แลกเปลี่ยนความคิดเห็น และแบ่งปันประสบการณ์เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ได้ หากว่ากระทู้ใดมีความไม่เหมาะสม ทางสมาชิกสามารถกดรายงานเพื่อแจ้งแอดมินเพื่อทำการตรวจสอบกระทู้ดังกล่าวได้



ภาพที่ ๒๒ แสดง Community Chat Room และ ฟอรั่ม



ภาพที่ ๒๓ แสดงการโต้ตอบ Community Chat Room และ ฟอรั่ม



ภาพที่ ๒๔ แสดงการรายงานกระทู้ที่ไม่เหมาะสม เพื่อให้แอดมินตรวจสอบจากระบบ

บทที่ ๔. ผลการดำเนินงานโครงการ

๔.๑ ผลการออกแบบภาพรวมเกมของทั้ง ๘ ด่าน

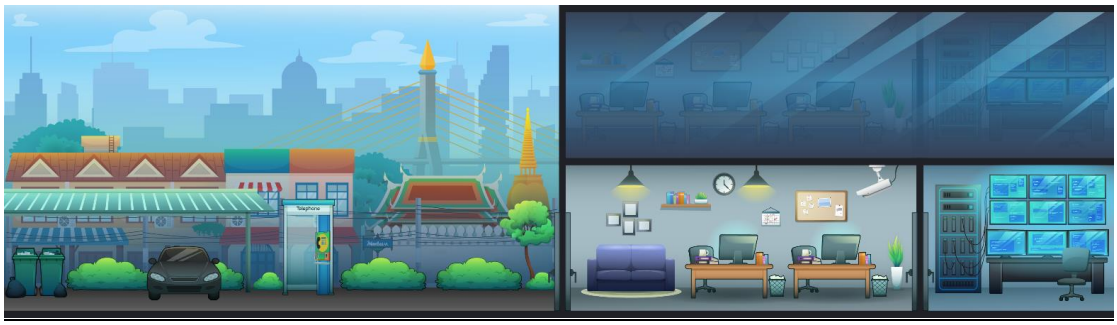
ผู้ใช้งานสามารถเลือกเล่นได้ทีละด่านตามลำดับ ๑ - ๘ เมื่อผ่านภารกิจของด่านนั้นๆ แล้วด่านถัดไปจะถูกปลดล็อค ก่อนเข้าทำภารกิจด่านที่ ๑ จะมีแบบทดสอบประเมินก่อนเล่น และจะมีแบบทดสอบอีกครั้งหากผู้เล่นได้ทำภารกิจครบทั้ง ๘ ด่านโดยสามารถเข้าได้ที่https://play.learncybersec.org/

ภาพที่ ๒๕ การออกแบบรูปแบบการเข้าร่วมเกม

ภาพที่ ๒๖ การออกแบบภาพรวมของทั้ง ๘ ด่าน

ด่าน ๑ (ประเทศไทย)

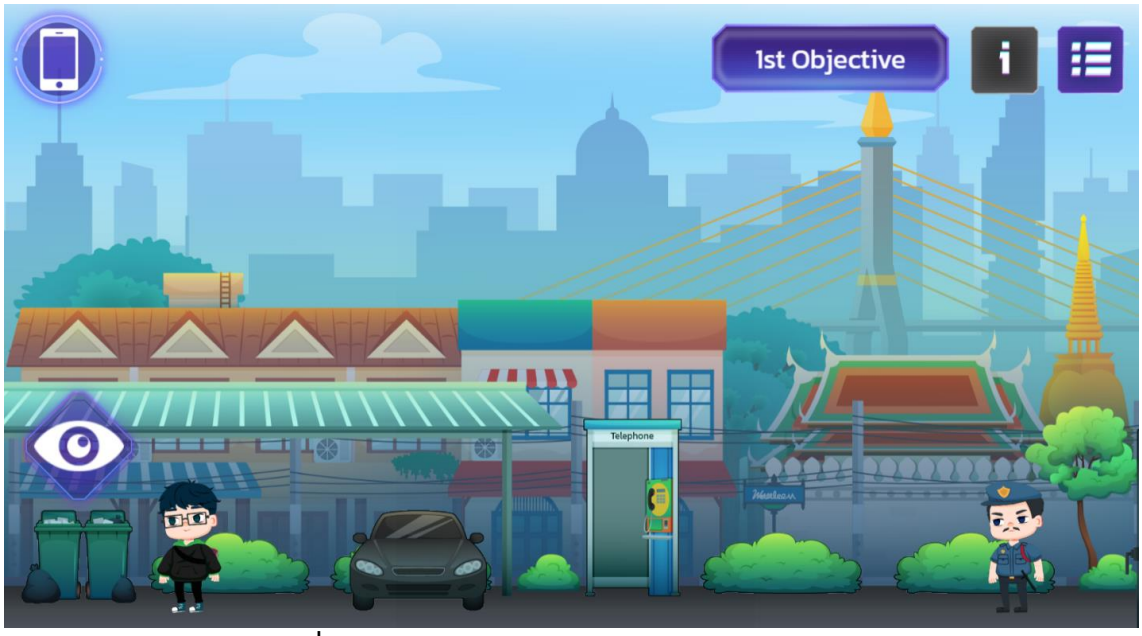
ดำเนินการออกแบบด่าน ๑ (ประเทศไทย) ลักษณะเป็นอาคารสำนักงานเล็กๆที่เผยพื้นที่เล่นแค่เพียง ๑ ชั้น โดยมีรถยนต์ ถังขยะพุ่มไม้ และตู้โทรศัพท์สาธารณะอยู่ภายนอกตัวอาคาร เมื่อเปิดเข้าไปภายในตัวอาคารจะแบ่งเป็น ๒ ห้อง ห้องแรกที่เปิดเข้าไป (ประตูธรรมดา) คือห้องของพนักงาน ๑ คนที่กำลังทำงานอยู่ และห้องด้านหลังคือห้อง Server ควบคุมระบบสัญญาณไฟจราจร



ภาพที่ ๒๗ Game Storyboard Design Chapter ๑

ลิงก์ https://play.learncybersec.org/

ภาพที่ ๒๘ Game Storyboard Design Chapter ๑



ภาพที่ ๒๙ Game Storyboard Design Chapter ๑

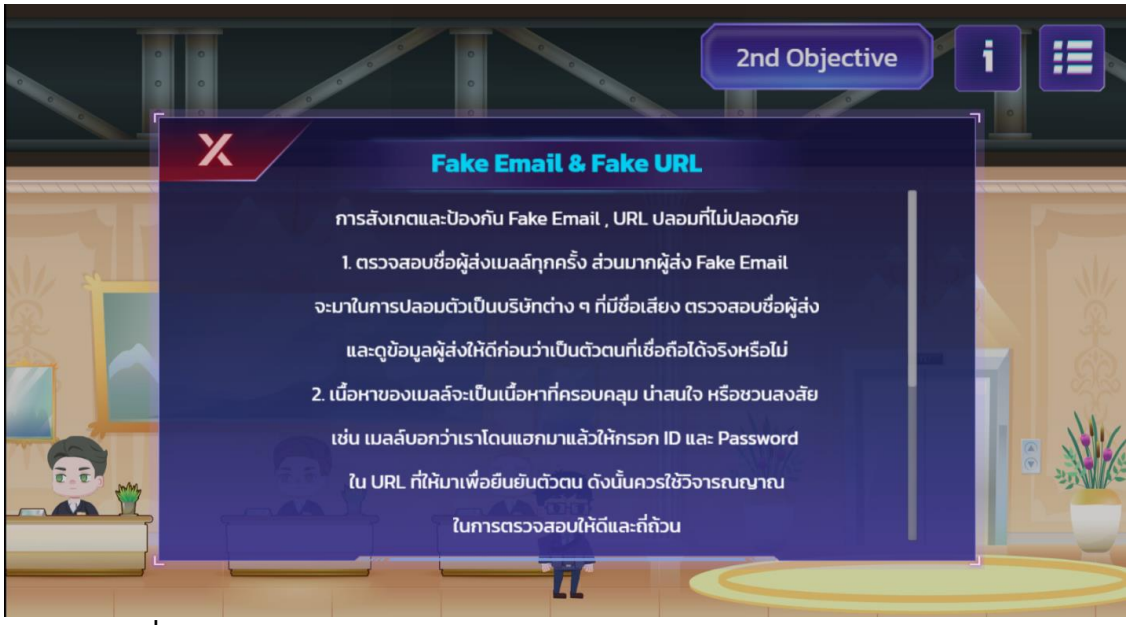
ภาพที่ ๓๐ Notification Knowledge Game Storyboard Design Chapter ๑

ภาพที่ ๓๑ คะแนนเมื่อผู้เล่นสามารถทำภารกิจได้สำเร็จ

ด่าน ๒ (นิทรรศการ ปารีส)

ดำเนินการออกแบบด่าน ๒ (ปารีส) ลักษณะเป็นอาคารนิทรรศการ ที่พื้นที่เล่น ๒ โดยชั้นที่ ๑ จะเป็นห้องโถงลงทะเบียน ส่วนชั้นที่ ๒ จะเป็นห้อง Monitor Control

ภาพที่ ๓๒ Game Storyboard Design Chapter ๒

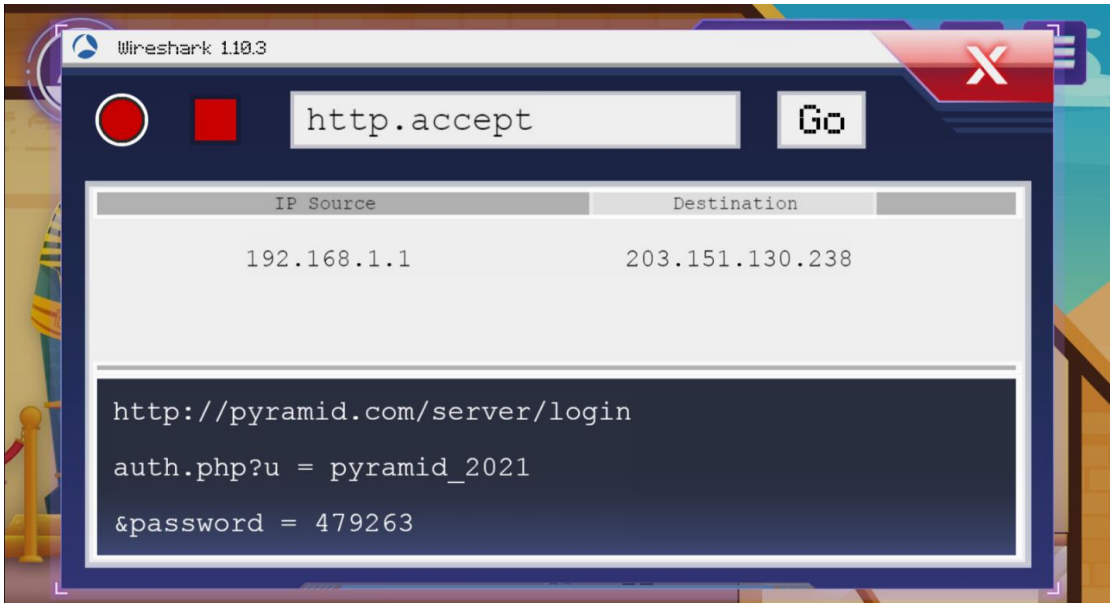


ภาพที่ ๓๓ Notification Knowledge Game Storyboard Design Chapter ๒

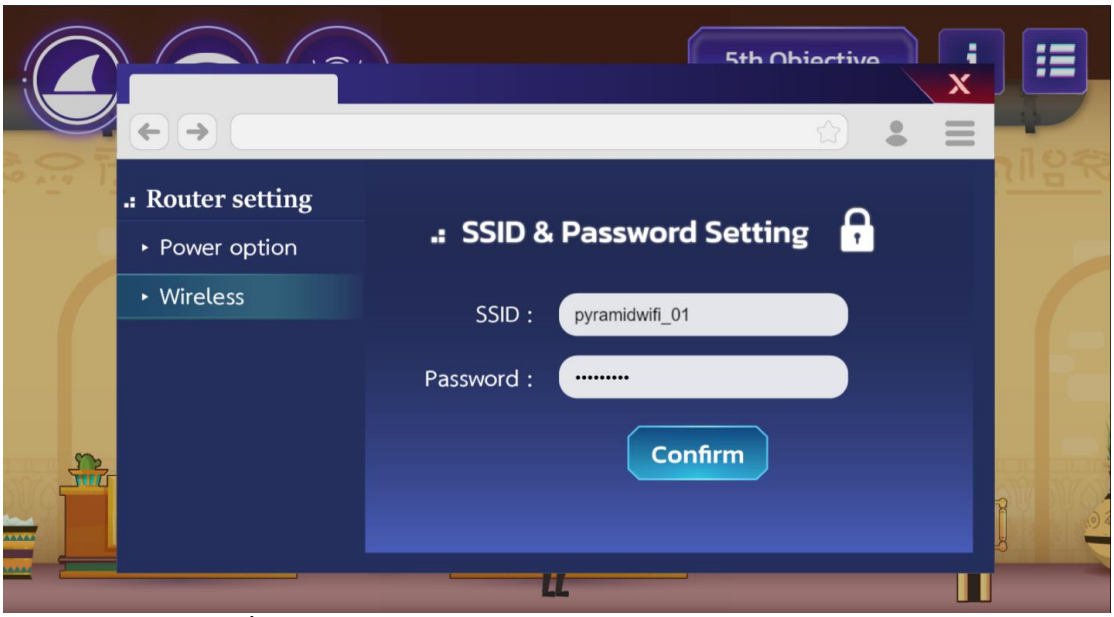
ด่าน ๓ ประเทศอียิปต์

หลอกเอาข้อมูลสำคัญภายในพีระมิดโดยการปลอมตัวเป็นนักท่องเที่ยวลักษณะของด่านจะมี ๒ ชั้น โดยชั้นล่างจะมีระบบควบคุมอยู่

ภาพที่ ๓๔ Game Storyboard Design Chapter ๓



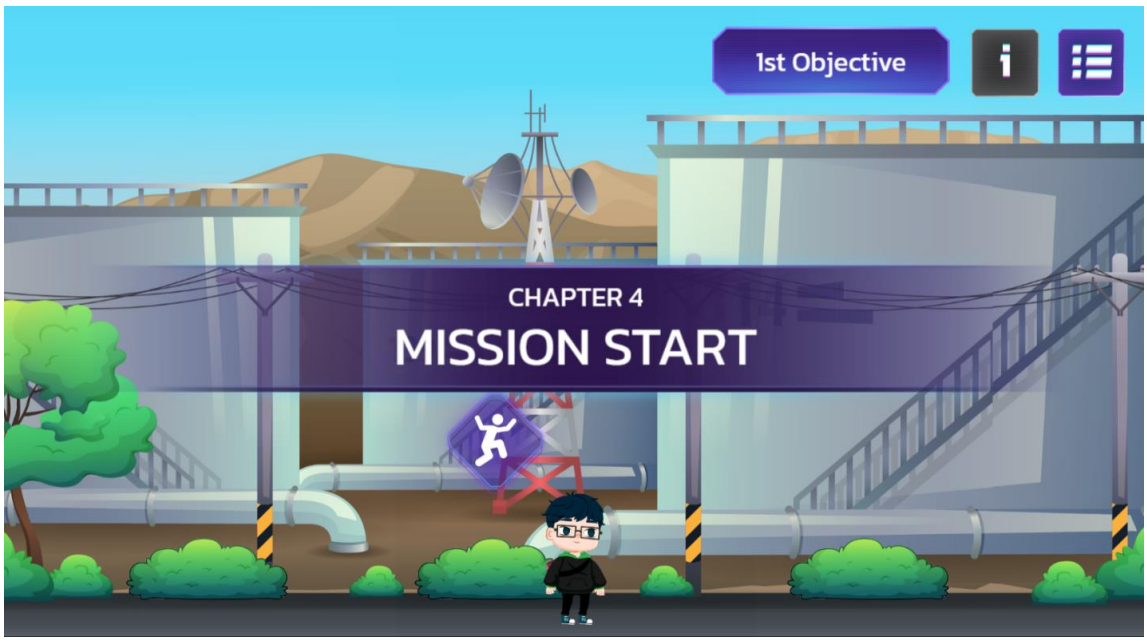
ภาพที่ ๓๕ Action in Game Storyboard Design Chapter ๓



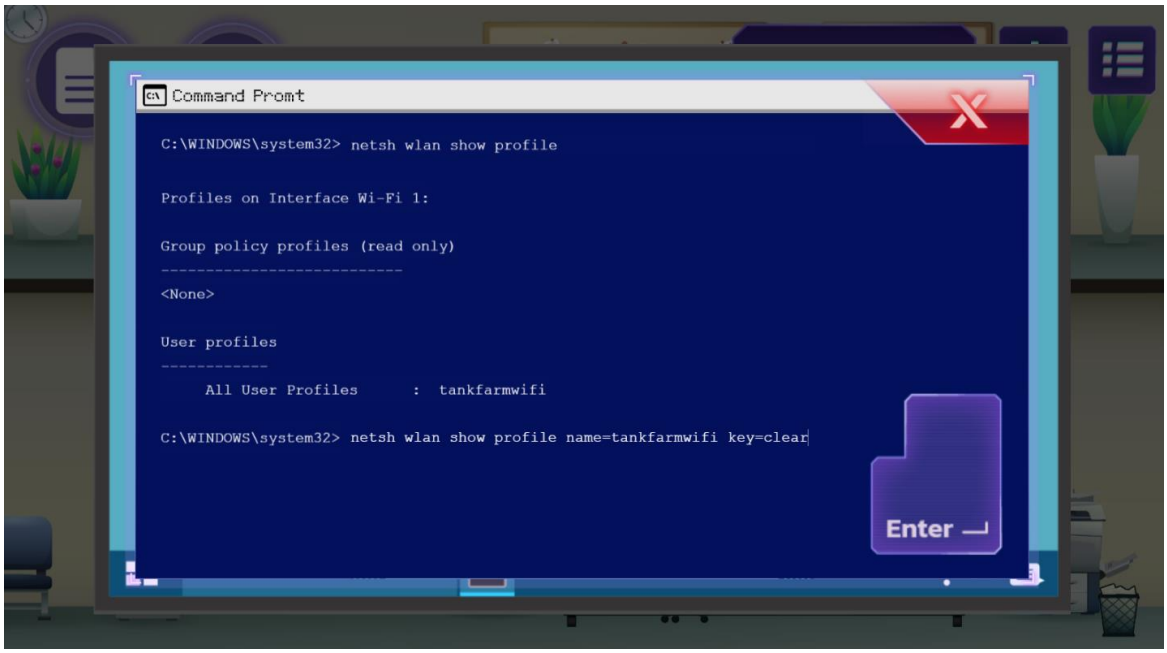
ภาพที่ ๓๖ Action in Game Storyboard Design Chapter ๓

ด่าน ๔ ประเทศอิหร่าน

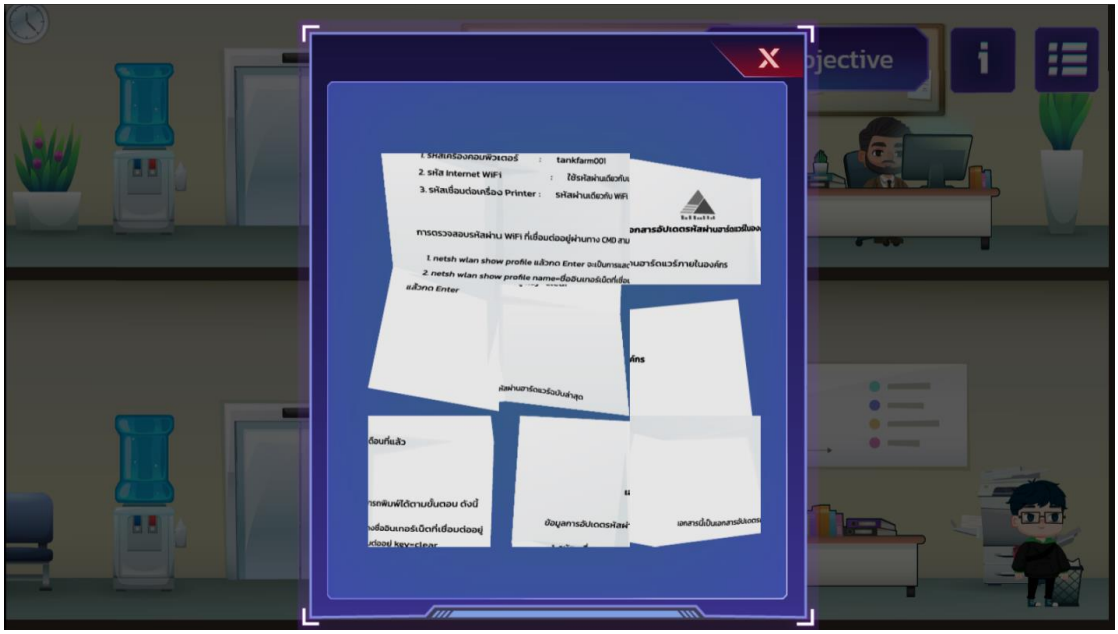
เข้าไปเจาะระบบ คลังน้ำมัน (ลักษณะเป็นห้องควบคุมแหล่งผลิตน้ำมัน) มีพื้นที่ทั้งหมดเป็นโรงงานควบคุมและ ส่งออกน้ำมัน มี ๑ ตึก ตึกมี ๓ ชั้น สภาพแวดล้อมภายนอกเป็นบรรยากาศโรงงาน



ภาพที่ ๓๗ Game Storyboard Design Chapter ๔



ภาพที่ ๓๘ Action in Game Storyboard Design Chapter ๔



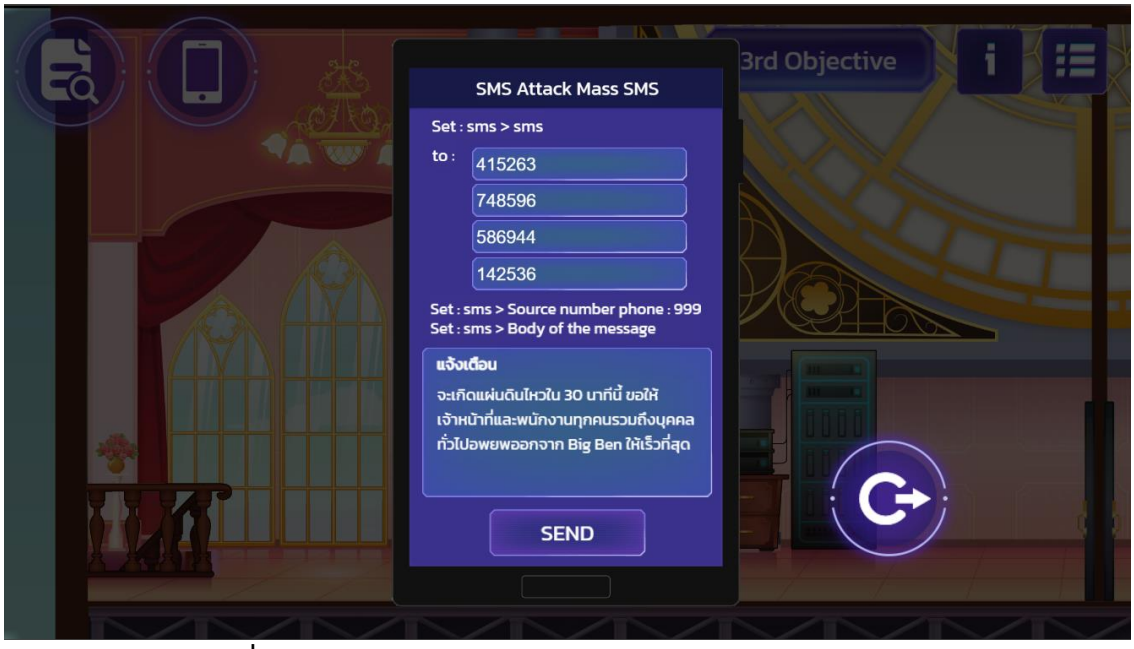
ภาพที่ ๓๙ Mini game Design Chapter ๔

ด่าน ๕ ประเทศอังกฤษ

อังกฤษ เข้าไปเจาะระบบเพื่อไปป่วน หอนาฬิกาบิกเบน (ห้องควบคุม ระบบของนาฬิกา) มีพื้นที่ ๔ ชั้น คลายตึกสำนักงานทั่วไป การตกแต่งเปนแบบbig ben ยุคโรแมนติค

ภาพที่ ๔๐ Game Storyboard Design Chapter ๕

ภาพที่ ๔๑ Notification Knowledge Game Storyboard Design Chapter ๕



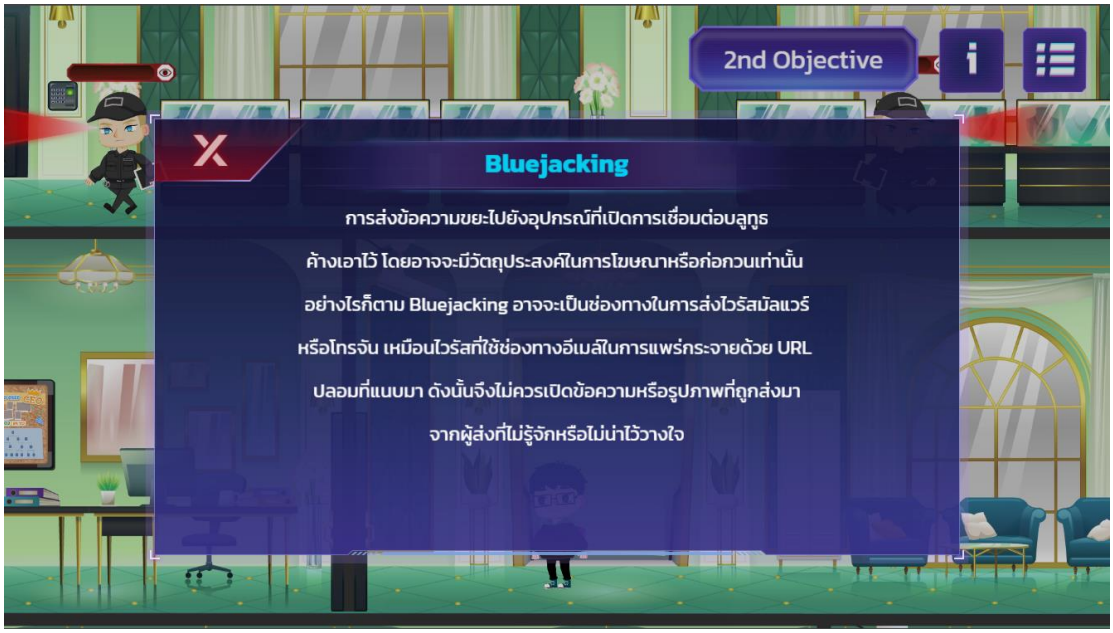
ภาพที่ ๔๒ Action in Game Storyboard Design Chapter ๕

ภาพที่ ๔๓ Action in Game Storyboard Design Chapter ๕

ด่าน ๖ ประเทศรัสเซีย

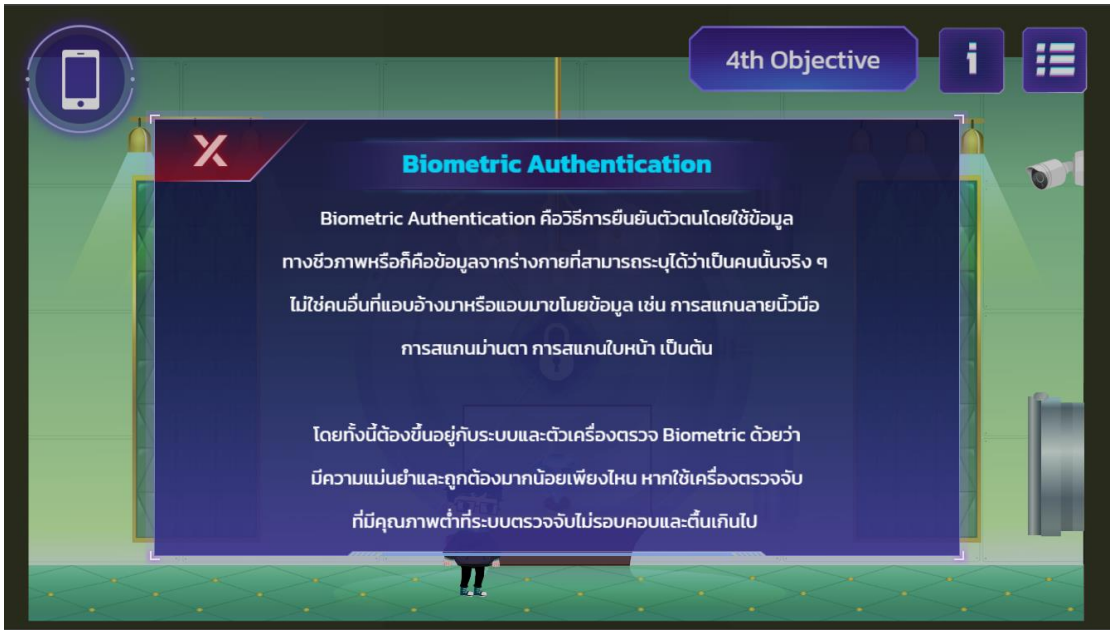
ตึกเก็บเพชรที่รัสเซีย ลักษณะด่านจะเป็นตึกแสดงนิทรรศกาล มีทั้งหมด ๓ ชั้นและมีลานจอดรถอยู่นอกตึก

ภาพที่ ๔๔ Game Storyboard Design Chapter ๖



ภาพที่ ๔๕ Notification Knowledge Game Storyboard Design Chapter ๖

ภาพที่ ๔๖ Action in Game Storyboard Design Chapter ๖

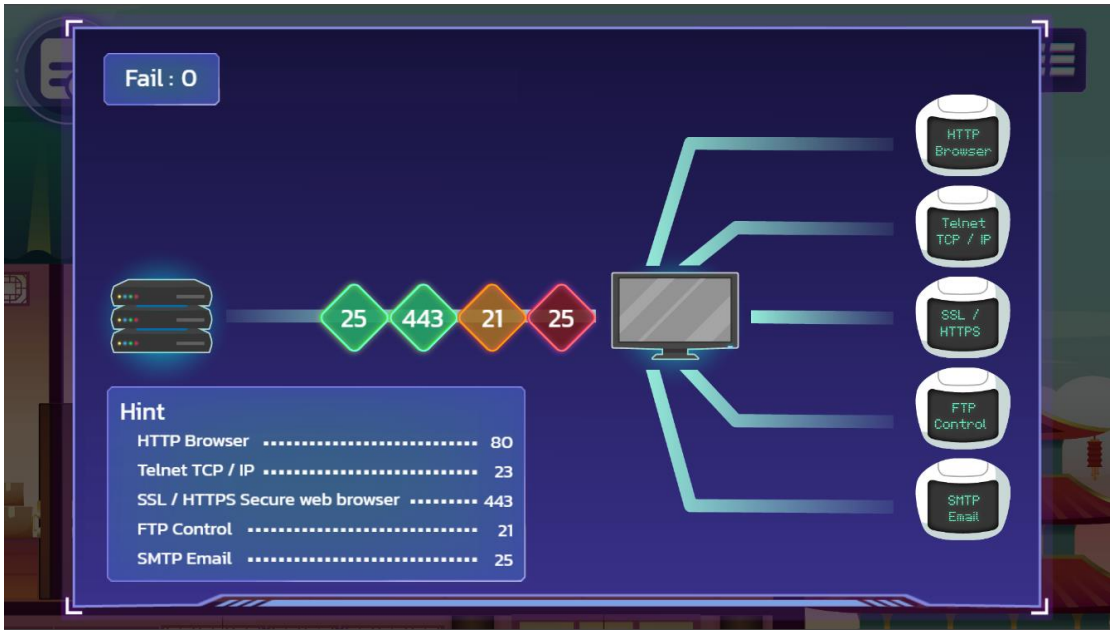


ภาพที่ ๔๗ Notification Knowledge Game Storyboard Design Chapter ๖

ด่าน ๗ ประเทศจีน

ภัตตาคารอาหารที่ใชพนักงานเสิรฟอาหารเปนหุนยนตที่ประเทศจีนผูเลนตองทำการปนปวนระบบควบคุมหุนยนตเสิรฟอาหาร ตึกภัตตาคารอาหาร มีทั้งหมด ๓ ชั้น และตึกขาง ๆ เปนหองควบคุมหุนยนตและโกดังเก็บหุนยนต มีทั้งหมด ๒ ชั้น

ภาพที่ ๔๘ Game Storyboard Design Chapter ๗



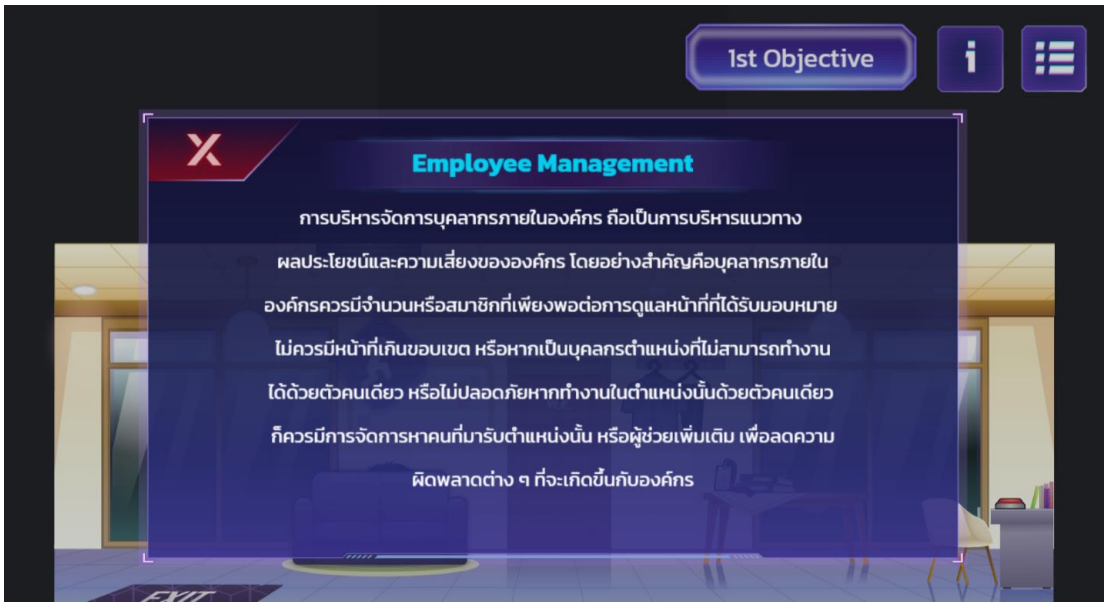
ภาพที่ ๔๙ Action in Game Storyboard Design Chapter ๗

ภาพที่ ๕๐ Action in Game Storyboard Design Chapter ๗

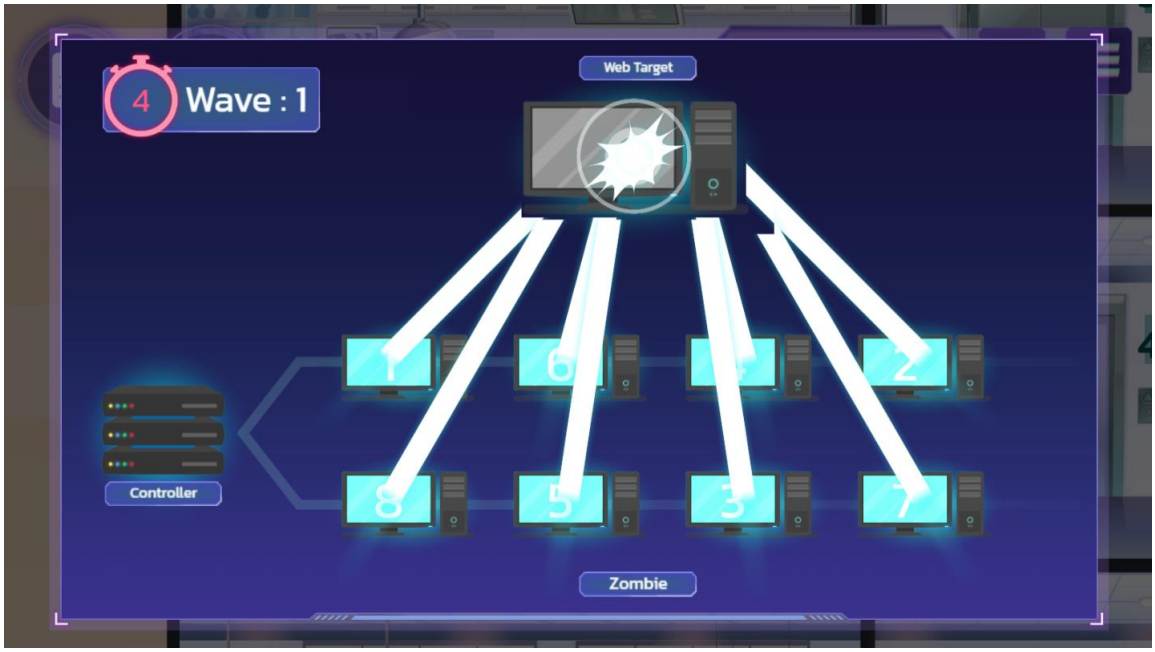
ด่าน ๘ ประเทศสหรัฐอเมริกา

ภารกิจสุดทายคือการเจาะระบบสถานีกระสวยอวกาศปลอมแปลงเปนนักบินของทางสถานี เพื่อที่จะไปดาวอังคารแลวนำธงขององคกรไปปกแทนธงของสหรัฐอเมริกา

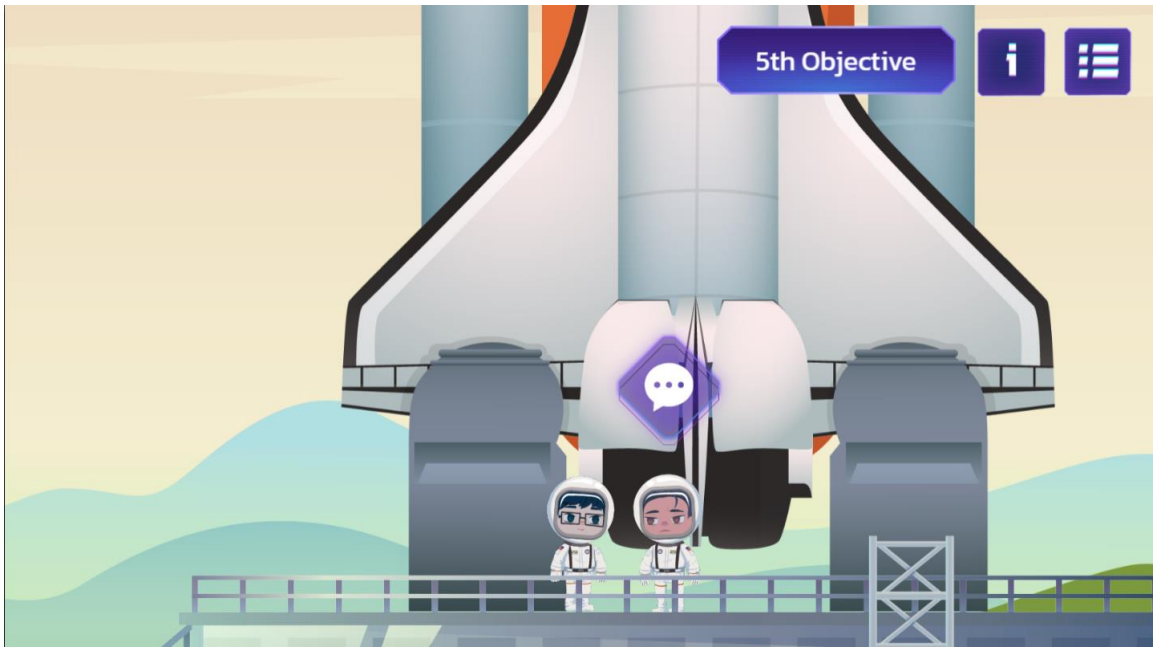
ภาพที่ ๕๑ Game Storyboard Design Chapter ๘



ภาพที่ ๕๒ Notification Knowledge Game Storyboard Design Chapter ๘



ภาพที่ ๕๓ Mini game Design Chapter ๘



ภาพที่ ๕๔ Action in Game Storyboard Design Chapter ๘

๔.๒ รายงานผลการจัดกิจกรรมสัมมนาแนะนำระบบ และเผยแพร่ระบบให้กับสาธารณะเริ่มต้นที่หน่วยงานการศึกษา

โครงการระบบออนไลน์เพื่อพัฒนาผู้เชี่ยวชาญด้านความปลอดภัยไซเบอร์ได้ดำเนินงานบรรลุตามวัตถุประสงค์ของโครงการ เนื่องจากการจัดกิจกรรมสัมนาได้รับผลตอบรับที่ดี โดยมีผู้เข้าร่วมหลายภาคส่วน ไม่ว่าจะเป็นกลุ่มนักเรียนนึกศึกษา กลุ่มหน่วยงานราชการ/รัฐวิสาหกิจ กลุ่มหน่วยงานเอกชน และกลุ่มประชาชนทั่วไป อีกทั้งยังได้รับความร่วมมือจากสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ ที่ได้มาช่วยถ่ายทอดความรู้ทางด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่ผู้เข้าร่วมกิจกรรมสัมนา ในส่วนของเนื้อหาที่สัมนามีความสอดสอดคล้องกับภาคปฏิบัติจริงในชีวิตประจำวัน ซึ่งจำนวนผู้เข้าร่วมกิจกรรมสัมมนาแนะนำระบบในครั้งนี้เกินจำนวนเป้าหมายที่ทางโครงการได้ตั้งเป้าไว้

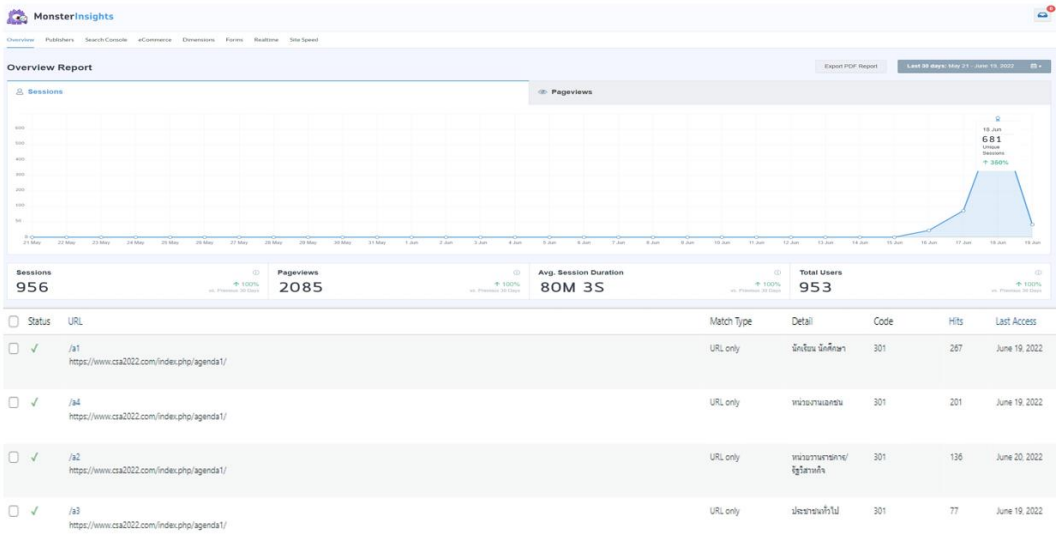
การจัดกิจกรรมการสัมนาได้เผยแพร่การถ่ายทอดสดใน วันที่ ๑๘ มิถุนายน ๒๕๖๕ เข้าชมผ่านช่องทาง https://www.learncybersec.org/csa2022 โดยทางผู้จัดทำได้แบ่งกลุ่มออกเป็น ๔ กลุ่มได้แก่ กลุ่มนักเรียน/นักศึกษา , หน่วยงานราชการ/รัฐวิสาหกิจ , หน่วยงานเอกชน และประชาชนทั่วไป ในการเข้าชมการถ่ายทอดงานสัมนา CSA๒๐๒๒ มีผู้เข้าร่วมงานในลักษณะ Virtual Conference เป็นจำนวนทั้งสิ้น ๖๘๑ คน โดยสรุปจำนวนผู้เข้าร่วมงานสัมนาได้ ดังนี้

กลุ่มที่ ๑ กลุ่มนักเรียนนักศึกษา จำนวน ๒๖๗ คน (คิดเป็น ๓๙.๒๑%)

กลุ่มที่ ๒ กลุ่มหน่วยงานราชการ/รัฐวิสาหกิจ จำนวน ๑๓๖ คน (คิดเป็น ๑๙.๙๗%)

กลุ่มที่ ๓ กลุ่มหน่วยงานเอกชน จำนวน ๒๐๑ คน (คิดเป็น ๒๙.๕๑%)

กลุ่มที่ ๔ กลุ่มประชาชนทั่วไป จำนวน ๗๗ คน (คิดเป็น ๑๑.๓๑%)

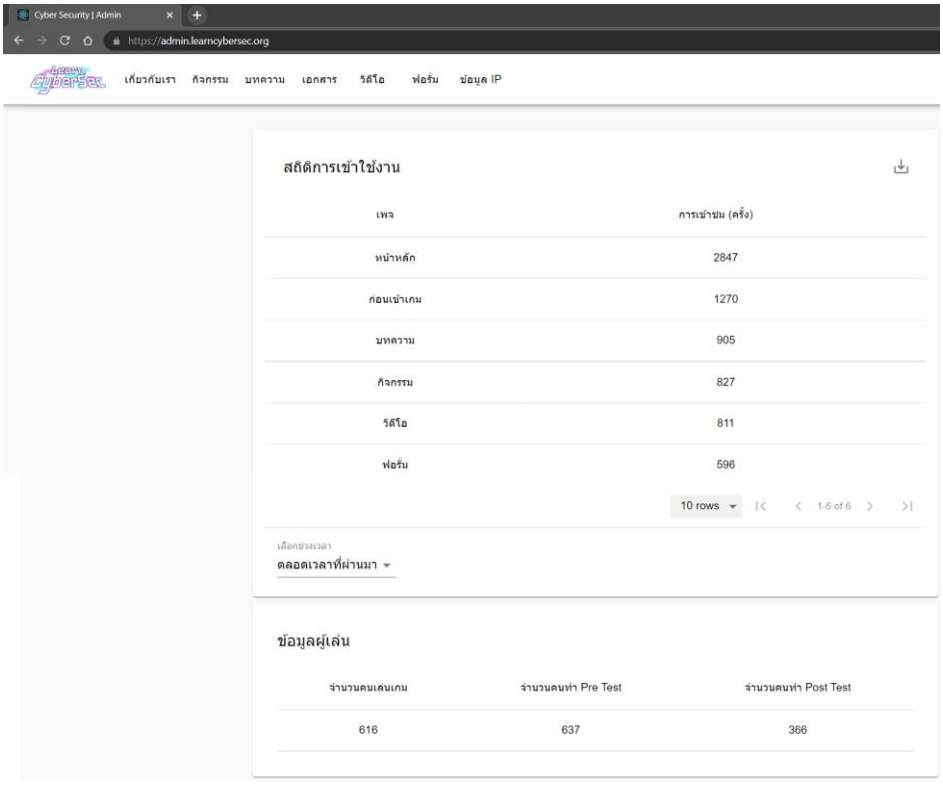


ภาพที่ ๕๕ จำนวนผู้เข้าร่วมกิจกรรมสัมมนาแนะนำระบบ

๔.๒ รายงานผลการใช้งานระบบและการประเมินผล

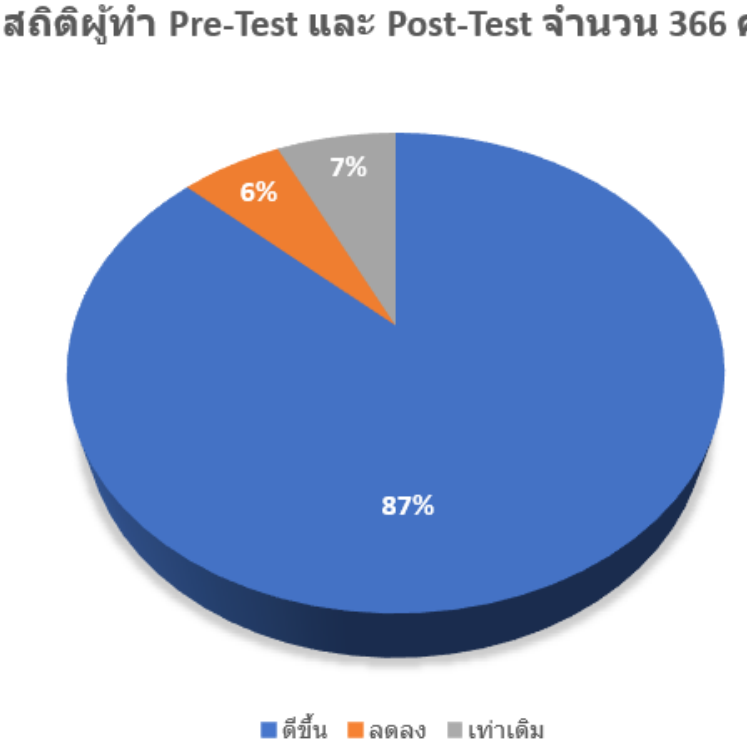
โครงการระบบออนไลน์เพื่อพัฒนาผู้เชี่ยวชาญด้านความปลอดภัยไซเบอร์ ได้จัดจัดสร้างระบบต้นแบบ Online Game-Based Cybersecurity Learning Platform (Basic-Beginner) ซึ่งเป็นช่องทางการเรียนรู้ การเพิ่มทักษะ ให้กับเยาวชนบุคคลที่มีความสนใจ ในเรื่องความตระหนักรู้ถึงภัยคุกคามและอาชญากรรมไซเบอร์และการรักษาความมั่นคงปลอดภัยไซเบอร์โดยสถิติจำนวนผู้เข้าใช้งานระบบของ https://www.learncybersec.org/ จากระบบผู้ดูแลระบบ (Back-End) โดยมีรายละเอียดดังนี้

๑. จำนวนผู้เข้าชมหน้าหลัก จำนวน ๒,๘๔๗ ครั้ง
๒. จำนวนผู้เข้าชมหน้าก่อนเข้าเกม จำนวน ๑,๒๗๐ ครั้ง
๓. จำนวนผู้เข้าชมหน้าบทความ จำนวน ๙๐๕ ครั้ง
๔. จำนวนผู้เข้าชมหน้ากิจกรรม จำนวน ๘๒๗ ครั้ง
๕. จำนวนผู้เข้าชมหน้าวีดีโอ จำนวน ๘๑๑ ครั้ง
๖. จำนวนผู้เข้าชมหน้าฟอรั่ม จำนวน ๕๙๖ ครั้ง



ภาพที่ ๕๖ สถิติจำนวนผู้เข้าใช้งานระบบ

จากภาพที่ ๒๖ สถิติจำนวนผู้เข้าใช้งานระบบแสดงให้เห็นถึงข้อมูลผู้เข้าเล่มเกม การประเมินผลข้อมูลผู้เข้าเล่นเกม มีจำนวนผู้เข้าทำข้อสอบก่อนเข้าเล่นเกม (Pre-Test) จำนวน ๖๓๗ คน ในจำนวน ๖๓๗ คนมีผู้เข้าทำข้อสอบหลังเข้าเล่นเกม (Post-Test) จำนวน ๓๖๖ คน จากการประเมินสถิติจากระบบหลังบ้าน (Back-End) ในจำนวนผู้ทำข้อสอบหลังเข้าเล่นเกม (Post-Test) จำนวน ๓๖๖ คนนั้นพบว่ามีจำนวน ๓๑๘ คน หรือ ๘๖.๘๙% มีเกณฑ์คะแนนที่ดีขึ้น มีผู้ที่ได้คะแนนลดลงจำนวน ๒๒ คน คิดเป็น ๖.๐๑% และมีผู้ที่ได้คะแนนเท่าเดิมจำนวน ๒๖ คน คิดเป็น ๗.๑๐% ดังภาพที่ ๒๗



ภาพที่ ๕๗ สถิติผู้ทำ Pre-Test และ Post-Test จำนวน ๓๖๖ คน

๔.๓ รายงานผลการประชาสัมพันธ์ผ่านทางสื่อต่างๆ และกิจกรรมการเผยแพร่สู่สาธารณะผ่านสื่อออนไลน์

โครงการระบบออนไลน์เพื่อพัฒนาผู้เชี่ยวชาญด้านความปลอดภัยไซเบอร์ ได้มีการวางแผนเนื้อหาออกแบบสื่อสำหรับการเผยแพร่สู่สาธารณะ โดยได้เผยแพร่ช่องทางประชาสัมพันธ์บนช่องทางประชาสัมพันธ์ต่างๆ ได้แก่ บนเว็บไซต์ของโครงการ , เฟซบุ๊ค และการแชร์ต่อไปบนเฟซบุ๊คเพจของหน่วยงานต่างๆ ทั้งภาครัฐ เอกชน และประชาชนทั่วไป ที่เกี่ยวข้อง ซึ่งเป็นไปตามวัตถุประสงค์ของโครงการ โดยมีรายละเอียดดังนี้

ภาพที่ ๕๘ โปสเตอร์ประชาสัมพันธ์ผ่านทางสื่อต่างๆ และกิจกรรมการเผยแพร่สู่สาธารณะผ่านสื่อออนไลน์

ภาพที่ ๕๙ การเผยแพร่บน เฟซบุ๊ค ของบริษัท เทิร์นคีย์ คอมมูนิเคชั่น เซอร์วิส จำกัด (มหาชน)

ภาพที่ ๖๐ การเผยแพร่บน เฟซบุ๊ค ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และโครงการThailand National Cyber Academe by NCSA

ภาพที่ ๖๑ การเผยแพร่บน เฟซบุ๊ค ของศูนย์ประชาสัมพันธ์ หน่วยข่าวกรองทางทหารกองพลทหารราบที่ ๑๕

ภาพที่ ๖๒ การเผยแพร่บน เฟซบุ๊ค ของภาควิชาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

ภาพที่ ๖๓ การเผยแพร่บน เฟซบุ๊คของ คณะวิศวกรรมศาสตร์ หลักสูตรนานาชาติ มหาวิทยาลัยศรีนครินทร์ทรวิโรฒ

ภาพที่ ๖๔ การเผยแพร่บน เฟซบุ๊คของภาควิชาการคอมพิวเตอร์และเทคโนโลยีสารสนเทศ มหาวิทยาลัยนเรศวร

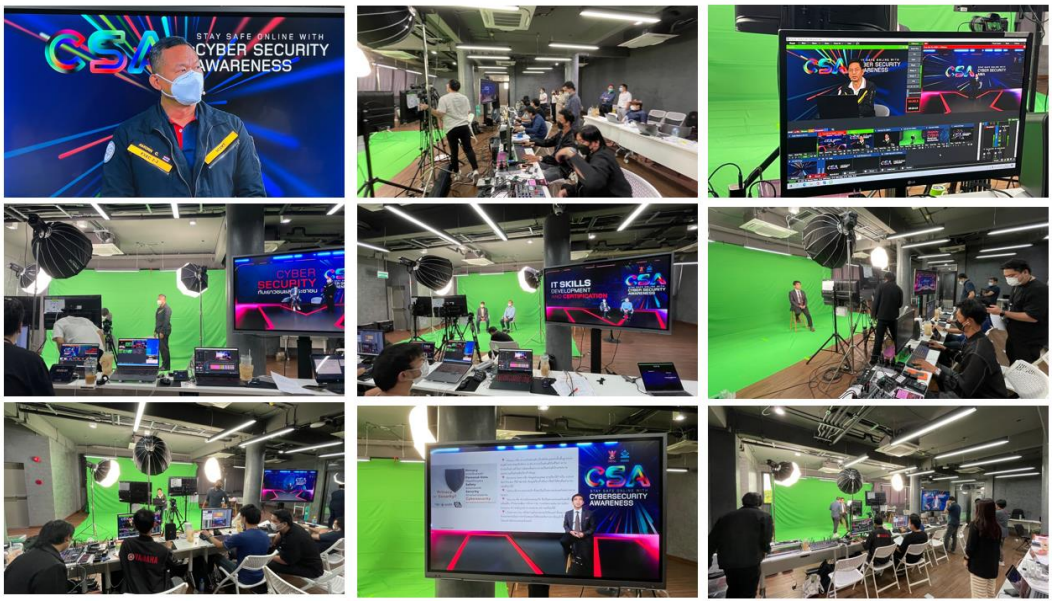
ภาพที่ ๖๕ การเผยแพร่บน เฟซบุ๊คของสาขาวิชาช่างอิเล็กทรอนิกส์ สถาบันเทคโนโลยีจิตรลดา

ภาพที่ ๖๖ การเผยแพร่บน เฟซบุ๊คของ CompTIA Thailand

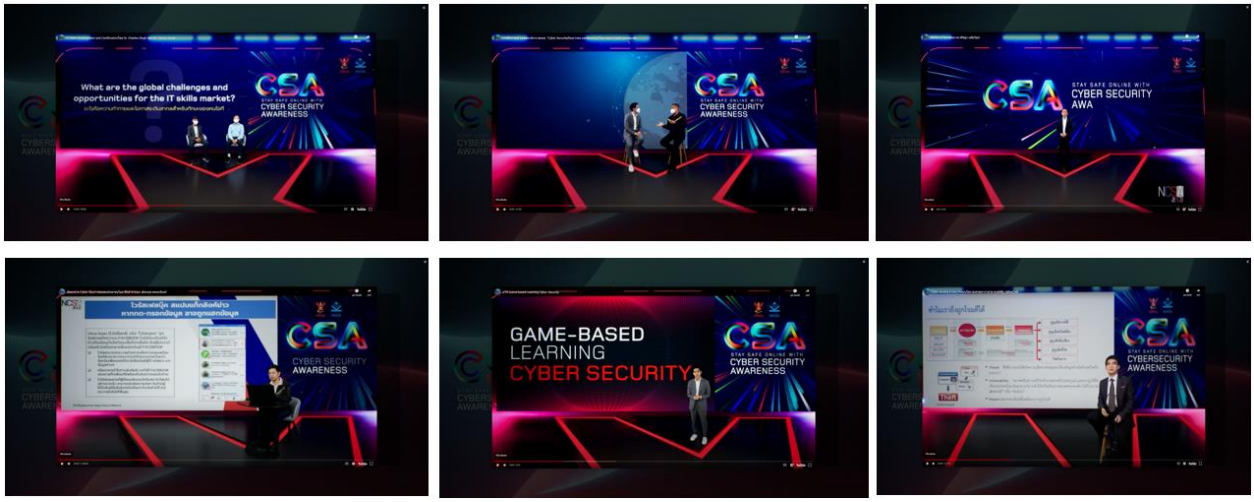
ภาพที่ ๖๗ การเผยแพร่บน เฟซบุ๊คของพงษ์แคสต์

ภาพที่ ๖๘ การเผยแพร่บน เฟซบุ๊คของ IT-Southeast

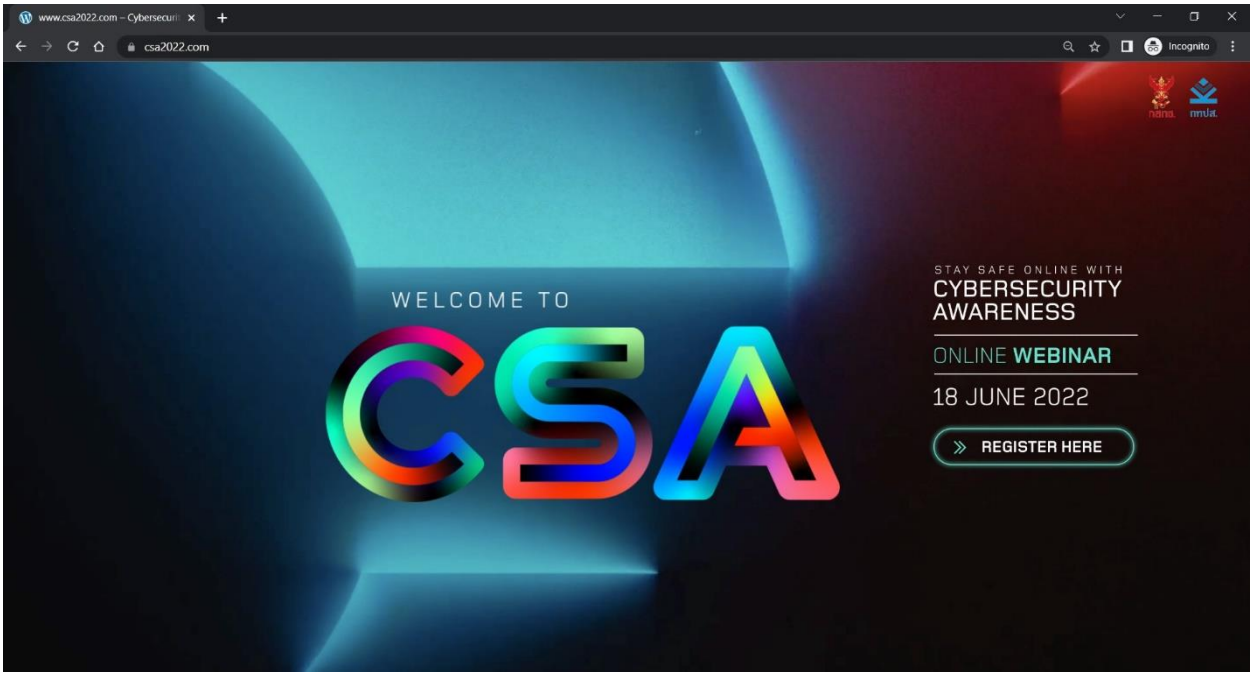
การถ่ายทอดสดทางโครงการได้จัดทำในรูปแบบ Virtual System โดยมีการนำเสนอในรูปแบบ ๓D Perspective ซึ่งจะออกมาเป็นภาพที่ให้ความรู้สึกเป็น ๓ มิติ มีลักษณะของความเหมือนที่สมจริงมากที่สุดทั้งสีสันบรรยากาศและทัศนียภาพ Graphic / Motion Graphic ให้ผู้ที่เข้าร่วมงานสัมนารู้สึกถึงการมีส่วนร่วมมีความน่าตื่นตาตื่นใจ เสมือนเข้ามาอยู่ในงานสัมนาครั้งนี้ด้วยตนเอง



ภาพที่ ๖๙ Live Streaming Production



ภาพที่ ๗๐ ๓D Perspective



ภาพที่ ๗๑ หน้าแรกก่อนเข้าลงทะเบียน

ภาพที่ ๗๒ รายละเอียดการเข้าลงทะเบียน

ภาพที่ ๗๓ รายละเอียดหัวข้อการสัมมนา

๔.๔ รายงานผลการดำเนินงานฉบับย่อสำหรับลงตีพิมพ์ในวารสารสำนักงาน กสทช.

บทคัดย่อ

ปัจจุบันภัยคุกคามทางไซเบอร์มีจำนวนที่เพิ่มสูงขึ้น และทวีความรุนแรงขึ้นตามลำดับ ส่งผลกระทบ และสร้างความเสียหายทั้งต่อระดับปัจเจกชน และระดับประเทศ ซึ่งนานาประเทศต่างให้ความสำคัญในการดำเนินงานเพื่อรับมือกับปัญหาภัยคุกคามดังกล่าวอย่างมาก ดังนั้นการตระหนักถึงเรื่องความมั่นคงปลอดภัยไซเบอร์นั้นจะช่วยสร้างความเข้าใจพื้นฐานเกี่ยวกับภัยคุกคาม และลดความเสี่ยงในโลกไซเบอร์ โดยการส่งเสริมการเรียนรู้ ในด้านนี้นอกจากการศึกษาผ่านทาง การเรียนในห้องเรียน หนังสือ สื่อการเรียนการสอนต่างนั้น อาจไม่เพียงพอในปัจจุบัน ที่กระบวนการศึกษาได้มีการพัฒนาสู่โลกดิจิทัล ทำให้มีความจำเป็นที่จะต้องมีการพัฒนาระบบการเรียนรู้ ในรูปแบบ Online Game-Based Cyber Security Learning ที่สามารถนำเรื่องของ Cyber Security ที่เข้าใจได้ยากนำมาจำลองเป็นเหตุการณ์ (Scenario) ในเรื่องต่างๆ ทำให้ผู้เรียนเกิดการเรียนรู้ไปกับการเล่นเกม โดยมีกลุ่มเป้าหมายในระดับเริ่มต้น พื้นฐานที่ นักเรียน นักศึกษา ระชาชน และผู้สนใจในเรื่องการรักษาความมั่นคงปลอดภัยไซเบอร์ สามารถเข้าใช้ระบบเพื่อเรียนรู้ผ่านการเล่นเกม อันจะเป็นเครื่องมือหนึ่งที่จะช่วยในการพัฒนาบุคคลากรด้านไซเบอร์ให้เกิดความ ตระหนัก เกิดการเรียนรู้ และเป็นจุดสนใจที่จะสามารถพัฒนาต่อยอด สู่การศึกษาในระดับเชี่ยวชาญในด้านนี้ต่อไปในอนาคต

คำสำคัญ: การรักษาความมั่นคงปลอดภัยทางไซเบอร์, การตระหนักเรื่องความมั่นคงปลอดภัยไซเบอร์,การเรียนรู้ผ่านเกมส์,การพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์

๑.๑ Abstract

The number of cyber threats is growing these days. and intensifying accordingly, affecting and causing damage to both the individual and national levels, with many countries focusing heavily on operations to combat such threats. As a result, cybersecurity awareness will help build a basic understanding of threats. and reduce cyber risks by promoting learning In this area, besides studying through Learning in the classroom, books, teaching materials are different. may not be enough at present that the educational process has evolved into the digital world Makes it necessary to develop a learning system in the form of Online Game-Based Cyber Security Learning that can bring the story of Cyber Security that is difficult to understand and simulate it as a scenario (Scenario) in a variety of contexts. Games should be used to teach students. Young people, students, the general public, and anyone with an interest in cybersecurity are its target audiences at the entry-level, fundamental level. can use the system to play games and learn. This will be one of the tools used to train and educate cyber workers. It is a concentration that can be strengthened to pursue further studies at the level of expertise in this field.

Keywords: Cyber Security Learning, Cybersecurity Awareness, Online Game-Based Cyber Security Learning, Cybersecurity Personnel Development.

๑. บทนำ

ปัจจุบันภัยคุกคามทางไซเบอร์มีจำนวนที่เพิ่มสูงขึ้น และทวีความรุนแรงขึ้นตามลำดับ ส่งผลกระทบ และสร้างความเสียหายทั้งต่อระดับปัจเจกชน และระดับประเทศ ในปี พ.ศ. ๒๕๖๔ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (Thailand Computer Emergency Response Team) ได้สรุปสถิติ ภัยคุกคามทางไซเบอร์ ดังตารางที่ ๑

สถิติภัยคุกคาม ประจำปี พ.ศ ๒๕๖๔

ประเภทภัยคุกคาม	รวม	สัดส่วน
Abusive Content	๑๔	๐.๖๘%
Availability	๕	๐.๒๔%
Fraud	๒๑๒	๑๐.๒๕%
Information Gathering	๒๔๘	๑๑.๙๙%
Information Security	๓๐	๑.๔๕%
Intrusion Attempts	๒๒๔	๑๐.๘๓%
Intrusions	๑๘๓	๘.๘๔%
Malicious Code	๔๗๙	๒๓.๑๕%
Vulnerability	๖๗๔	๓๒.๕๘%
Other	๐	๐.๐๐%
รวม	๒๐๖๙	๑๐๐.๐๐%

ตารางที่ ๑ สถิติภัยคุกคามทางไซเบอร์ในปี พ.ศ. ๒๕๖๔ โดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย

ซึ่งนานาประเทศต่างให้ความสำคัญในการดำเนินงานเพื่อรับมือกับปัญหาภัยคุกคามดังกล่าวอย่างมาก ดังนั้นการตระหนักถึงความปลอดภัยของระบบไซเบอร์นั้นจะช่วยสร้างความเข้าใจพื้นฐานเกี่ยวกับภัยคุกคาม และความเสี่ยงในโลกไซเบอร์ การทำกิจกรรมต่าง ๆ ในโลกไซเบอร์และการเผชิญกับความเสี่ยงต่าง ๆ ซึ่งประเทศไทยควรที่จะส่งเสริมการเรียนรู้ เพื่อเพิ่มความตระหนักถึงภัยในโลกไซเบอร์ อาทิ นักเรียน นักศึกษา หรือ ผู้สนใจในเรื่องการรักษาความปลอดภัยไซเบอร์ ควรได้รับการพัฒนา ความรู้ ความเข้าใจ เกี่ยวกับเรื่องดังกล่าวอย่างต่อเนื่อง เพื่อที่จะสามารถรับมือกับภัยคุกคามที่เกี่ยวข้องกับไซเบอร์ที่มีพัฒนาการทางเทคโนโลยี และข้อมูลอยู่ตลอดเวลา

จากแนวคิดหลักการดังกล่าวนั้นมีความเชื่อมโยงและสอดคล้องกับแผนแม่บทและแผนยุทธศาสตร์ชาติ ดังจะเห็นได้ว่าจากการที่ สำนักงาน กสทช. ได้มีการส่งเสริมและสนับสนุนการพัฒนาทรัพยากรสื่อสาร การวิจัย และพัฒนาด้าน กิจการกระจายเสียง กิจการโทรทัศน์ กิจการโทรคมนาคมและเทคโนโลยี สารสนเทศกรอบทิศทางในการวิจัยและพัฒนาเชิงนวัตกรรมเทคโนโลยีสารสนเทศและโทรคมนาคมด้านอุตสาหกรรม ๔.๐ (Industry ๔.๐) เพื่อรองรับกับสภาพแวดล้อมระบบนิเวศดิจิทัลที่เปลี่ยนแปลงอย่างรวดเร็วและเชื่อมโยงกันในทุกๆ ด้านโดยมีเป้าหมายตามแผนแม่บทกิจการโทรคมนาคมกับการพัฒนาที่เชื่อมโยงกับยุทธศาสตร์ชาติ ๒๐ ปีตลอดจนนโยบายและ

แผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมทำให้มีความเชื่อมโยงที่เกี่ยวข้องกับกระทรวงและหน่วยงานต่างๆซึ่งมีแผนงานและนโยบายในเรื่องของความต้องการในการที่จะพัฒนาเพิ่มพูนทักษะของบุคคลากรในด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศให้มีเพิ่มมากยิ่งขึ้นไป

๒.๑ สำนักงานสภาความมั่นคงแห่งชาติ สำนักนายกรัฐมนตรี

ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. ๒๕๖๐ – ๒๕๖๔

“๒.๑.๓ ความพร้อมทางด้านบุคลากร ความพร้อมทางด้านบุคลากรถือเป็นสิ่งที่สำคัญอย่างยิ่ง ทั้งในด้านความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ทั้งระดับนโยบายและปฏิบัติ และด้านความรู้ความเชี่ยวชาญเฉพาะทางซึ่งจากการสำรวจ พบว่ากว่าร้อยละ ๕๐ หน่วยงานรัฐและเอกชนยังไม่ได้ให้ความสำคัญกับการจัดทำแผนพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ และ ร้อยละ ๗๙ ของหน่วยงานจะมีข้อจำกัดในการ สร้างแรงจูงใจให้บุคลากรเสริมศักยภาพให้กับตนเอง เช่น การสอบใบประกาศนียบัตรการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยเฉพาะใบประกาศนียบัตรที่ได้รับการยอมรับในระดับสากล ซึ่งประเทศไทยควรกำหนดทิศทางและให้ความสำคัญกับการส่งเสริมและสนับสนุนการพัฒนาบุคลากรที่มีความรู้ความเชี่ยวชาญในด้านความมั่นคงปลอดภัยไซเบอร์เพิ่มขึ้น เพื่อเตรียมการรับมือกับภัยคุกคาม ที่อาจเกิดขึ้นในรูปแบบต่าง ๆ ได้อย่างครอบคลุมและมีประสิทธิภาพยิ่งขึ้น”

“ประเด็นยุทธศาสตร์ที่ ๕ สร้างความตระหนักและส่งเสริมความร่วมมือ ภายในประเทศด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

เป้าหมาย

๑. ประชาชนทั่วไปทุกระดับทุกเพศและวัยที่เป็นผู้ใช้อินเทอร์เน็ต มีความตระหนักถึงภัยคุกคามทางไซเบอร์ และมีความรู้เรื่องการรักษาความปลอดภัยทางไซเบอร์

๒. รัฐ ภาคเอกชน และประชาสังคมร่วมมือกันในการรักษาความมั่นคงปลอดภัยไซเบอร์

๓. ช่องทาง/กลไกการสื่อสารแนวนโยบายสู่การปฏิบัติในภาคเอกชนและภาคประชาสังคม

ตัวชี้วัด

๑. การจัดทำคู่มือเผยแพร่ความรู้เกี่ยวกับด้านไซเบอร์และการประเมินผล

๒. จำนวนครั้งการประชาสัมพันธ์ผ่านสื่อประเภทต่าง ๆ /กลไกต่าง ๆ

๓. การจัดฝึกอบรมให้ความรู้แก่ประชาชนผู้ใช้อินเทอร์เน็ตและการประเมินผล”

๒.๒ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

นโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม

(พ.ศ. ๒๕๖๑ – ๒๕๘๐)

“๘) ภัยคุกคาม, ไซเบอร์

การจัดการกับภัยในรูปแบบใหม่ๆ รวมถึงภัยคุกคามจากสารสนเทศรูปแบบต่างๆ มีการพัฒนาและเปลี่ยนแปลงรูปแบบอย่างต่อเนื่องจึงต้องเตรียมความพร้อมเพื่อรับมือเพิ่มขีดความสามารถของบุคลากรในการรักษาความมั่นคงปลอดภัยและการพัฒนาทักษะความรู้เพื่อป้องกันตนเองและหน่วยงานลดความเสี่ยงจากการถูกโจมตีหรือภัยคุกคามและลดความท้าทายจากผลกระทบทอาจเกิดขึ้น”

“๓.๓ การกำหนดมาตรการการเฝ้าระวังและรับมือภัยคุกคามไซเบอร์เหมาะสมและสอดคล้องตามมาตรฐานสากลโดยเฉพาะการปกป้องโครงสร้างพื้นฐานที่มีความจำเป็นอย่างยิ่งยวด (Critical Infrastructure) เช่น โครงสร้างพื้นฐานทางไฟฟ้า โครงสร้างพื้นฐานทางการเงิน เพื่อให้มีความมั่นคงปลอดภัยเพียงพอ ต่อการค้าและการลงทุน การสร้างเครือข่ายแลกเปลี่ยนข้อมูลภัยคุกคามไซเบอร์ พร้อมกำหนดหน่วยงาน รับแจ้งเหตุ และสร้างกลไกการบังคับใช้กฎหมายที่มีประสิทธิภาพในการป้องกันปราบปรามการกระทำความผิด ไม่ให้มีผลต่อระบบความมั่นคงปลอดภัยดิจิทัล ทั้งนี้การส่งเสริมให้เกิดความตระหนักและเท่าทันภัยคุกคามทางไซเบอร์เป็นสิ่งสำคัญที่ต้องดำเนินการอย่างต่อเนื่อง”

๒.๓ กระทรวงกลาโหม

นโยบายเร่งด่วนของรัฐมนตรีว่าการกระทรวงกลาโหม ประจำปีงบประมาณ พ.ศ. ๒๕๖๒ (๑ ต.ค. ๖๑ - ๓๐ ก.ย. ๖๒)

“๒.๓ เสริมสร้างขีดความสามารถในการปฏิบัติการด้านไซเบอร์ทั้งเชิงรุกและเชิงรับอย่างต่อเนื่อง เพื่อรองรับภัยคุกคามด้านไซเบอร์ที่มีผลกระทบต่อความมั่นคงของชาติ ตลอดจนให้การสนับสนุนการดำเนินการด้านไซเบอร์ระดับประเทศ รวมทั้งบูรณาการความร่วมมือกับทุกภาคส่วนทั้งภายในและต่างประเทศที่เกี่ยวข้องในการพัฒนาขีดความสามารถด้านกิจการอวกาศของกระทรวงกลาโหมเพื่อรองรับภัยคุกคามด้านอวกาศที่มีผลกระทบต่อความมั่นคงของชาติโดยเฉพาะการพัฒนา ด้านองค์ความรู้ และขีดความสามารถของกำลังพลจากระดับผู้ใช้งาน (User) สู่การเป็นผู้ควบคุมและบริหารสถานีดาวเทียม (Operator) ซึ่งจะนำไปสู่การพึ่งพาตนเองได้ในอนาคต”

ด้วยเหตุนี้จึงเล็งเห็นความสำคัญในเรื่องภัยคุกคามทางไซเบอร์การเข้าถึงเรื่องของความปลอดภัยของระบบไซเบอร์ความรู้ความเข้าใจในเรื่องดังกล่าวยังมีอยู่น้อยจึงมีแนวคิดที่จะจัดทำโครงการ Cyber Security Learning Platform เพื่อเป็นสื่อกลางในการศึกษารูปแบบการโจมตีทางไซเบอร์ (Cyber attack) กับการป้องกันอันตรายและการสร้างความปลอดภัยทางไซเบอร์ (Cyber Security) และการป้องกันภัยคุกคามจากการใช้เทคโนโลยีสารสนเทศและการสื่อสารขึ้นเพื่อให้กับเยาวชน และนักศึกษาเกิดการเรียนรู้เข้าใจและสามารถนำความรู้เกี่ยวกับความปลอดภัยทางไซเบอร์ไปพัฒนา ในด้านต่างๆ ได้ทันกับเทคโนโลยีสารสนเทศและการสื่อสารที่เปลี่ยนแปลงอย่างรวดเร็ว

อย่างไรก็ตามในการพัฒนาบุคลากรด้านไซเบอร์มักประสบปัญหาด้านงบประมาณที่ใช้ในการอบรมการผ่านการสอบประกาศนียบัตรที่รับรองมาตรฐานซึ่งต้องใช้ทั้งงบประมาณที่สูง บุคลากรที่มีศักยภาพสูง อีกทั้งต้องใช้เงินลงทุนในเครื่องมือที่ราคาแพงและต้องใช้ระยะเวลาที่ยาวนานในการฝึกฝนกว่าที่จะสามารถพัฒนาบุคลากรไซเบอร์ให้สามารถปฏิบัติการได้อย่างมีประสิทธิภาพ

๒. วัตถุประสงค์

เพื่อออกแบบและพัฒนาระบบต้นแบบ Online Game-Based Cybersecurity Learning Platform สำหรับใช้ในการพัฒนาบุคคลากรด้านไซเบอร์และเป็นช่องทางให้เยาวชน นักเรียน นักศึกษา ประชาชนสามารถเข้าถึงระบบการเรียนรู้เรื่องของภัยคุกคามทางไซเบอร์การโจมตีทางไซเบอร์และศึกษาเทคนิค วิธีป้องกัน ผ่านระบบ ซึ่งสามารถเข้าถึงได้ตลอดเวลาและไม่มีค่าใช้จ่ายในการใช้งาน ซึ่งจะแป็นส่วนที่ช่วยส่งเสริมการเรียนรู้ทางด้าน Cyber Security และเป็นส่วนหนึ่งที่ช่วยสร้างรากฐานการประกอบวิชาชีพด้านความมั่นคงปลอดภัยไซเบอร์ให้มีคุณภาพทัดเทียมมาตรฐานสากลและเป็นคลังสมองที่สำคัญของประเทศ

๓. วิธีการศึกษา

กำหนดกรอบแนวคิดโครงการ ทำการศึกษา กฎหมาย แผนแม่บทที่เกี่ยวข้อง เอกสารมาตรฐานทางเทคนิค ทฤษฎีที่เกี่ยวข้อง รายงานการวิจัยและข้อมูลจากต่างประเทศ การปรึกษาผู้เชี่ยวชาญที่มีประสบการณ์ ปรึกษาข้อคิดเห็นข้อแนะนำจากหน่วยงานต่างๆที่เกี่ยวข้อง

๔. ผลการศึกษา

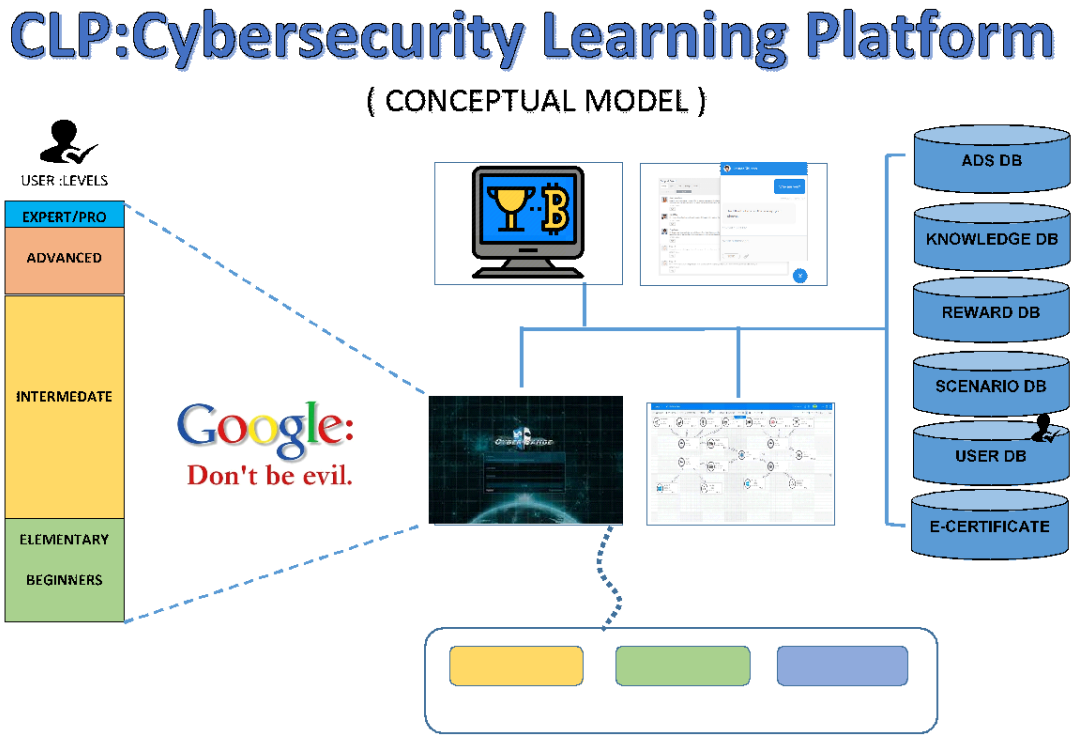
๔.๑ กรอบแนวคิด

จากกรอบแนวคดคิดจัดทำระบบการเรียนรู้ทางด้าน Cyber Security ที่ผู้เรียนสามารถเรียนได้เอง สามารถเข้าใช้งานได้ทุกเวลา โดยสามารถเข้าใช้งานผ่านอินเทอร์เน็ต การเรียนรู้จะเป็นไปในรูปแบบ Game-Based Learning ทำให้การเรียนรู้ผ่านการเล่นเกม เพื่อที่จะสื่อเรื่องของความรู้ทางด้าน Cyber Security ไปได้ในกลุ่มผู้เรียนที่หลากหลาย โดยนำทฤษฎีการเรียนรู้จากประสบการณ์’ หรือ Experiential Learning Theory (ELT) มาใช้และนำมาออกแบบ Game-Based Learning มาใช้ในการเรียนรู้ การออกแบบเกมมีเป้าหมายที่มุ่งเน้นเป็นเครื่องมือที่สนับสนุนการศึกษา การเรียนรู้ โดยเกมดิจิทัลเป็นเครื่องมือการเรียนรู้ ที่สามารถเพิ่มแรงจูงใจของนักเรียนเพื่อการเรียนรู้เพราะมีส่วนร่วมของผู้เล่นทำให้พวกเขามีส่วนร่วมและมีแรงจูงใจ ยิ่งไปกว่านั้นผู้เล่นยังสนุกไปกับการเล่นเกมเพราะพวกเขาต้องเรียนรู้ ซึ่งแน่นอน เมื่อการเล่นเกมดำเนินต่อไปดังนั้นผู้เล่นต้องมีการพัฒนาทักษะและเรียนรู้กลยุทธ์ใหม่ ๆ จนกว่าเกมจะล่นเสร็จสมบูรณ์และอีกหนึ่งคุณสมบัติของเกมที่ สอดคล้องกับการเรียนรู้ที่ดีนั่นคือ เกมให้ความคิดเห็นสั้น ๆ สิ่งนี้ช่วยให้ผู้เล่นสามารถ สำรวจสภาพแวดล้อมของเกม ลองสมมติฐานของพวกเขา เรียนรู้โดยทดลองและข้อผิดพลาดและรับข้อมูลทันที และพวกเขาสามารถใช้เพื่อกำหนดสมมติฐานที่ผิดพลาดอีกครั้งในสภาพแวดล้อมที่ถูกจำลองขึ้น ลักษณะนี้จะ สอดคล้องกับข้อกำหนดการศึกษาระบุว่าแนวทางการศึกษาส่วนใหญ่ ต้องการให้การศึกษาแก่นักเรียน พร้อมข้อเสนอแนะเกี่ยวกับความสำเร็จของพวกเขา

ดังนั้นเกมจึงเป็นสื่อที่เหมาะสำหรับการส่งเสริมความเป็นจริง กระบวนการเรียนรู้และ “ เรียนรู้ด้วยการทำ” ประสบการณ์การเรียนรู้ของตัวเองในแง่นี้ เกมสามารถให้ประสบการณ์การเรียนรู้ที่มีความหมายโดยจำลองสถานการณ์แบบโต้ตอบที่จะพบในโลกแห่งความจริง ปัญหาที่เกิดขึ้นด้วยเหตุนี้เกมจึงเป็นตัวแทนของสื่อที่ดีเพื่อส่งเสริมการเรียนรู้อย่างและพัฒนาทักษะการแก้ปัญหาของนักเรียนการปฏิบัติตามและนำไปสู่ประสิทธิภาพที่สูงขึ้น

ทางโครงการจึงมีแนวคิดจัดทำระบบ Cyber Security Learning Platform เพื่อพัฒนาบุคลากรทางด้านความมั่นคงปลอดภัยไซเบอร์ ที่สามารถเข้าใช้งานผ่านช่องทางอินเทอร์เน็ต Web based โดยระบบการเรียนรู้ของโครงการได้ดำเนินการจัดทำเป็นต้นแบบในระดับเริ่มต้น (Beginner) ซึ่งในส่วนระดับกลาง (Intermediate) และระดับสูง (Advance) และผู้เชี่ยวชาญ (expert) จะเป็นส่วนที่ต้องพัฒนาต่อยอดไปเฟสต่อๆไปในอนาคต การออกแบบ Game-Based Cybersecurity Learning Platform จะทำให้ผู้ใช้งานได้รับความสนุกสนาน และดึงดูดความสนใจ และทำให้เกิด Self Simulate Competition

เนื้อหาที่นำมาใช้นั้นจะมีการนำเสนอเนื้อหาด้าน Cyber Security ตามความยากง่ายในรูปแบบของทั้งการให้ข้อมูล คำถาม ปัญหาเพื่อวิเคราะห์ และแบบจำลอง (Scenario) เพื่อแก้ไขทั้งนี้ระบบได้นำเอาหลักการ พัฒนาเช่นเดียวกับ Cyber Range มาใช้ ทั้งนี้เนื้อหาที่นำมาใช้นั้นจะมีการทำ peer review หรือตรวจสอบกับหน่วยงานหรือสถาบันการศึกษาที่เป็นที่ยอมรับและเชื่อถือ โครงการนี้มีลักษณะรูปแบบโครงสร้าง (Conceptual Model) ดังแสดงในรูปที่ ๑



ภาพที่ ๗๔ โครงสร้างระบบ Cyber Security Learning Platform

จากรูปข้างต้น ระบบ Cyber Security Learning Platform ที่สร้างจะอยู่บน Cloud เพื่อสะดวกต่อการเข้าใช้งานและรองรับการเพิ่ม Traffic จากผู้เข้าใช้งานได้ สำหรับระบบซอฟท์แวร์นั้น มีการออกแบบและพัฒนาให้เป็น Online Game-Based โดยผู้เรียนสามารถเข้าเล่นเกมไปในโมดูลต่างๆ โดยในส่วนผู้ควบคุมระบบสามารถบริหารจัดการการใช้งานต่าง ๆ เช่น มีการบันทึกประวัติการใช้งาน, มี Chat board, ระบบการ Reward เป็นต้น นอกจากนี้ ระบบ ซอฟท์แวร์จะประกอบด้วยฐานข้อมูลของประวัติผู้เข้าใช้ (User Database) เพื่อติดตาม ความสัมฤทธิ์ผล, ฐานข้อมูลบทเรียน (Knowledge Database), สถานการณ์จำลอง (Scenario Database), ฐานข้อมูลอันดับผู้ชนะรางวัล (Reward Database) ระบบจะเป็นช่องทางเรียนรู้แบบ Online Self Training ทั้งนี้ในอนาคตยังสามารถจัดทำ e-certificate รับรองให้แก่ผู้เรียนที่สำเร็จได้อีกด้วย

๔.๒ ขอบเขตของงาน

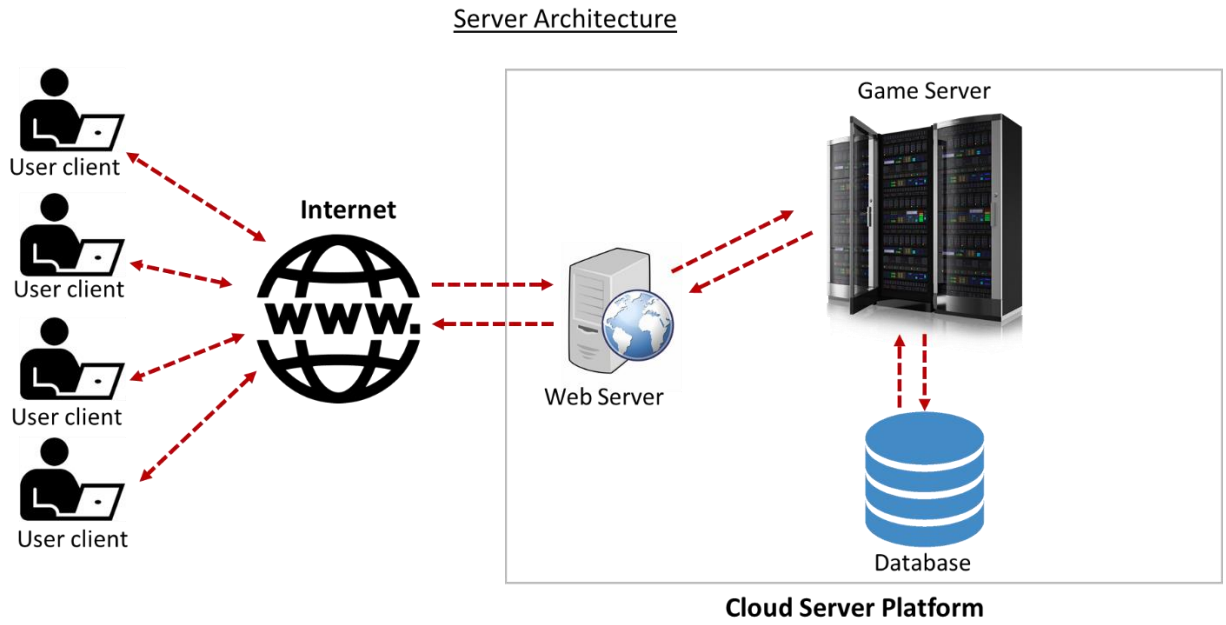
จัดทำต้นแบบระบบ Online Game-Based Cybersecurity Learning Platform ในส่วน Elementary and Basic Level ออกแบบ และจัดทำเนื้อหา ความรู้ Scenarios สำหรับเข้าเล่นทดลองปฏิบัติ มีส่วน Community chat room เพื่อให้ผู้ใช้งานสามารถสื่อสารใน Web Platform และมีการจัดประชุมหรือสัมนาร่วมกับสถาบันการศึกษา หรือองค์กรภาครัฐ/เอกชน รวมถึงบุคคลที่มีความสนใจเพื่อรับฟังข้อคิดเห็นหรือสร้างความร่วมมือและประชาสัมพันธ์การใช้งานระบบที่สร้างขึ้น พร้อมทั้งดำเนินการเก็บข้อมูลการใช้งานระบบและรายงานสรุปผลการดำเนินงาน

๔.๓ การดำเนินงาน

๔.๓.๑ การจัดหาระบบ Server เพื่อให้เหมาะสมกับลักษณะการใช้งานระบบ

จากการที่ผู้ใช้งานจะใช้งานได้สะดวกตลอดเวลานั้นทำให้ระบบต้องมีการใช้งานผ่านอินเทอร์เน็ตได้อย่างมีประสิทธิภาพ ดังนั้นทางโครงการจึงเลือกที่จะใช้วิธีเช่าใช้บริการระบบ Cloud Server จากทางผู้ให้บริการ โดยจะคิดค่าเช่าระบบตามปริมาณการใช้พื้นที่และปริมาณข้อมูล Traffic ที่ไหลเข้าออกของระบบ โดยในระยะแรกในระหว่างการพัฒนาระบบจะทำให้มีค่าใช้จ่ายที่ต่ำในแต่ละเดือนเมื่อระบบพร้อมให้บริการ คาดว่าจะมี Traffic User ที่ประมาณการไว้ที่ ๒๐๐ Concurrent User ซึ่งในช่วงนี้ก็จะทำให้มีค่าบริการรายเดือนที่เพิ่มสูงตามขนาด Traffic ที่มีการใช้งาน

System Architectures



ภาพที่ ๗๕ System Architectures

Google Cloud as a Service
https://firebase.google.com/

๔.๓.๒ การออกแบบระบบ Cybersecurity Learning Platform

จากทฤษฎีการเรียนรู้ที่นำมาใช้ในการออกแบบจะเป็นทฤษฎีการเรียนรู้จากประสบการณ์' หรือ Experiential Learning Theory (ELT) โดย ดร.เดวิด เอ. โคล์บ (Dr.David A. Kolb) นักทฤษฎีการศึกษา ซึ่งเป็นผู้ริเริ่มแนวคิดนี้โดยหลักการของ ELT มีอยู่ว่า คนเรามีรูปแบบการเรียนรู้อยู่ ๔ โหมดซึ่งหมุนเป็นวงจร สลับสับเปลี่ยนอย่างต่อเนื่องตลอดเวลาได้แก่ experiencing (มีประสบการณ์ลงมือทำ) reflecting (ใคร่ครวญ) thinking (คิดวิเคราะห์ สังเคราะห์ความรู้ใหม่ด้วยตนเอง) และ acting (ลงมือทำซ้ำจากความรู้ ความเข้าใจที่พัฒนาขึ้น) จากเมื่อนำมาประยุกต์ใช้ออกแบบ Game-Based โดยกำหนดกิจกรรมการเรียนรู้คือ การกำหนดองค์ประกอบที่มีลักษณะ การเรียนรู้จากเกม จากนั้นจึงทำการเชื่อมโยงองค์ประกอบเหล่านี้ทำให้เกิดกระบวนทัศน์ทางจิตวิทยาการสอน ในแบบ ProActive โดยจะพิจารณาได้ว่าเราไม่ได้เรียนรู้ เพียงวิธีเดียว แต่ในรูปแบบต่าง ๆ ที่ขึ้นอยู่กับเกี่ยวกับความถนัดส่วนตัวในสถานการณ์ สถานที่เรียนรู้เกิดขึ้นและเนื้อหา ที่จะเรียนรู้ มีรูปแบบมีคำอธิบายของวิธีการที่แตกต่างกัน การเรียนรู้สำหรับคนต่าง ๆ จะขึ้นอยู่กับทฤษฎีการเรียนรู้อันแสดงถึงการเรียนรู้ที่ไม่ได้มีข้อจำกัดเฉพาะ และในความเป็นจริงทุกคนสามารถมีการจัดการในเรื่องที่แตกต่างกันได้ตามสถานการณ์

ประสบการณ์ Game-Based Learning นอกจากความคิดเกี่ยวกับที่ต้องการใช้เป็นวิธีใหม่จากการเรียนรู้แบบดั้งเดิมรูปแบบและรวมถึงนวัตกรรมและความคิดสร้างสรรค์ โดยขึ้นอยู่กับคุณสมบัติเหล่านี้

๑. วัตถุประสงค์การเรียนรู้ที่เข้าใจ ข้อความที่ชัดเจนและเฉพาะเจาะจงของสิ่งที่ผู้เรียนรู้จะสามารถดำเนินการได้ในตอนท้าย ของกิจกรรม
๒. บทบาทของการสอนที่ซึ่งแตกต่างจากแบบดั้งเดิม การสอนแบบ ProActive เกิดการทดลอง เรียนรู้ รูปแบบ ความสงสัย และเกิดการศึกษาเพิ่มเติม
๓. บทบาทของผู้เรียนที่เปลี่ยนไป Fun to learn ในการโต้ตอบและการใช้งาน
๔. สภาพแวดล้อมของเกม โลกที่จำลองขึ้น กลศาสตร์ของเกมที่ใช้ และส่วนอื่นอีก (เช่นการสนทนาระหว่างเพื่อน chat, การสืบค้นข้อมูลเพิ่มเติม)
๕. กลยุทธ์การเรียนรู้ ซึ่งถือเป็นเส้นทางในการส่งเสริมการเรียนรู้ที่มีประสิทธิภาพ กระบวนการ.จุดเด่นการเล่นเกม ที่หมายถึง การเล่นเกมในด้านที่ต้องการ หรือความเหมาะสมกับมุมมองการเรียนรู้ในแต่ละแบบ
๖. การส่งเสริมการเรียนรู้ที่จะมาจากกลไกของเกมที่สามารถส่งเสริมการเรียนรู้ให้พัฒนาขึ้นไปได้
๗. ลักษณะของงาน จุดเด่นในเกม ผู้เล่นมีความอิสระที่จะกำกับตนเอง การใช้ประสบการณ์ตัวเองในการกำหนดวิธีการต่าง ๆ

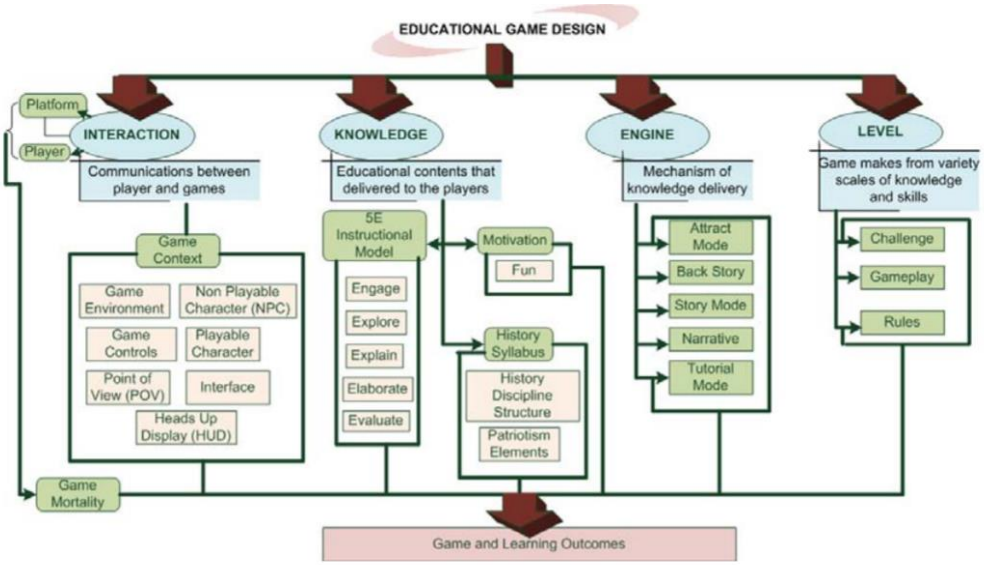
๔.๓.๓ Cyber Security Knowledge for Game-Based Learning Design

Cyber Security Knowledge Base for Elementary and Basic Level

เนื้อหาความรู้ที่นำมาอยู่ใน Game จะเป็นความรู้จาก Ethical Hacking Course ที่เป็นจุดสำคัญของการตระหนักเรื่องภัยคุกคามไซเบอร์และเป็นจุดสนใจในการเรียนรู้ในระดับสูงขึ้นต่อไป

การออกแบบ Game Design Scenario and Flow อ้างอิงจากการออกแบบ Education Game Design

[๑๘]



ภาพที่ ๗๖ Game Design Scenario

ในการออกแบบเกมทางด้าน Mechanic จะนำกลยุทธ์การใช้วิธีการ ทาง Cyber Security มากระทำเพื่อไปสู่เป้าหมายของเกม โดยสอดแทรก action ทางด้าน cyber security เช่นการใช้ Social engineering หลอกล่อให้เหยื่อในเกมหลงกล โดยผู้เล่นจะต้องใช้เครื่องมือต่างๆ ในการเจาะระบบ เช่น Network Scanning, Phishing , Malware , Trojan, Encryption, Password crack, etc.

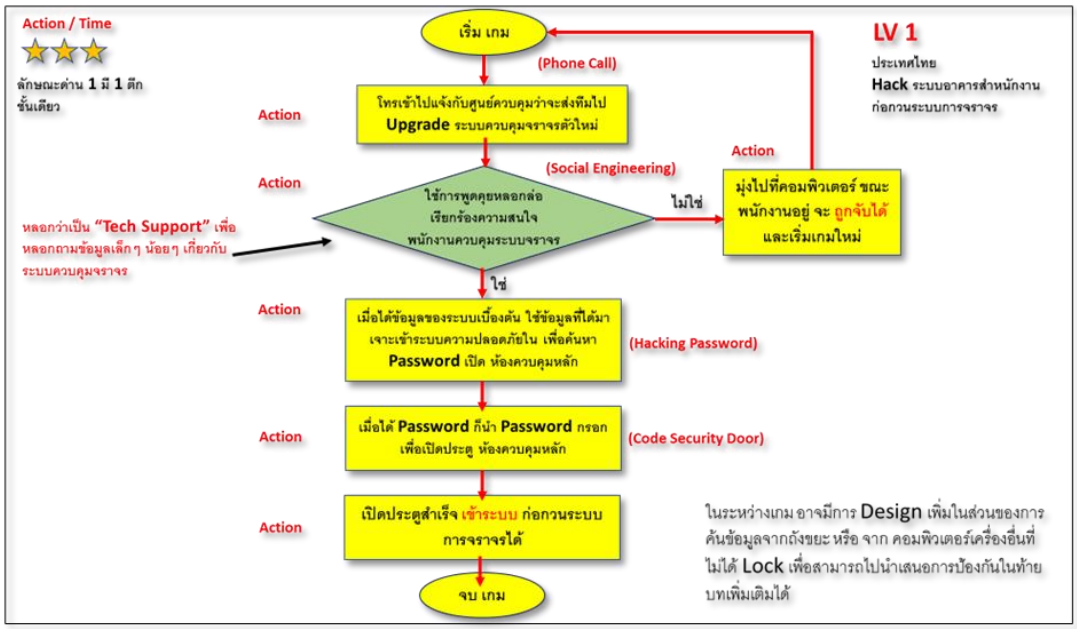
ในเกมจะมี Action ให้เลือกโดยจำกัด ตามเงื่อนไขของแต่ละด่าน และต้องแข่งกับเวลาซึ่ง Scoring จะสัมพันธ์กับการใช้เวลาในเกม โดยในการดำเนินเรื่องของเกม จะมีจุด Action ที่เมื่อผู้เล่นเลือกวิธีการนี้จะทำให้ถูกหักแต้มอยู่ในด่านด้วย

ลักษณะเกมจะแทรกความรู้ ระหว่างเล่น และเมื่อเล่นจบในแต่ละด่าน จะมีสรุป อธิบายรายละเอียดรวมถึงผลกระทบ และยังบอกวิธีการป้องกัน และ จะเป็นคำแนะนำ เพื่อให้เกิดความตระหนักรู้ และการค้นคว้าหาข้อมูลต่อในเรื่องของความปลอดภัยทางไซเบอร์มากขึ้นลักษณะเกมจะแทรกความรู้ ระหว่างเล่น และเมื่อเล่นจบในแต่ละด่าน จะมีสรุป อธิบายรายละเอียดรวมถึงผลกระทบ และยังบอกวิธีการป้องกัน และ จะเป็นคำแนะนำ เพื่อให้เกิดความตระหนักรู้ และการค้นคว้าหาข้อมูลต่อในเรื่องของความปลอดภัยทางไซเบอร์มากขึ้น

๔.๓.๔ Game Design Level/Scenario

ตัวอย่าง ด่าน ๑ ประเทศไทย, การ Hack ระบบอาคารสำหนักงาน เพื่อก่อกวนระบบควบคุมการจราจร

๑st Stage



ภาพที่ ๗๗ การออกแบบตัวอย่าง Scenario ด่านที่ ๑

๔.๓.๕ ภาพรวม Web UI Design

ในการ Design ออกแบบหน้า website เบื้องต้น จะออกแบบ Dashboard ที่มีความง่ายในการใช้งานไม่ซับซ้อน โดยจะมีการนำ ข่าวสารเกี่ยวกับ IT , Technology , Cybersecurity Knowledge, Video Link Knowledge มาอยู่บนหน้า Web โดยในหน้าของเวบไซท์ จะมีให้ผู้ใช้ Log in , Register ไม่ว่าจะเป็น ผ่าน Social network (Facebook, Twitter) & Email (Google Account)

มีหัวข้อให้ความรู้เกี่ยวกับความปลอดภัยทางไซเบอร์ เพื่อให้เกิดความตระหนักในการใช้งานบนโลกออนไลน์ ผู้ใช้สามารถเข้าไปทำความเข้าใจและศึกษาข้อมูลได้ตาม หัวข้อต่างๆ และจะมีแบบฝึกหัดให้ทำท้ายบท

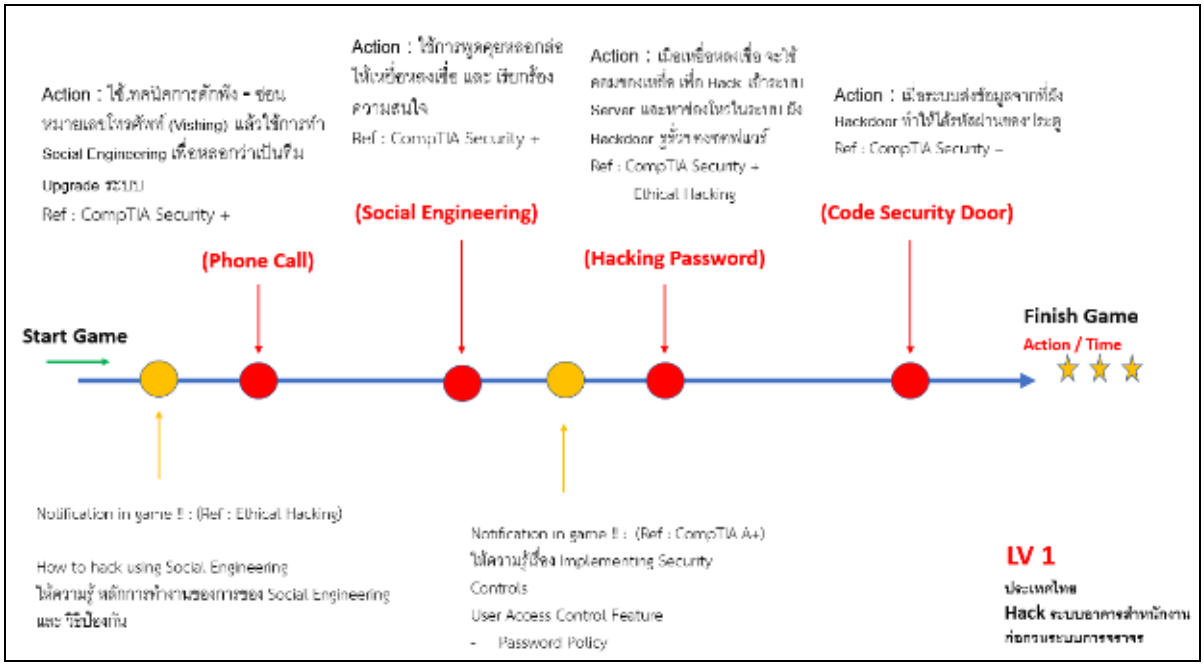
ในส่วนของเกม จะเป็นเกมที่มีความสนุก และ สอดแทรกความรู้เข้าไป เบื้องต้นมีทั้งหมด ๘ ด่าน โดยไล่ระดับความยากขึ้นไป ในแต่ละด่านจะมี Action ให้ทำ โดยคะแนนจะมาจากเวลา และ ความถูกต้องของผู้เล่น และยังมีการจัดลำดับผู้เล่นอีกด้วย

ส่วนหนึ่งของหน้าเวบ จะมีเป็น ห้องตั้งกระทู้ , Chat board ให้ทางผู้ใช้งานสามารถพูดคุยเกี่ยวกับเรื่องความปลอดภัยทางไซเบอร์ สอบถามปัญหาแบ่งปันข้อมูลกันได้

๔.๓.๖ Game Design Story Board

ดำเนินการออกแบบและจำลองสถานการณ์ในเกม ตามแผนงานจำนวน ๘ ด่าน (Mission) โดยระหว่างเล่นเกมผู้เล่นก็จะได้เรียนรู้ไปกับ Action และ Notification ต่างๆ ในเกมที่จะคอยเสริมสร้างความรู้ความตระหนักทางไซเบอร์

ตัวอย่างการออกแบบด่าน ๑



ภาพที่ ๗๘ ตัวอย่างการออกแบบจำลอง Action ในเกม ด่านที่ ๑

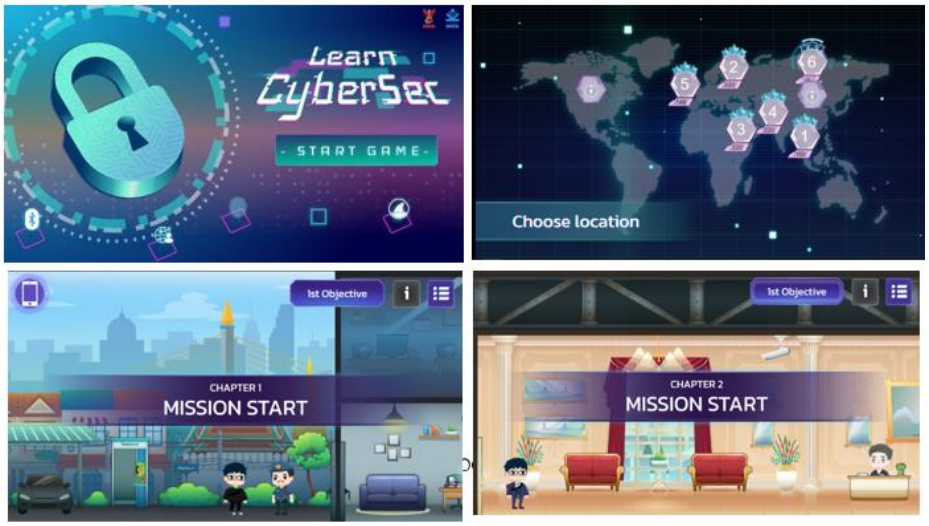
ภาพที่ ๗๙ ตัวอย่างการออกแบบด่าน ๑

๔.๓.๖ รายงานผลการจัดทำระบบ

มีบทเรียนทั้งหมด ๘ ด่าน

สามารถเลือกเล่นได้ทีละด่านตามลำดับ ๑ - ๘ เมื่อผ่านภารกิจของด่านนั้นๆแล้วด่านถัดไปจะถูกปลดล็อค ก่อนเข้าทำภารกิจด่านที่ ๑ จะมีแบบทดสอบประเมินก่อนเล่น (Pre-Test) และจะมีแบบทดสอบอีกครั้งหากผู้เล่นได้ทำภารกิจครบทั้ง ๘ ด่าน (Post-Test)

ลิงก์ https://www.learncybersec.org/game



ภาพที่ ๘๐ ผลการออกแบบภาพรวมเกมของทั้ง ๘ ด่าน (๑)

ภาพที่ ๘๑ ผลการออกแบบภาพรวมเกมของทั้ง ๘ ด่าน (๒)

๔.๓.๗ รายงานผลการจัดกิจกรรมสัมมนาแนะนำระบบ และเผยแพร่ระบบให้กับสาธารณะเริ่มต้นที่หน่วยงานการศึกษา

โครงการระบบออนไลน์เพื่อพัฒนาผู้เชี่ยวชาญด้านความปลอดภัยไซเบอร์ได้ดำเนินงานบรรลุตามวัตถุประสงค์ของโครงการ เนื่องจากการจัดกิจกรรมสัมนาได้รับผลตอบรับที่ดี โดยมีผู้เข้าร่วมหลายภาคส่วน ไม่ว่าจะเป็นกลุ่มนักเรียนนึกศึกษา กลุ่มหน่วยงานราชการ/รัฐวิสาหกิจ กลุ่มหน่วยงานเอกชน และกลุ่มประชาชนทั่วไป อีกทั้งยังได้รับความร่วมมือจากสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ ที่ได้มาช่วยถ่ายทอดความรู้ทางด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่ผู้เข้าร่วมกิจกรรมสัมนา ในส่วนของเนื้อหาที่สัมนามีความสอดสอดคล้องกับภาคปฏิบัติจริงในชีวิตประจำวัน ซึ่งจำนวนผู้เข้าร่วมกิจกรรมสัมมนาแนะนำระบบในครั้งนี้เกินจำนวนเป้าหมายที่ทางโครงการได้ตั้งเป้าไว้

ภาพที่ ๘๒ โปสเตอร์ประชาสัมพันธ์ผ่านทางสื่อต่างๆ และกิจกรรมการเผยแพร่สู่สาธารณะผ่านสื่อออนไลน์

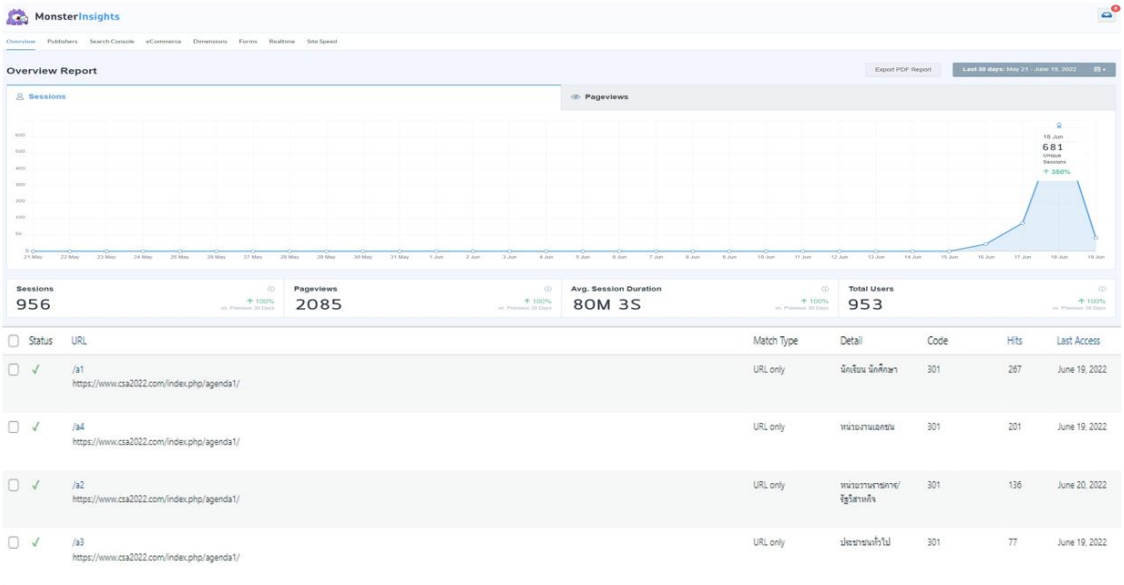
การจัดกิจกรรมการสัมนาได้เผยแพร่การถ่ายทอดสดใน วันที่ ๑๘ มิถุนายน ๒๕๖๕ เข้าชมผ่านช่องทาง https://www.learncybersec.org/csa2022 โดยทางผู้จัดทำได้แบ่งกลุ่มออกเป็น ๔ กลุ่มได้แก่ กลุ่มนักเรียน/นักศึกษา , หน่วยงานราชการ/รัฐวิสาหกิจ , หน่วยงานเอกชน และประชาชนทั่วไป ในการเข้าชมการถ่ายทอดงานสัมนา CSA๒๐๒๒ มีผู้เข้าร่วมงานในลักษณะ Virtual Conference เป็นจำนวนทั้งสิ้น ๖๘๑ คน โดยสรุปจำนวนผู้เข้าร่วมงานสัมนาได้ ดังนี้

กลุ่มที่ ๑ กลุ่มนักเรียนนักศึกษา จำนวน ๒๖๗ คน (คิดเป็น ๓๙.๒๑%)

กลุ่มที่ ๒ กลุ่มหน่วยงานราชการ/รัฐวิสาหกิจ จำนวน ๑๓๖ คน (คิดเป็น ๑๙.๙๗%)

กลุ่มที่ ๓ กลุ่มหน่วยงานเอกชน จำนวน ๒๐๑ คน (คิดเป็น ๒๙.๕๑%)

กลุ่มที่ ๔ กลุ่มประชาชนทั่วไป จำนวน ๗๗ คน (คิดเป็น ๑๑.๓๑%)

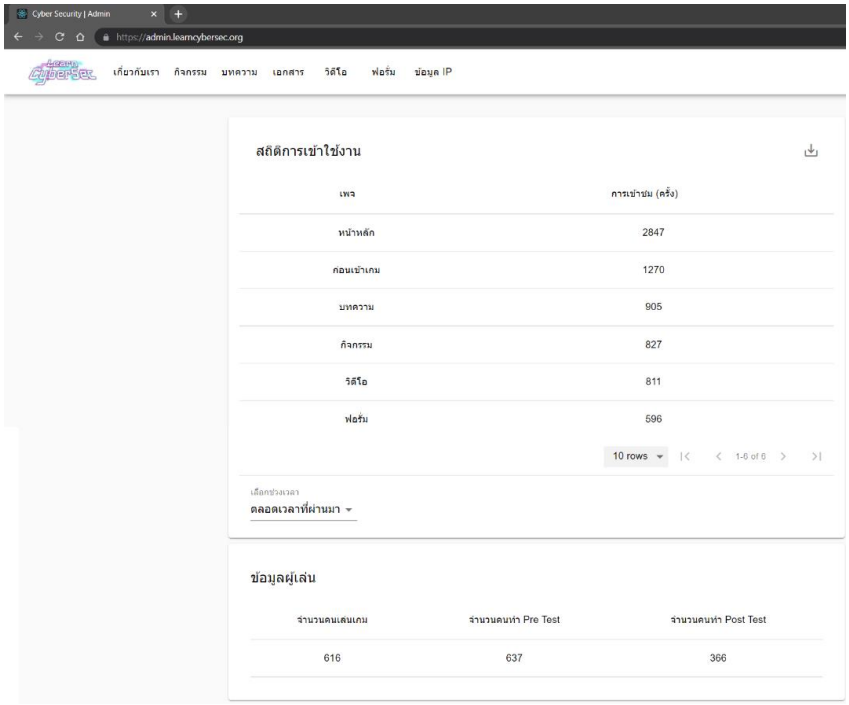


ภาพที่ ๘๓ จำนวนผู้เข้าร่วมกิจกรรมสัมมนาแนะนำระบบ

๔.๓.๘ รายงานผลการใช้งานระบบและการประเมินผล

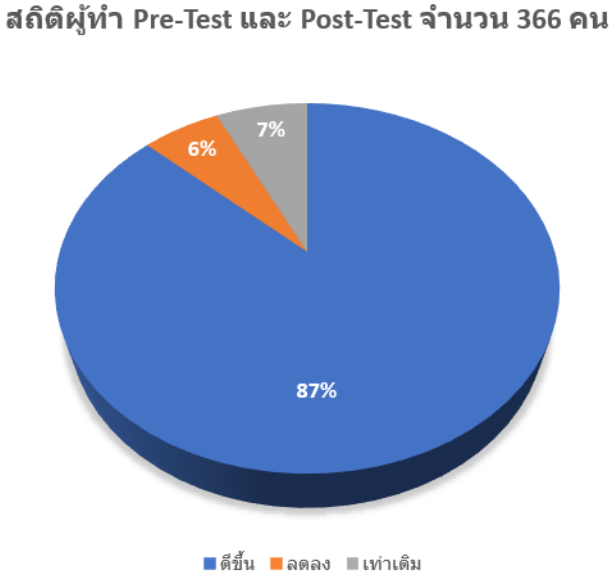
โครงการระบบออนไลน์เพื่อพัฒนาผู้เชี่ยวชาญด้านความปลอดภัยไซเบอร์ ได้จัดจัดสร้างระบบต้นแบบ Online Game-Based Cybersecurity Learning Platform (Basic-Beginner) ซึ่งเป็นช่องทางการเรียนรู้ การเพิ่มทักษะ ให้กับเยาวชนบุคคลที่มีความสนใจ ในเรื่องความตระหนักรู้ถึงภัยคุกคามและอาชญากรรมไซเบอร์และการรักษาความมั่นคงปลอดภัยไซเบอร์โดยสถิติจำนวนผู้เข้าใช้งานระบบของ https://www.learncybersec.org/ จากระบบผู้ดูแลระบบ (Back-End) โดยมีรายละเอียดดังนี้

๑. จำนวนผู้เข้าชมหน้าหลัก จำนวน ๒,๘๔๗ ครั้ง
๒. จำนวนผู้เข้าชมหน้าก่อนเข้าเกม จำนวน ๑,๒๗๐ ครั้ง
๓. จำนวนผู้เข้าชมหน้าบทความ จำนวน ๙๐๕ ครั้ง
๔. จำนวนผู้เข้าชมหน้ากิจกรรม จำนวน ๘๒๗ ครั้ง
๕. จำนวนผู้เข้าชมหน้าวีดีโอ จำนวน ๘๑๑ ครั้ง
๖. จำนวนผู้เข้าชมหน้าฟอรั่ม จำนวน ๕๙๖ ครั้ง



ภาพที่ ๘๔ สถิติจำนวนผู้เข้าใช้งานระบบ

จากภาพที่ ๘๔ สถิติจำนวนผู้เข้าใช้งานระบบแสดงให้เห็นถึงข้อมูลผู้เข้าเล่มเกม การประเมินผลข้อมูลผู้เข้าเล่นเกม มีจำนวนผู้เข้าทำข้อสอบก่อนเข้าเล่นเกม (Pre-Test) จำนวน ๖๓๗ คน ในจำนวน ๖๓๗ คนมีผู้เข้าทำข้อสอบหลังเข้าเล่นเกม (Post-Test) จำนวน ๓๖๖ คน จากการประเมินสถิติจากระบบหลังบ้าน (Back-End) ในจำนวนผู้ทำข้อสอบหลังเข้าเล่นเกม (Post-Test) จำนวน ๓๖๖ คนนั้นพบว่ามีจำนวน ๓๑๘ คน หรือ ๘๖.๘๙% มีเกณฑ์คะแนนที่ดีขึ้น มีผู้ที่ได้คะแนนลดลงจำนวน ๒๒ คน คิดเป็น ๖.๐๑% และมีผู้ที่ได้คะแนนเท่าเดิมจำนวน ๒๖ คน คิดเป็น ๗.๑๐% ดังภาพที่ ๘๕



ภาพที่ ๘๕ สถิติผู้ทำ Pre-Test และ Post-Test จำนวน ๓๖๖ คน

๕. บทสรุปและข้อเสนอแนะ

ทำอย่างไรให้การเรียนรู้ทางด้านความมั่นคงปลอดภัยไซเบอร์ เป็นเรื่องที่เข้าใจได้และเป็นจุดสนใจในการเรียนรู้ต่อไปในขั้นสูง

การจัดทำระบบ Online Game-Based Cyber Security Learning ถือได้ว่าเป็นตัวอย่างสื่อการเรียนรู้ที่ควรมีการพัฒนาไปในปัจจุบันที่ การเรียนไม่จำเป็นต้องอยู่ในห้องเรียน การศึกษาสามารถเข้าถึงได้ตลอดเวลา การเรียนรู้ที่ฝึกให้ผู้เรียนคิดตามและเกิดประสบการณ์ โดยใช้การเรียนรู้ผ่านเกมเพื่อปรับปรุงการศึกษาด้านความมั่นคงปลอดภัยไซเบอร์ การใช้แบบจำลองเป็นแรงจูงใจแต่ก็มีจุดที่ยากสำหรับการออกแบบเกม ความยากและซับซ้อนเกินไปอาจจะไม่เกิดความสนุกในการเล่น ทำให้ผู้เรียนลดความสนใจลงไปได้ อย่างไรก็ดี เกมสามารถเป็นวิธีที่มีประสิทธิภาพในการแนะนำการรักษาความปลอดภัยทางไซเบอร์ให้กับเยาวชน ในขณะที่เกมความปลอดภัยทางไซเบอร์ในปัจจุบันเริ่มมีการจัดทำกันมากขึ้น สิ่งนี้ชี้ให้เห็นว่าศักยภาพในการเรียนรู้ด้วยเกมเจะเป็นแรงดึงดูดและแนะนำเรื่องการรักษาความปลอดมั่นคงปลอดภัยทางไซเบอร์ไปในวงกว้างสำหรับเยาวชนในปัจจุบันได้

บรรณานุกรม

[๑] สำนักงานสภาความมั่นคงแห่งชาติ, ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ, พ.ศ. ๒๕๖๐ - ๒๕๖๔, หน้า ๒๑.

[๒] (ISC๒) Cyber Security Workforce Study, “Cyber Security Professionals Focus on Developing New Skills as Workforce Gap Widens”,๒๐๑๘ Study Results”, ๒๗๑๘,

[๓] NATO Cooperative Cyber Defence Centre of Excellence, https://ccdcoe.org/exercises/.

[๔] C. C. Evangelos, “Cyber-security training: A Comparative Analysis of Cyber-ranges and Emerging trends”, M.Sc. Thesis, ๒๐๑๙.

[๕] J. Davis and S. Magrath, “A survey of cyber ranges and testbeds”. DSTO – Defence Science and Technology Organisation, Technical Report DSTO-GD-๐๗๗๑, ๒๐๑๓.

[๖] W. F. Lynn III, "Defending a new domain: the Pentagon's Cyberstrategy," ๒๐๑๐ DTIC Document.

[๗] Broad Agency Announcement (BAA), “National Cyber Range”, DARPA, ๒๐๐๘.

[๘] กองทัพบก, แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร, พ.ศ. ๒๕๕๙ - ๒๕๖๑, หน้าที่ ๒๑

[๙] J. A. Amorim, M. Hendrix, S. F. Andler and P. M. Gustavsson, “Gamified training for cyber defence: Methods and automated tools for situation and threat assessment”, In NATO Modelling and Simulation Group (MSG) Annual Conference ๒๐๑๓ (MSG-๑๑๑).

[๑๐] P. Backlund, M. Hendrix, “Educational Games - Are They Worth The Effort”, ๕th International Conference on Games and Virtual Worlds for Serious Applications (VS-Games), United Kingdom, ๒๐๑๓.

[๑๑] S. Scholefield, L. A. Shepherd, “Gamification Techniques for Raising Cyber Security Awareness”, in Moallem A. (eds) HCI for Cybersecurity, Privacy and Trust. HCII ๒๐๑๙. Lecture Notes in Computer Science, vol ๑๑๕๙๔. Springer, Cham.

[๑๒] A. Marczewski, https://www.gamified.uk/user-types/gamification-mechanics-elements/

[๑๓] G. Zichermann, C. Cunningham, “Gamification by Design:Implementing Game Mechanics in Web and Mobile Apps”,O'Reilly Media, ๒๐๑๑.

[๑๔] C. L. Nancy, and O. A. Joshua,”Cyber Red/Blue and. Gamified Military. Cyberspace Operations”, Lincoln Laboratory Journal, Vol. ๒๓, ๒๐๑๙.

[๑๕] C. Irvine and M. Thompson,”CyberCIEGE Scenario Design and Implementation”, USENIX Summit on Gaming, Games, and Gamification in Security Education, San Diego, CA, ๒๐๑๔.

[๑๖] Kolb, A. Y., & Kolb, D. A. (๒๐๑๘). Eight important things to know about the experiential learning cycle. Australian educational leader, ๔๐(๓), https://learningfromexperience.com/downloads/research-library/eight-important-things-to-know-about-the-experiential-learning-cycle.pdf

[๑๗] Free Ethical Hacking Tutorials: Course for Beginners, https://www.guru99.com/ethical-hacking-tutorials.html

[๑๘] Nor Azan Mat Zin and Wong Seng Yue “Design and Evaluation of History Digital Game Based Learning (DGBL) Software”

[๑๙] Esther Oprins*and Gillian Visschedijk , “The game-based learning evaluation model (GEM): Measuring the effectiveness of serious games using a standardised method”

ภาคผนวก ก

เอกสารประกอบการบรรยาย