เครื่องมือช่วยประเมินช่องโหว่ด้านความมั่นคงเพื่อการยกระดับเวอร์ชันของซอฟต์แวร์

นางสาวศิริขวัญ ตรีทิพยรักษ์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมซอฟต์แวร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2559

Security Vulnerability Assessment Tool for Software Version Upgrade

Miss Sirikwan Treetippayaruk

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science Program in Software Engineering
Department of Computer Engineering
Faculty of Engineering
Chulalongkorn University
Academic Year 2016

หัวข้อวิทยานิพนธ์	เครื่องมือช่วยประเมินช่องโหว่ด้านความมั่นคงเพื่อการยกระดับเวอร์ชันของซอฟต์แวร์
โดย	นางสาวศิริขวัญ ตรีทิพยรักษ์
สาขาวิชา	วิศวกรรมซอฟต์แวร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	รองศาสตราจารย์ ดร.ทวิตีย์ เสนีวงศ์ ณ อยุธยา

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

.....คณบดีคณะวิศวกรรมศาสตร์
(รองศาสตราจารย์ ดร.สุพจน์ เตชวรสินสกุล)

คณะกรรมการสอบวิทยานิพนธ์

.....ประธานกรรมการ
(รองศาสตราจารย์ ดร.วิวัฒน์ วัฒนาวุฒิ)

.....อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(รองศาสตราจารย์ ดร.ทวิตีย์ เสนีวงศ์ ณ อยุธยา)

.....กรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.เกริก ภิรมย์โสภา)

.....กรรมการภายนอกมหาวิทยาลัย
(ผู้ช่วยศาสตราจารย์ ดร.ชวลิต ศรีสถาพรพัฒน์)

ศิริขวัญ ตรีทิพยรักษ์ : เครื่องมือช่วยประเมินช่องโหว่ด้านความมั่นคงเพื่อการยกระดับเวอร์ชันของซอฟต์แวร์ (Security Vulnerability Assessment Tool for Software Version Upgrade) อ.ที่ปรึกษาวิทยานิพนธ์หลัก: รศ. ดร.ทวิตีย์ เสนีวงศ์ ณ อยุธยา, 70 หน้า.

ซอฟต์แวร์ที่ติดตั้งในเครื่องคอมพิวเตอร์อาจจะมีช่องโหว่ที่ทำให้ผู้โจมตีสามารถเข้าถึงหรือใช้ประโยชน์จากคอมพิวเตอร์ได้ ซึ่งการป้องกันที่ดีที่สุดคือการยกระดับเวอร์ชันซอฟต์แวร์ เพื่อแก้ไขปัญหาต่างๆ ผู้ขายผลิตภัณฑ์ซอฟต์แวร์มักออกเวอร์ชันใหม่ๆ อยู่เป็นระยะเพื่อเพิ่มความสามารถของซอฟต์แวร์ แก้ไขข้อบกพร่อง หรือแก้ไขจุดอ่อนด้านความมั่นคง อย่างไรก็ตามการที่ผู้ดูแลระบบขององค์กรหรือผู้ใช้งานจะยกระดับเวอร์ชันซอฟต์แวร์ให้เป็นปัจจุบันทุก ๆ ซอฟต์แวร์เป็นเรื่องที่ทำได้ยาก เพราะมักเกิดความกังวลในปัญหาที่อาจตามมาหลังจากยกระดับเวอร์ชันซอฟต์แวร์

ดังนั้นในงานวิจัยนี้จึงเสนอเครื่องมือเพื่อประเมินความรุนแรงของช่องโหว่ในซอฟต์แวร์ที่ติดตั้งในคอมพิวเตอร์เปรียบเทียบกับซอฟต์แวร์เวอร์ชันล่าสุด โดยที่การประเมินจะนำคะแนนซีวีเอสเอสเข้ามาประเมินความรุนแรงของช่องโหว่และจะใช้คะแนนซีวีเอสเอสทั้ง 3 กลุ่ม คือ กลุ่มตัววัดพื้นฐาน กลุ่มตัววัดตามเวลา และกลุ่มตัววัดตามสภาพแวดล้อม โดยที่คะแนนกลุ่มตัววัดพื้นฐานจะได้มาจากเอ็นวีดีและคะแนนกลุ่มตัววัดตามเวลาจะได้มาจากไอบีเอ็ม เอกซ์เอฟอี ส่วนคะแนนกลุ่มตัววัดตามสภาพแวดล้อมได้จากการเลือกตามประเภทสารสนเทศในองค์กรตามระดับผลกระทบต่อองค์กรจากการสูญเสียองค์ประกอบด้านความมั่นคงจาก NIST เครื่องมือสามารถแนะนำได้ว่าควรยกระดับเวอร์ชันซอฟต์แวร์หรือไม่ และผู้ใช้งานสามารถเลือกยกระดับเวอร์ชันซอฟต์แวร์ที่มีผลกระทบมากที่สุดก่อนได้

ในการประเมินความพึงพอใจของผู้ใช้เครื่องมือได้คะแนน 4.26 จากคะแนนเต็ม 5 นอกจากนี้ประสิทธิภาพของเครื่องมือในการค้นหาชื่อและเวอร์ชันของซอฟต์แวร์จากฐานข้อมูลเอ็นวีดีได้ค่าเอฟ-เมเชอร์เฉลี่ยเป็น 0.9919 ซึ่งผลการประเมินทั้งสองอยู่ในระดับที่น่าพอใจ

ภาควิชา วิศวกรรมคอมพิวเตอร์ ลายมือชื่อนิสิต .....

สาขาวิชา วิศวกรรมซอฟต์แวร์ ลายมือชื่อ อ.ที่ปรึกษาหลัก .....

ปีการศึกษา 2559

5870969821 : MAJOR SOFTWARE ENGINEERING
KEYWORDS: SECURITY / VULNERABILITY / CVSS / NVD / SECURITY ASSESSMENT / SOFTWARE UPGRADE

SIRIKWAN TREETIPPAYARUK: Security Vulnerability Assessment Tool for Software Version Upgrade. ADVISOR: ASSOC. PROF.TWITTIE SENIVONGSE, Ph.D., 70 pp.

Software installed on a computer may have vulnerabilities that allow an attacker to access or exploit a computer and the best protection is upgrading software. Software vendors periodically release software updates to upgrade software to the latest versions with new features, to fix bugs, or to fix security weaknesses. However, it is difficult for administrators or users to upgrade all software to the latest version, because there are concerns about problems that might ensue after upgrading the software version.

Therefore, this thesis proposes a tool to assess severity of the vulnerabilities of the installed software version in comparison with that of the latest version. The assessment is based on the CVSS vulnerability scoring system and considers all metric groups, i.e. Base, Temporal, and Environmental metric groups. The Base score of particular software is taken from the National Vulnerability Database (NVD) and the Temporal score from IBM XForce Exchange. The Environmental score follows NIST classification of the security impact an information system would have on an organization. The assessment tool can suggest whether the upgrade to the latest versions is necessary. Thus, the users can decide to upgrade software version that has the most severe vulnerability first.

In a user satisfaction evaluation, the tool scores 4.26 out of 5. In addition, the performance of the tool in finding software names and versions information in the NVD in terms of the average F-measure is 0.9919. Both evaluation results are satisfactory.

Department: Computer Engineering Student's Signature .....
Field of Study: Software Engineering Advisor's Signature .....
Academic Year: 2016

กิตติกรรมประกาศ

ข้าพเจ้าขอขอบพระคุณ รองศาสตราจารย์ ดร.ทวิตีย์ เสนีวงศ์ ณ อยุธยา อาจารย์ที่ปรึกษาวิทยานิพนธ์ ที่กรุณาเสียสละเวลาให้ความรู้ คำแนะนำ คำปรึกษา และแนวทางในการทำวิจัยตลอดระยะเวลาการศึกษา จนทำให้การจัดทำวิทยานิพนธ์นี้สำเร็จลุล่วงไปได้ด้วยดี

ขอขอบพระคุณ รองศาสตราจารย์ ดร.วิวัฒน์ วัฒนาวุฒิ ประธานกรรมการการสอบวิทยานิพนธ์ ผู้ช่วยศาสตราจารย์ ดร.เกริก ภิรมย์โสภา และผู้ช่วยศาสตราจารย์ ดร.ชวลิต ศรีสถาพรพัฒน์ กรรมการการสอบวิทยานิพนธ์ที่กรุณาให้ความรู้และคำแนะนำต่างๆ ที่เป็นประโยชน์ในการทำวิทยานิพนธ์

ขอขอบพระคุณ คุณพ่อและคุณแม่ที่ให้โอกาสในการศึกษา ให้ความรัก ความห่วงใย กำลังใจและการสนับสนุนข้าพเจ้าในทุกๆ สิ่ง จนประสบความสำเร็จ

ขอบคุณเพื่อนๆ ร่วมงานที่บริษัทที่คอยช่วยเหลือข้าพเจ้าในการทำวิทยานิพนธ์ ทั้งในเรื่องทรัพยากรในการพัฒนาเครื่องมือและความรู้ต่างๆ

ขอบคุณเพื่อนๆ นิสิตสาขาวิศวกรรมซอฟต์แวร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ที่คอยช่วยเหลือ ให้คำปรึกษา แลกเปลี่ยนความรู้ในการทำวิทยานิพนธ์

สารบัญ

หน้า

หน้า

หน้า

สารบัญตาราง

สารบัญภาพ

บทที่ 1
บทนำ

1.1. ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบันคอมพิวเตอร์ได้เข้ามามีบทบาทในองค์กรมากขึ้น โดยที่องค์กรได้นำซอฟต์แวร์เข้ามาช่วยในการทำงานแทนมนุษย์เพื่ออำนวยความสะดวกสบายและเพิ่มประสิทธิภาพในการดำเนินธุรกิจได้มากขึ้น เนื่องจากซอฟต์แวร์สามารถทำงานได้ดีกว่ามนุษย์ในหลาย ๆ ด้าน เช่น ความถูกต้องแม่นยำ ความเป็นระบบระเบียบ ความรวดเร็วในการทำงาน การทำงานที่ยุ่งยากซับซ้อนให้ง่ายขึ้น และมีความจำที่ดีกว่ามนุษย์เป็นอย่างมาก เป็นต้น แต่ซอฟต์แวร์เหล่านี้ยังต้องการผู้ใช้งาน (User) หรือผู้ดูแลระบบเป็นผู้ดูแลแก้ไขปัญหาที่เกิดจากการใช้งานซอฟต์แวร์

ในเครื่องคอมพิวเตอร์จะประกอบไปด้วยซอฟต์แวร์หลายรายการ เพราะแต่ละซอฟต์แวร์จะมีหน้าที่การทำงานเฉพาะที่แตกต่างกันไป การจะติดตั้งซอฟต์แวร์ใด ๆ ในเครื่องคอมพิวเตอร์ จะขึ้นอยู่กับความต้องการในการใช้งานของผู้ใช้งาน และเมื่อเวลาผ่านไปผู้ขายผลิตภัณฑ์ซอฟต์แวร์จะออกเวอร์ชันใหม่ออกมาเป็นระยะเพื่อแก้ไขปัญหาต่าง ๆ เช่น การแก้จุดบกพร่องในซอฟต์แวร์ การปรับปรุงความมั่นคงให้ดีขึ้น หรือการปรับปรุงให้ผู้ใช้งานใช้งานได้ง่ายขึ้น เป็นต้น ซึ่งการที่ผู้ใช้งานหรือผู้ดูแลระบบจะทำการยกระดับเวอร์ชันซอฟต์แวร์ให้เป็นปัจจุบันทุก ๆ ซอฟต์แวร์เป็นเรื่องที่ทำได้ยาก เพราะกลัวต่อปัญหาที่อาจตามมาหลังจากยกระดับเวอร์ชันซอฟต์แวร์

ปัญหาที่อาจตามมาหลังจากยกระดับเวอร์ชันซอฟต์แวร์ เช่น

1. การกลัวว่าซอฟต์แวร์เวอร์ชันใหม่เข้าไม่ได้กับระบบปฏิบัติการที่ใช้งานอยู่
2. ซอฟต์แวร์ที่ต้องการยกระดับเวอร์ชันทำงานอยู่บนเซิร์ฟเวอร์ที่ให้บริการหลัก (Core Service) ของธุรกิจขององค์กร หากมีการรีสตาร์ตเครื่องเซิร์ฟเวอร์แล้วส่งผลให้บางเซอร์วิสในเครื่องเซิร์ฟเวอร์ไม่ทำงาน จะส่งผลกระทบต่อการดำเนินธุรกิจ
3. เมื่อยกระดับเวอร์ชันซอฟต์แวร์แล้ว ซอฟต์แวร์อาจจะส่งผลกระทบต่อระบบอื่น
4. ซอฟต์แวร์ที่ติดตั้งในเครื่องคอมพิวเตอร์ยังใช้งานได้ดีจึงไม่เห็นความจำเป็นที่จะต้องยกระดับเวอร์ชันซอฟต์แวร์ [1]
5. การที่ซอฟต์แวร์มีหน้าที่การทำงานที่ดูเหมือนไม่มีส่วนเกี่ยวข้องกับความมั่นคง ทำให้ผู้ใช้งานไม่เข้าใจถึงเหตุผลที่ต้องยกระดับเวอร์ชันของซอฟต์แวร์ [1]

อย่างไรก็ตามซอฟต์แวร์เหล่านี้อาจจะมีช่องโหว่ประกอบอยู่ด้วย ซึ่งช่องโหว่เหล่านี้เป็นความความผิดพลาดในซอฟต์แวร์ที่ทำให้แฮกเกอร์สามารถเข้าถึงระบบหรือเครือข่ายได้โดยตรง [2] ดังนั้นหากช่องโหว่เหล่านี้ถูกใช้ประโยชน์จากผู้โจมตี (Attacker) อาจจะก่อให้เกิดผลกระทบในด้านความ

มั่นคงของระบบและข้อมูลภายในองค์กรถูกเปิดเผย รวมไปถึงอาจก่อให้เกิดผลกระทบกับการดำเนินธุรกิจขององค์กรได้

การปรับปรุงซอฟต์แวร์ที่เกี่ยวข้องกับความมั่นคงจึงเป็นหนึ่งในกลไกการป้องกันคอมพิวเตอร์ที่ดีที่สุด [1] ดังนั้นจากปัญหาที่กล่าวมาข้างต้นผู้วิจัยจึงเกิดคำถามว่าจะสามารถช่วยผู้ใช้งานหรือผู้ดูแลระบบคอมพิวเตอร์ภายในองค์กร ในการพิจารณาการยกระดับเวอร์ชันซอฟต์แวร์ได้อย่างไร ผู้วิจัยจึงเกิดแนวคิดที่จะพัฒนาเครื่องมือช่วยประเมินช่องโหว่ด้านความมั่นคงเพื่อการพิจารณายกระดับเวอร์ชันของซอฟต์แวร์ ผู้วิจัยจะทำการประเมินช่องโหว่ของซอฟต์แวร์ที่ติดตั้งอยู่ในเครื่องคอมพิวเตอร์ซึ่งอาจเป็นเครื่องคอมพิวเตอร์ของผู้ใช้งานหรือเป็นเครื่องคอมพิวเตอร์ขององค์กร และเปรียบเทียบกับช่องโหว่ของเวอร์ชันล่าสุดของซอฟต์แวร์เหล่านั้น โดยอิงระบบการให้คะแนนช่องโหว่ซีวีเอสเอส และรายงานความรุนแรงของผลกระทบของช่องโหว่ของซอฟต์แวร์ทั้งสองเวอร์ชัน เพื่อแนะนำการยกระดับเวอร์ชันเพื่อเพิ่มความมั่นคงหากซอฟต์แวร์เวอร์ชันล่าสุดมีความรุนแรงของผลกระทบน้อยกว่าเวอร์ชันที่ติดตั้งอยู่ปัจจุบัน การประเมินช่องโหว่นี้จะเป็นข้อมูลสนับสนุนให้กับผู้ใช้งานหรือผู้ดูแลระบบใช้ประกอบการพิจารณายกระดับหรือไม่ยกระดับเวอร์ชันของซอฟต์แวร์ได้อย่างเหมาะสม

1.2. วัตถุประสงค์ของการวิจัย

เพื่อพัฒนาเครื่องมือช่วยประเมินช่องโหว่ด้านความมั่นคงเพื่อการยกระดับเวอร์ชันของซอฟต์แวร์

1.3. ขอบเขตการวิจัย

1. ฐานข้อมูลที่ใช้ค้นหารายการช่องโหว่ในซอฟต์แวร์ จะใช้ฐานข้อมูลจากเอ็นวีดี
2. รายชื่อซอฟต์แวร์ที่นำมาเปรียบเทียบจะต้องเป็นซอฟต์แวร์ที่มีในฐานข้อมูลเอ็นวีดีเท่านั้น
3. ช่องโหว่ที่ใช้ในการพิจารณาจะอ้างอิงจากช่องโหว่ที่มาจากรายการซีวีอีเท่านั้น
4. รองรับทั้งการเปรียบเทียบซีวีเอสเอส เวอร์ชัน 2 และซีวีเอสเอส เวอร์ชัน 3
5. คะแนนซีวีเอสเอสที่นำมาเปรียบเทียบจะต้องเป็นเวอร์ชันเดียวกัน
6. คะแนนจากกลุ่มตัววัดพื้นฐานจะใช้คะแนนที่ได้จากฐานข้อมูลของเอ็นวีดี ทั้งซีวีเอสเอส เวอร์ชัน 2 และซีวีเอสเอส เวอร์ชัน 3
7. คะแนนจากกลุ่มตัววัดตามเวลาจะใช้คะแนนที่ได้จากการเรียกใช้เอพีไอของไอบีเอ็ม เอกซ์เอฟอี ทั้งซีวีเอสเอส เวอร์ชัน 2 และซีวีเอสเอส เวอร์ชัน 3

8. คะแนนจากกลุ่มตัววัดตามสภาพแวดล้อมจะใช้คะแนนที่ได้จาก NIST Special Publication 800-60 [3] ทั้งซีวีเอสเอส เวอร์ชัน 2 และซีวีเอสเอส เวอร์ชัน 3
9. สแกนรายชื่อซอฟต์แวร์และเวอร์ชันโดยการสแกนวินโดวส์รีจิสทรี
10. สแกนเวอร์ชันของระบบปฏิบัติการวินโดวส์โดยการสแกนวินโดวส์รีจิสทรี
11. เครื่องมือสามารถแสดงคะแนนความรุนแรงของช่องโหว่ในซอฟต์แวร์เวอร์ชันที่ติดตั้งในเครื่องคอมพิวเตอร์ได้
12. เครื่องมือสามารถแสดงคะแนนความรุนแรงของช่องโหว่ในซอฟต์แวร์เวอร์ชันล่าสุดที่มีในฐานข้อมูลช่องโหว่ได้
13. เครื่องมือสามารถแสดงคะแนนความรุนแรงของช่องโหว่ทั้งหมดของเครื่องคอมพิวเตอร์ได้
14. เครื่องมือสามารถแนะนำการยกระดับหรือไม่จำเป็นต้องยกระดับเวอร์ชันของซอฟต์แวร์
15. เครื่องมือสามารถแสดงการเปลี่ยนแปลงของคะแนนความรุนแรงหากมีการยกระดับเวอร์ชันซอฟต์แวร์ต่างๆ
16. เครื่องมือไม่สามารถค้นหาซอฟต์แวร์ที่ไม่ปรากฏในวินโดวส์รีจิสทรีได้อัตโนมัติ
17. เครื่องมือไม่สามารถเปรียบเทียบคะแนนซีวีเอสเอสในกรณีที่มีการเปลี่ยนชื่อซอฟต์แวร์ หรือเป็นซอฟต์แวร์ประเภทเดียวกันแต่ผู้ผลิตต่างรายกันได้
18. เครื่องมือสามารถให้ผู้ใช้ระบุชื่อของซอฟต์แวร์อื่นที่ต้องการเปรียบเทียบคะแนนซีวีเอสเอสกับซอฟต์แวร์เวอร์ชันที่มีในเครื่องคอมพิวเตอร์ได้

1.4. ประโยชน์ที่คาดว่าจะได้รับ

1. ได้เครื่องมือที่ช่วยผู้ดูแลระบบในการประเมินช่องโหว่ด้านความมั่นคง
2. ได้เครื่องมือที่ช่วยผู้ดูแลระบบในการแนะนำการยกระดับเวอร์ชันซอฟต์แวร์ได้โดยสามารถระบุโอกาสในการเพิ่มความมั่นคงของซอฟต์แวร์

1.5. วิธีดำเนินงานวิจัย

1. ศึกษางานวิจัยที่เกี่ยวข้อง
2. ศึกษาข้อมูลช่องโหว่ของเอ็นวีดี
3. ศึกษาซีวีเอสเอส เวอร์ชัน 2 และเวอร์ชัน 3
4. ศึกษาข้อมูลช่องโหว่ของ ไอบีเอ็ม เอกซ์เอฟอี
5. ศึกษา NIST Special Publication 800-60 Volume II

6. จัดทำโครงร่างวิทยานิพนธ์
7. ออกแบบเครื่องมือและวิธีการประเมินผล
8. พัฒนาเครื่องมือ
9. ทดสอบและประเมินผลเครื่องมือ
10. สรุปผลการพัฒนาเครื่องมือ
11. เรียงเรียบและจัดทำวิทยานิพนธ์
12. จัดทำบทความทางวิชาการ

1.6. ผลงานตีพิมพ์

ส่วนหนึ่งของงานวิจัยนี้ได้รับการตอบรับเพื่อตีพิมพ์เป็นบทความวิจัยในหัวข้อเรื่อง “Security Vulnerability Assessment for Software Version Upgrade” โดย Sirikwan Treetippayaruk and Twittie Senivongse ในงานประชุมวิชาการ 18th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD) ซึ่งจัดขึ้นโดย IEEE Computer Society และ International Association for Computer and Information Science (ACIS) ณ เมืองคานาซาว่า (Kanazawa) ประเทศญี่ปุ่น ระหว่างวันที่ 26 –28 มิถุนายน 2560

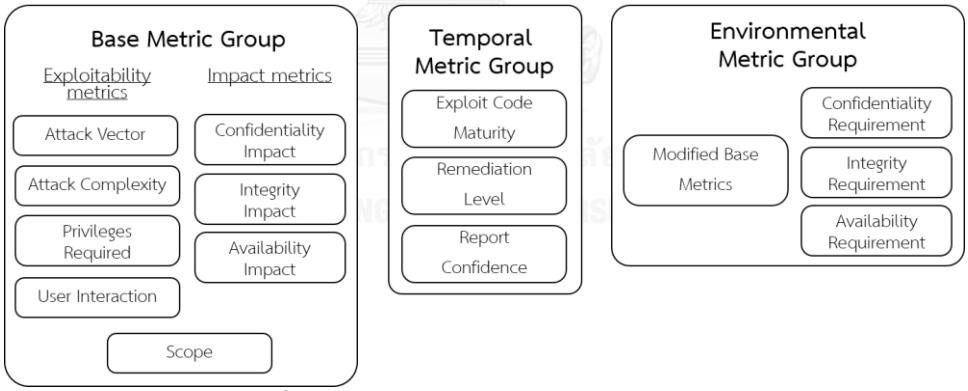
บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1. ทฤษฎีที่เกี่ยวข้อง

2.1.1. ซีวีเอสเอส

ซีวีเอสเอส [4] (CVSS ย่อมาจาก Common Vulnerability Scoring System) เป็นระบบการให้คะแนนช่องโหว่ของซอฟต์แวร์และเครือข่ายซึ่งเป็นมาตรฐานที่ใช้กันในวงกว้างทั่วโลก จัดทำโดย FIRST.org หรือ Forum of Incident Response and Security Teams คะแนนซีวีเอสเอสจะแสดงให้เห็นถึงความรุนแรงของผลกระทบของช่องโหว่ที่มีต่อความมั่นคงของระบบ ข้อมูลคะแนนซีวีเอสเอสที่เผยแพร่อยู่ในปัจจุบันเป็นข้อมูลเวอร์ชัน 2 แต่ในเดือนมิถุนายน ปี 2015 ทาง FIRST.org ได้เริ่มประกาศใช้ซีวีเอสเอสเวอร์ชัน 3 ออกมา ทำให้ข้อมูลช่องโหว่ที่พบก่อนเดือนมิถุนายน ปี 2015 จะเป็นข้อมูลคะแนนเวอร์ชัน 2 แต่ข้อมูลช่องโหว่ที่พบหลังจากนั้นจะมีคะแนนทั้งเวอร์ชัน 2 และ 3

ซีวีเอสเอสเวอร์ชัน 3 ประกอบด้วยกลุ่มของตัววัด 3 กลุ่ม ได้แก่ กลุ่มตัววัดพื้นฐาน (Base Metric Group) , กลุ่มตัววัดตามเวลา (Temporal Metric Group) และ กลุ่มตัววัดตามสภาพแวดล้อม (Environmental Metric Group) ดังรูปที่ 2.1 โดยมีรายละเอียดดังนี้



รูปที่ 2.1 กลุ่มตัววัดของซีวีเอสเอสเวอร์ชัน 3

1. กลุ่มตัววัดพื้นฐาน (Base Metric Group) แทนคุณลักษณะที่แท้จริง (Intrinsic Characteristics) ของช่องโหว่โดยคะแนนจะไม่เปลี่ยนแปลงตามเวลาหรือสภาพแวดล้อมของผู้ใช้งาน กลุ่มตัววัดพื้นฐานจะประกอบด้วยตัววัดย่อย ๆ อีก 3 กลุ่ม คือ

a. **Exploitability Metrics** เป็นกลุ่มตัววัดที่สะท้อนความง่ายของเทคนิคที่สามารถใช้ประโยชน์จากช่องโหว่ได้ ตัววัดที่อยู่ในกลุ่มนี้ประกอบไปด้วย

- **Attack Vector (AV)** เป็นตัววัดที่แทนวิธีการที่ผู้โจมตีสามารถเข้าถึงช่องโหว่เพื่อใช้ประโยชน์จากช่องโหว่ เช่น เข้าถึงผ่านทาง Network, Adjacent, Local หรือ Physical
- **Attack Complexity (AC)** เป็นตัววัดที่แสดงถึงความซับซ้อนในการใช้ประโยชน์จากช่องโหว่ของผู้โจมตี กล่าวคือในการโจมตีจำเป็นต้องมีการเตรียมการหรือเตรียมสภาพแวดล้อมให้เหมาะสมก่อนการโจมตี เช่น ต้องมีการเปลี่ยนแปลง Configuration ก่อนโจมตี หรือต้อง Inject เข้าระบบเครือข่ายก่อนการโจมตี หรือไม่เพียงใด
- **Privileges Required (PR)** เป็นตัววัดที่แสดงถึงสิทธิ์ของผู้โจมตีที่จะสามารถใช้ประโยชน์จากช่องโหว่ได้ เช่น ไม่ต้องมีสิทธิ์ใด ๆ หรือ ต้องมีสิทธ์ หรือต้องมีสิทธ์เป็นผู้ดูแลระบบ
- **User Interaction (UI)** เป็นตัววัดที่แสดงถึงความจำเป็นของผู้โจมตีในการมี Interaction ก่อนใช้ประโยชน์จากช่องโหว่ เช่น การโจมตีกระทำได้เฉพาะในระหว่างที่ผู้ดูแลระบบกำลังทำการติดตั้งซอฟต์แวร์อยู่

b. **Impact Metrics** เป็นกลุ่มตัววัดที่สะท้อนผลกระทบโดยตรงจากการใช้ประโยชน์จากช่องโหว่ได้สำเร็จ ประกอบไปด้วย

- **Confidentiality Impact (C)** เป็นตัววัดที่แสดงถึงผลกระทบต่อการสูญเสียการรักษาความลับเมื่อผู้โจมตีใช้ประโยชน์จากช่องโหว่ได้สำเร็จ ซึ่งการรักษาความลับหมายถึง การจำกัดการเข้าถึงข้อมูลและเปิดเผยข้อมูลกับผู้ที่ได้รับอนุญาตเท่านั้น
- **Integrity Impact (I)** เป็นตัววัดที่แสดงถึงผลกระทบต่อการสูญเสียบูรณภาพเมื่อผู้โจมตีใช้ประโยชน์จากช่องโหว่ได้สำเร็จ ซึ่งบูรณภาพหมายถึงความน่าเชื่อถือและความถูกต้องของข้อมูล
- **Availability Impact (A)** เป็นตัววัดที่แสดงถึงผลกระทบต่อการสูญเสียสภาพพร้อมใช้งานเมื่อผู้โจมตีใช้ประโยชน์จากช่องโหว่ได้สำเร็จ ซึ่งสภาพพร้อมใช้งานหมายถึง ความพร้อมในการเข้าถึงข้อมูล

c. **Scope (S)** เป็นตัววัดที่แสดงให้เห็นว่าเมื่อผู้โจมตีใช้ประโยชน์จากช่องโหว่ได้สำเร็จภายในขอบเขตการอนุญาต (Authorization Scope) หนึ่ง ๆ แล้ว การโจมตีนั้นส่งผล

กระทบต่อไปยังขอบเขตการอนุญาตอื่นด้วยหรือไม่ เช่น การโจมตีเครื่องเสมือน (Virtual Machine) หนึ่ง ๆ ส่งผลกระทบต่อไปยังเครื่องโฮสต์หรือไม่

2. กลุ่มตัววัดตามเวลา (Temporal Metric Group) แทนคุณลักษณะของช่องโหว่ที่เปลี่ยนแปลงตามเวลา แต่ไม่เปลี่ยนแปลงตามสภาพแวดล้อมของผู้ใช้งาน จะประกอบไปด้วยตัววัดดังนี้

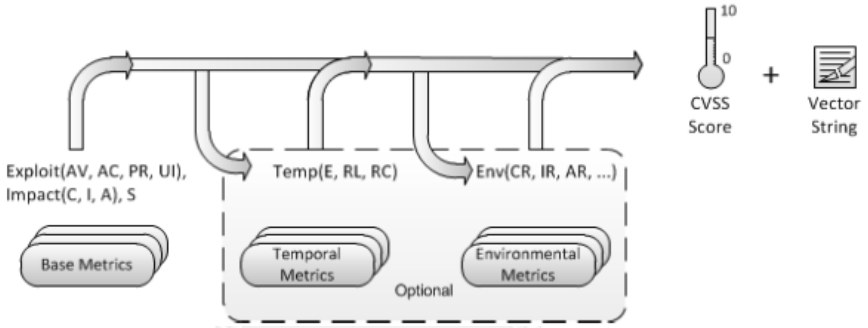
- **Exploit Code Maturity (E)** เป็นตัววัดที่แสดงถึงโอกาส (Likelihood) ที่ช่องโหว่จะถูกโจมตี มักจะขึ้นกับสถานะปัจจุบันของเทคนิคการโจมตี
- **Remediation Level (RL)** เป็นตัววัดที่แสดงถึงการแก้ไขช่องโหว่เมื่อเวลาผ่านไป เช่น มีการเผยแพร่ Workaround, Hotfix, Patch ออกมา
- **Report Confidence (RC)** เป็นตัววัดที่แสดงถึงความเชื่อมั่นในรายละเอียดของช่องโหว่ เช่น เมื่อเวลาผ่านไป ผู้ขายผลิตภัณฑ์ซอฟต์แวร์ทำการยืนยันการมีอยู่ของช่องโหว่

3. กลุ่มตัววัดตามสภาพแวดล้อม (Environmental Metric Group) แทนคุณลักษณะเฉพาะของช่องโหว่ที่เปลี่ยนแปลงตามสภาพแวดล้อมของผู้ใช้งาน จะประกอบไปด้วยตัววัดดังนี้

- **Security Requirements (CR, IR, AR)** ประกอบไปด้วย Confidentiality Requirement (CR) , Integrity Requirement (IR) และ Availability Requirement (AR) เป็นตัววัดที่ช่วยให้ปรับเปลี่ยนผลกระทบจากการสูญเสียการรักษาความลับ ผลกระทบจากการสูญเสียบูรณภาพ และผลกระทบจากการสูญเสียสภาพพร้อมใช้งาน ให้ตรงกับสภาพแวดล้อมขององค์กรของผู้ใช้งาน เช่น หากซอฟต์แวร์ที่มีช่องโหว่นั้นเป็นซอฟต์แวร์ที่สนับสนุนฟังก์ชันงานทางธุรกิจขององค์กร โดยที่สภาพพร้อมใช้งานของฟังก์ชันงานนั้นมีความสำคัญมากต่อธุรกิจ องค์กรสามารถกำหนดให้ AR มีค่าสูงกว่าเมื่อเทียบกับ CR และ IR
- **Modified Base Metrics** เป็นตัววัดที่ช่วยให้ปรับเปลี่ยนกลุ่มตัววัดพื้นฐานให้ตรงตามสภาพแวดล้อมของผู้ใช้งานมากขึ้น เช่น ในกรณีที่มีการปรับสภาพแวดล้อมแล้ว การปรับมีผลต่อ การใช้ประโยชน์จากช่องโหว่ (Exploitability) ต่อผลกระทบจากการใช้ประโยชน์ (Impact) หรือ ต่อการเปลี่ยนขอบเขต การอนุญาต (Scope) องค์กรสามารถปรับค่ากลุ่มตัววัดพื้นฐานให้เหมาะสมได้

ในการคำนวณคะแนนซีวีเอสเอส กลุ่มตัววัดตามเวลาและกลุ่มตัววัดตามสภาพแวดล้อม เป็นกลุ่มตัววัดที่เป็นทางเลือก (Optional) ซึ่งผู้ใช้งานไม่จำเป็นต้องนำกลุ่มตัววัด 2 กลุ่มนี้มาคำนวณก็ได้ แต่ถ้าหากนำกลุ่มตัววัด 2 กลุ่มนี้มาร่วมคำนวณด้วยจะสะท้อนให้เห็นถึงความรุนแรงที่เกิดจากช่องโหว่ณ ปัจจุบัน ในสภาพแวดล้อมของผู้ใช้งานได้ถูกต้องมากขึ้น

แต่ละกลุ่มตัววัดจะมีคะแนนตั้งแต่ 0 ถึง 10 และถูกนำมาคำนวณร่วมกันทีละกลุ่มตามรูปที่ 2.2 โดยที่คะแนนซีวีเอสเอสจะเป็นคะแนนของกลุ่มตัววัดสุดท้ายที่นำมาคำนวณ และมีค่าตั้งแต่ 0 ถึง 10 เช่นกัน คะแนนซีวีเอสเอสที่มีค่าน้อยจะหมายถึงช่องโหว่มีความรุนแรงน้อย และค่ามากหมายถึงช่องโหว่มีความรุนแรงมาก ในงานวิจัยนี้จะคำนวณคะแนนซีวีเอสเอสจากทั้ง 3 กลุ่มตัววัด กล่าวคือการคำนวณคะแนนของกลุ่มตัววัดตามเวลาจะนำคะแนนของกลุ่มตัววัดพื้นฐานมาร่วมคำนวณด้วย และการคำนวณคะแนนของกลุ่มตัววัดตามสภาพแวดล้อมจะนำคะแนนของกลุ่มตัววัดตามเวลามาคำนวณด้วย ซึ่งคะแนนซีวีเอสเอสจะเป็นคะแนนของกลุ่มตัววัดตามสภาพแวดล้อมนั่นเอง



รูปที่ 2.2 การคำนวณคะแนนซีวีเอสเอสจากกลุ่มตัววัด

เมื่อคำนวณคะแนนซีวีเอสเอสได้แล้วคะแนนที่ได้จะเป็นคะแนนในเชิงปริมาณซึ่งสามารถเปลี่ยนให้เป็นคะแนนเชิงคุณภาพได้ โดยนำคะแนนซีวีเอสเอสมาจับคู่เข้ากับตารางที่ 2.1 เช่น คำนวณคะแนนซีวีเอสเอสของช่องโหว่ได้ 4.5 ช่องโหว่นี้จะมีความรุนแรงอยู่ที่ระดับ Medium

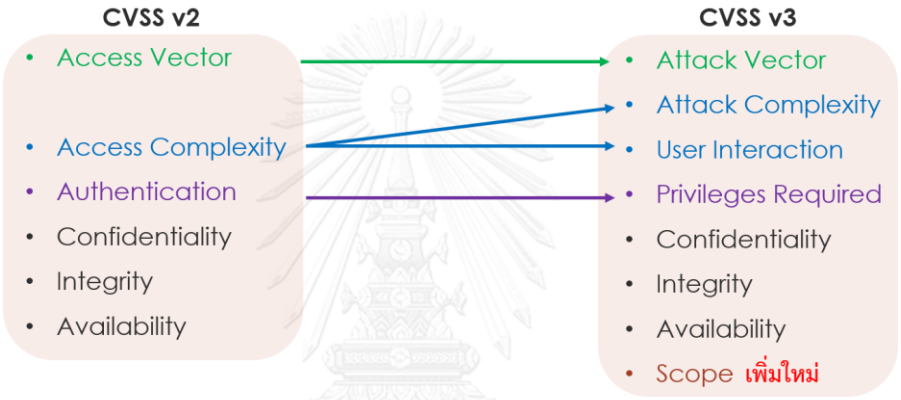
ตารางที่ 2.1 ระดับความรุนแรงจากคะแนนซีวีเอสเอส

ระดับ	คะแนนซีวีเอสเอส
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

2.1.1.1. ความแตกต่างของซีวีเอสเอส เวอร์ชัน 2 และ 3

ในซีวีเอสเอสเวอร์ชัน 2 [5] ประกอบด้วยกลุ่มของตัววัด 3 กลุ่ม ได้แก่ กลุ่มตัววัดพื้นฐาน กลุ่มตัววัดตามเวลา และกลุ่มตัววัดตามสภาพแวดล้อม เช่นเดียวกันกับซีวีเอสเอส เวอร์ชัน 3 สิ่งที่ต่างกัน คือ ตัววัดย่อย ๆ ในกลุ่มตัววัดพื้นฐาน และกลุ่มตัววัดตามสภาพแวดล้อม

ในกลุ่มตัววัดพื้นฐานของซีวีเอสเอส เวอร์ชัน 3 ได้มีการเพิ่มตัววัดใหม่ คือ Scope (S) ส่วนตัววัด Attack Complexity (AC) และ User Interaction (UI) ได้มาจากการแยกตัววัดของ Access Complexity ของซีวีเอสเอส เวอร์ชัน 2 ออกมา และตัววัด Attack Vector (AV) และ Privileges Required (PR) เปลี่ยนชื่อมาจากตัววัด Access Vector และ Authentication ของซีวีเอสเอส เวอร์ชัน 2 ตามลำดับ ดังรูปที่ 2.3



รูปที่ 2.3 ความแตกต่างของกลุ่มตัววัดพื้นฐานของซีวีเอสเอส เวอร์ชัน 2 และ 3

ในกลุ่มตัววัดตามเวลาไม่มีการเปลี่ยนแปลง และในกลุ่มตัววัดตามสภาพแวดล้อม ในส่วนของ Security Requirements (CR, IR, AR) ไม่มีการเปลี่ยนแปลง แต่ได้มีการเพิ่ม Modified Base Metrics เข้ามาในซีวีเอสเอส เวอร์ชัน 3 และตัดตัววัด Collateral Damage Potential และTarget Distribution ในซีวีเอสเอส เวอร์ชัน 2 ออก ดังรูปที่ 2.4

รูปที่ 2.4 ความแตกต่างของกลุ่มตัวตามสภาพแวดล้อมของซีวีเอสเอส เวอร์ชัน 2 และ 3

2.1.2. เอ็นวีดี

เอ็นวีดี [6] (NVD ย่อมาจาก National Vulnerability Database) เป็นแหล่งรวบรวมข้อมูลช่องโหว่ทางด้านซอฟต์แวร์ของรัฐบาลกลางของประเทศสหรัฐอเมริกา เอ็นวีดีประกอบด้วยฐานข้อมูลของ

รายการตรวจสอบด้านความมั่นคง (Security Checklists) ฐานข้อมูลเกี่ยวกับความมั่นคงที่เกี่ยวข้องกับความบกพร่องของซอฟต์แวร์ ฐานข้อมูลเกี่ยวกับการ ตั้งค่าระบบที่ผิดพลาด (Misconfigurations) ฐานข้อมูลเกี่ยวกับชื่อของซอฟต์แวร์ (Product Names) และฐานข้อมูลเกี่ยวกับตัววัดผลกระทบ (Impact Metric)

ในปัจจุบันเอ็นวีดีมีจำนวนช่องโหว่ภายใต้มาตรฐานการตั้งชื่อช่องโหว่ด้วยซีวีอี (Common Vulnerabilities and Exposures หรือ CVE) [2] ทั้งหมด 80,162 รายการ พร้อมทั้งประเมินความรุนแรงของช่องโหว่เหล่านี้ด้วยคะแนนกลุ่มตัววัดพื้นฐานของซีวีเอสเอส เวอร์ชัน 2 และหลังจากเดือนมิถุนายน ปี 2015 ทางเอ็นวีดีเริ่มมีการประเมินความรุนแรงของช่องโหว่ด้วยคะแนนกลุ่มตัววัดพื้นฐานของซีวีเอสเอส เวอร์ชัน 3 แล้ว

2.1.3. ไอบีเอ็ม เอกซ์เอฟอี

ไอบีเอ็ม เอกซ์เอฟอี [7] (IBM XFE ย่อมาจาก IBM X-Force Exchange) เป็นแพลตฟอร์มบนคลาวด์ (Cloud-Based Platform) ที่แบ่งปันข้อมูลด้านความมั่นคงของระบบให้แก่สมาชิกคนอื่น ๆ ในชุมชนเอกซ์เอฟอี และสามารถค้นหาข้อมูลโดยใช้ IPv4, IPv6 หรือ ยูอาร์แอล โดยจะบอกคะแนนความเสี่ยง (Risk Score) จำนวนมัลแวร์ สามารถค้นหาโดยชื่อแอปพลิเคชัน ค้นหาช่องโหว่โดยใช้รายการซีวีอี และสามารถค้นหามัลแวร์ของไฟล์ที่อัปโหลดเข้าไปได้ด้วย

ข้อมูลช่องโหว่มาจากฐานข้อมูล X-Force [8] ซึ่งเป็นหนึ่งในฐานข้อมูลที่เก่าที่สุดที่เปิดเผยและพร้อมใช้งานในโลก ในปัจจุบันมีข้อมูลช่องโหว่มากกว่า 88,000 รายการ นอกจากนี้ยังมีตัววัดมาตรฐานที่เกี่ยวข้องกับช่องโหว่ คือซีวีเอสเอส ในรายการซีวีอีจะมีข้อมูลการประเมินผลกระทบของช่องโหว่ด้วยคะแนนซีวีเอสเอส 2 กลุ่ม คือ กลุ่มตัววัดพื้นฐานและกลุ่มตัววัดตามเวลา โดยกลุ่มตัววัดพื้นฐานจะมีทั้งคะแนนซีวีเอสเอสทั้ง 2 เวอร์ชัน หากเป็นรายการช่องโหว่ตั้งแต่ปี 2016 บางรายการจะให้คะแนนกลุ่มตัววัดพื้นฐานด้วยซีวีเอสเอส เวอร์ชัน 3

2.1.4. NIST Special Publication 800-60 Volume II

NIST Special Publication 800-60 Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories [3] เป็นเอกสารที่พัฒนาโดย National Institute of Standards and Technology หรือเรียกย่อ ๆ ว่า NIST เอกสารนี้จัดทำขึ้นตามความต้องการของสำนักงบประมาณของประเทศสหรัฐอเมริกาและจัดเตรียมไว้ใช้งานกับรัฐบาลกลางรวมไปถึงองค์กรที่ไม่แสวงหาผลกำไรของอเมริกาด้วย มีจุดประสงค์เพื่อกำหนดประเภทสารสนเทศ (Information Type) ของระบบสารสนเทศภายในองค์กร และระดับผลกระทบต่อองค์กร

หากสารสนเทศนั้น ๆ สูญเสียองค์ประกอบด้านความมั่นคงไป ได้แก่ ผลกระทบจากการสูญเสียการรักษาความลับ (Confidentiality Impact) ผลกระทบจากการสูญเสียบูรณภาพ (Integrity Impact) และ ผลกระทบจากการสูญเสียสภาพพร้อมใช้งาน (Availability Impact) ทั้งนี้เพื่อกำหนดรายการการควบคุมด้านความมั่นคง (Security Controls) ที่องค์กรควรพัฒนา ให้กับระบบสารสนเทศต่าง ๆ ของตน โดยระดับของผลกระทบจะแบ่งออกเป็น 3 ระดับ คือ High Medium และ Low ตัวอย่างของประเภทสารสนเทศในองค์กรและระดับผลกระทบต่อองค์กรจากการสูญเสียองค์ประกอบด้านความมั่นคงแสดงดังตารางที่ 2.2 โดยระดับผลกระทบที่เป็นตัวอักษรเอียง หมายถึง ระดับผลกระทบอาจเปลี่ยนแปลงได้หากมีเงื่อนไขบางอย่างเกิดขึ้นกับระบบสารสนเทศขององค์กร

ตารางที่ 2.2 ตัวอย่างระดับผลกระทบตามประเภทสารสนเทศ

	Loss of Confidentiality Impact	**Loss of Integrity Impact**	**Loss of Availability Impact**
Administrative Management			
Help Desk Services	*Low*	*Low*	*Low*
Security Management	*Moderate*	**Moderate**	*Low*
Workplace Policy Development and Management	**Low**	**Low**	**Low**
Financial Management			
Asset and Liability Management	*Low*	*Low*	**Low**
Reporting and Information	*Low*	**Moderate**	**Low**
Funds Control	*Moderate*	**Moderate**	**Low**
Accounting	*Low*	*Moderate*	**Low**
Payments	*Low*	*Moderate*	*Low*

2.2. งานวิจัยที่เกี่ยวข้อง

2.2.1. Betrayed By Updates: How Negative Experiences Affect Future Security

งานวิจัย [1] ได้ทำการสัมภาษณ์นักศึกษานอกสาขาวิชาวิทยาการคอมพิวเตอร์ซึ่งใช้ระบบปฏิบัติการวินโดวส์ ในเรื่องการยกระดับเวอร์ชันของซอฟต์แวร์ และพบว่ามี 3 สาเหตุหลักที่ทำให้ผู้ใช้งานระบบปฏิบัติการวินโดวส์ไม่ยอมยกระดับเวอร์ชันของซอฟต์แวร์ คือ

1. ส่วนต่อประสานกับผู้ใช้งานเปลี่ยน เมื่อส่วนต่อประสานกับผู้ใช้งานเปลี่ยนทำให้กระทบต่อการทำงานของผู้ใช้งาน ส่งผลให้ต้องมีการเรียนรู้การใช้งานซอฟต์แวร์ใหม่ ซึ่งผู้ใช้งานไม่เต็มใจที่จะเรียนรู้การใช้งานซอฟต์แวร์ใหม่

2. ไม่เข้าใจว่าทำไมต้องยกระดับเวอร์ชันของซอฟต์แวร์ ไม่เข้าใจว่าซอฟต์แวร์นั้นคืออะไร ใช้ทำงานอะไร และไม่ทราบว่าซอฟต์แวร์นั้นเป็นซอฟต์แวร์ที่ทำงานให้กับโปรแกรมอื่น ๆ เช่น JAVA โดยส่วนใหญ่การยกระดับเวอร์ชันของซอฟต์แวร์จะทำกับซอฟต์แวร์ที่ใช้งานบ่อย ๆ เพราะการยกระดับจะทำให้ได้ใช้ฟีเจอร์ล่าสุดและสามารถที่จะมีปฏิสัมพันธ์กับผู้ใช้งานซอฟต์แวร์เวอร์ชันเดียวกันได้ง่าย ในส่วนของซอฟต์แวร์ที่ถูกใช้งานน้อย หรือไม่ใช้งานเลยจะมีแนวโน้มในการยกระดับเวอร์ชันซอฟต์แวร์น้อย

3. ซอฟต์แวร์ยังทำงานและตอบสนองความต้องการได้จึงไม่จำเป็นต้องยกระดับเวอร์ชันของซอฟต์แวร์ เนื่องจากการยกระดับเวอร์ชันของซอฟต์แวร์ส่วนใหญ่จะให้ข้อมูลน้อยจนถึงไม่ให้เลย ดังนั้นผู้ใช้งานจึงไม่เต็มใจที่จะเสี่ยงกับการเปลี่ยนแปลงของส่วนต่อประสานกับผู้ใช้งาน ความเสี่ยงที่ฟีเจอร์ที่จำเป็นจะถูกลบออกจากซอฟต์แวร์ หรือความเสี่ยงที่ซอฟต์แวร์จะไม่ทำงาน สำหรับซอฟต์แวร์ที่มีฟังก์ชันการทำงานที่ดูเหมือนไม่มีส่วนเชื่อมโยงกับความมั่นคงของระบบ เช่น Adobe Reader ผู้ถูกสัมภาษณ์จะไม่เข้าใจว่าทำไมถึงจำเป็นต้องยกระดับเวอร์ชันของซอฟต์แวร์นี้ เพราะซอฟต์แวร์นี้ใช้เพียงแค่อ่านไฟล์ PDF เท่านั้น

อีกสาเหตุหนึ่งที่ผู้ใช้งานไม่ยกระดับเวอร์ชันของซอฟต์แวร์คือเจ้าของผลิตภัณฑ์ซอฟต์แวร์บอกรายละเอียดการเปลี่ยนแปลงที่มีในเวอร์ชันใหม่ไม่ละเอียด ผู้ใช้งานจึงไม่เห็นความแตกต่างที่ชัดเจนว่าหากยกระดับเวอร์ชันของซอฟต์แวร์ใหม่แล้ว การแก้ไขจุดบกพร่อง (Fix Bugs) หรือการปรับความมั่นคง (Security Update) จะดีขึ้นอย่างไร

จากงานวิจัยนี้ทำให้ทราบว่าอีกหนึ่งสาเหตุที่ทำให้ผู้ใช้งานไม่ยกระดับเวอร์ชันของซอฟต์แวร์เป็นเพราะผู้ใช้งานไม่เห็นความแตกต่างที่ชัดเจนในเรื่องของการปรับปรุงความมั่นคงเมื่อติดตั้งเวอร์ชันใหม่ ผู้วิจัยจึงได้แนวคิดในการรายงาน การเปรียบเทียบเวอร์ชันของซอฟต์แวร์ในเรื่องช่องโหว่ที่มีอยู่ เพื่อเป็นข้อมูลประกอบการตัดสินใจยกระดับเวอร์ชัน

2.2.2. เครื่องมือช่วยบริหารความปลอดภัยโดยใช้ฐานข้อมูลจุดอ่อนระบบเปิด

งานวิจัย [9] ได้เสนอเครื่องมือช่วยบริหารความปลอดภัยโดยใช้ฐานข้อมูลจุดอ่อนระบบเปิด โดยเครื่องมือนี้จะสแกนรายชื่อซอฟต์แวร์ที่มีอยู่ในเครื่องคอมพิวเตอร์ด้วยซอฟต์แวร์โอซีเอส อินเวนทอรี (OCS Inventory ย่อมาจาก Open Computer and Software Inventory) และจะเก็บข้อมูลรายชื่อซอฟต์แวร์และเวอร์ชันที่ต้องการตรวจสอบรายการช่องโหว่ จากนั้นจะทำการค้นหาช่องโหว่จากฐานข้อมูลช่องโหว่ระบบเปิดว่ารายการซอฟต์แวร์เวอร์ชันที่ค้นหามานั้น มีช่องโหว่รายการใดบ้าง เพื่อให้ผู้ดูแลระบบสามารถจัดการรายการช่องโหว่ที่มีในเครื่องคอมพิวเตอร์ได้

งานวิจัยดังกล่าวทำการค้นหาช่องโหว่ของซอฟต์แวร์เวอร์ชันที่ติดตั้งในเครื่องคอมพิวเตอร์เท่านั้น แต่ไม่มีการประเมินผลกระทบของช่องโหว่ที่ค้นพบ ทำให้ไม่ทราบว่าช่องโหว่รายการใดรุนแรงมากน้อยเพียงใด หากต้องการจะแก้ไขช่องโหว่นั้นจะทำได้ยาก เพราะในความเป็นจริงแล้วไม่สามารถแก้ไขช่องโหว่ได้ทุกช่องโหว่ จึงควรที่จะประเมินผลกระทบของช่องโหว่ด้วยเพื่อให้สามารถเลือกแก้ไขช่องโหว่ที่รุนแรงที่สุดก่อน ผู้วิจัยจะใช้แนวทางในการตรวจสอบรายชื่อซอฟต์แวร์ที่ติดตั้งอยู่ในเครื่องคอมพิวเตอร์และช่องโหว่ที่มีอยู่ในซอฟต์แวร์เหล่านั้นจากงานวิจัยนี้ แต่จะทำการประเมินความรุนแรงของช่องโหว่และเปรียบเทียบกับเวอร์ชันล่าสุดของซอฟต์แวร์นั้น ๆ ด้วย เพื่อเป็นข้อมูลให้กับผู้ใช้งานหรือผู้ดูแลระบบ

2.2.3. Enhancing Service-Side QoS Monitoring for Web Services

งานวิจัย [10] ได้เสนอเครื่องมือสำหรับเฝ้าสังเกตคุณภาพการให้บริการ (Quality of services) บนฝั่งเซิร์ฟเวอร์สำหรับเว็บเซอร์วิซ โดยวัดคุณภาพการให้บริการ 6 ด้าน และในด้านที่ผู้วิจัยสนใจคือด้านตัววัดสำหรับความมั่นคง โดยงานวิจัยดังกล่าวจะทำการสแกนรายชื่อซอฟต์แวร์ที่มีอยู่ในเครื่องเซิร์ฟเวอร์ที่ให้บริการเว็บเซอร์วิซ หลังจากนั้นจะนำรายชื่อซอฟต์แวร์และเวอร์ชันไปค้นหารายการช่องโหว่ที่เกี่ยวข้องกับซอฟต์แวร์นั้นจากฐานข้อมูลเอ็นวีดี เพื่อให้ทราบว่าซอฟต์แวร์เวอร์ชันที่ติดตั้งในเครื่องเซิร์ฟเวอร์นั้นมีรายการช่องโหว่ใดบ้าง และประเมินความรุนแรงของช่องโหว่ที่มีต่อเครื่องเซิร์ฟเวอร์โดยใช้คะแนนซีวีเอสเอส โดยถือว่าหากเซิร์ฟเวอร์ที่ติดตั้งเว็บเซอร์วิซมีช่องโหว่ที่รุนแรงย่อมส่งผลต่อคุณภาพด้านความมั่นคงในการให้บริการของเว็บเซอร์วิซด้วย ซึ่งคะแนนซีวีเอสเอสที่นำมาใช้นั้นจะใช้เพียงแค่กลุ่มตัววัดพื้นฐานเท่านั้น

จากการที่งานวิจัยดังกล่าวมีการประเมินความรุนแรงของช่องโหว่โดยใช้คะแนนซีวีเอสเอสในกลุ่มตัววัดพื้นฐานเท่านั้น จึงทำให้ไม่สามารถสะท้อนสภาพของซอฟต์แวร์ขององค์กร ณ ปัจจุบันได้ดีนัก ผู้วิจัยจะใช้แนวทางจากงานวิจัยดังกล่าวนี้แต่จะพิจารณากลุ่มตัววัดตามเวลาและกลุ่มตัววัดตามสภาพแวดล้อมร่วมด้วยในการคำนวณคะแนนซีวีเอสเอส

2.2.4. Improving CVSS-based vulnerability prioritization and response with context information

งานวิจัย [11] กล่าวว่าการแก้ไขช่องโหว่เป็นงานที่ใช้แรงงานและค่าใช้จ่ายจำนวนมาก จึงได้นำเสนอวิธีที่ช่วยให้ผู้จัดการด้านความมั่นคงมีข้อมูลประกอบการตัดสินใจลงทุนในการจัดลำดับความสำคัญของช่องโหว่ในองค์กรให้ดีขึ้น และรายการช่องโหว่ที่นำมาคำนวณนำมาจากเอ็นวีดี แต่เอ็นวีดีได้ให้คะแนนซีวีเอสเอสไว้เพียงแค่กลุ่มตัววัดพื้นฐานเท่านั้น อย่างไรก็ตามผู้จัดการด้านความมั่นคงทราบว่าความรุนแรงของช่องโหว่จะแตกต่างกันมากในบริบทขององค์กรที่แตกต่างกัน ดังนั้นคะแนนซีวีเอสเอสที่ให้โดยเอ็นวีดีจึงไม่เพียงพอที่จะจัดลำดับความสำคัญของช่องโหว่

ในงานวิจัยนี้จึงได้เปรียบเทียบ 2 สถานการณ์เพื่อจัดลำดับความสำคัญของช่องโหว่ในองค์กร สถานการณ์แรกเป็นการประเมินผลกระทบของช่องโหว่ด้วยคะแนนซีวีเอสเอสโดยใช้เพียงกลุ่มตัววัดพื้นฐานเท่านั้น ส่วนสถานการณ์ที่สองเป็นการประเมิน ผลกระทบของช่องโหว่ด้วยคะแนนซีวีเอสเอสทั้ง 3 กลุ่ม

คะแนนซีวีเอสเอสในส่วนของกลุ่มตัววัดตามเวลาได้มาจากการประมาณโดยใช้โมเดลของ Frei [12] ตัววัด Exploit Code Maturity ได้มาจาก $F(x) = 1 - \left(\frac{k}{x}\right)^a$ โดยที่ a = 0.26 , k = 0.00161 และ x คือ อายุของช่องโหว่ ซึ่งอายุของช่องโหว่ในที่นี้นับจากวันแรกที่มีการเปิดเผยช่องโหว่จนถึงวันที่ช่องโหว่นั้นถูกคำนวณคะแนนซีวีเอสเอส และตัววัด Remediation Level ได้มาจาก $F(x) = 1 - exp(-\frac{x}{\lambda})^k$ โดยที่ λ = 0.209 , k = 4.04 และ x คือ อายุของช่องโหว่

คะแนนซีวีเอสเอสในส่วนของกลุ่มตัววัดตามสภาพแวดล้อมที่เกี่ยวข้องกับผลกระทบจากการสูญเสียองค์ประกอบด้านความมั่นคง ซึ่งผลกระทบที่เป็นไปได้ทั้งหมดคือ High, Medium หรือ Low ผู้วิจัยให้ระดับผลกระทบเริ่มต้นเป็น Medium หลังจากนั้นจึงไปสัมภาษณ์ผู้จัดการด้านความมั่นคงจากหลายองค์กรเพื่อให้จัดลำดับผลกระทบจากการสูญเสียการรักษาความลับ บูรณภาพ และสภาพพร้อมใช้งาน โดยให้ระบุว่าการสูญเสียด้านใดจะมีผลกระทบมากที่สุด (ระบุเป็น High) และการสูญเสียด้านใดจะมีผลกระทบน้อยที่สุด (ระบุเป็น Low) จากการสัมภาษณ์จะได้ผลสรุปว่า ผลกระทบจากการสูญเสียการรักษาความลับ บูรณภาพ และสภาพพร้อมใช้งาน เป็น Medium Low และ High ตามลำดับ จากนั้นจึงนำระดับผลกระทบนี้ไปใช้คำนวณคะแนนซีวีเอสเอส

เมื่อได้คำนวณคะแนนซีวีเอสเอสของทั้งสองสถานการณ์เปรียบเทียบกันแล้ว พบว่าสถานการณ์ที่สองสะท้อนความรุนแรงที่แท้จริงของช่องโหว่จากมุมมองขององค์กรได้ดีขึ้น และผู้จัดการด้านความมั่นคงสามารถเลือกจัดการช่องโหว่ได้อย่างมีประสิทธิภาพมากขึ้น

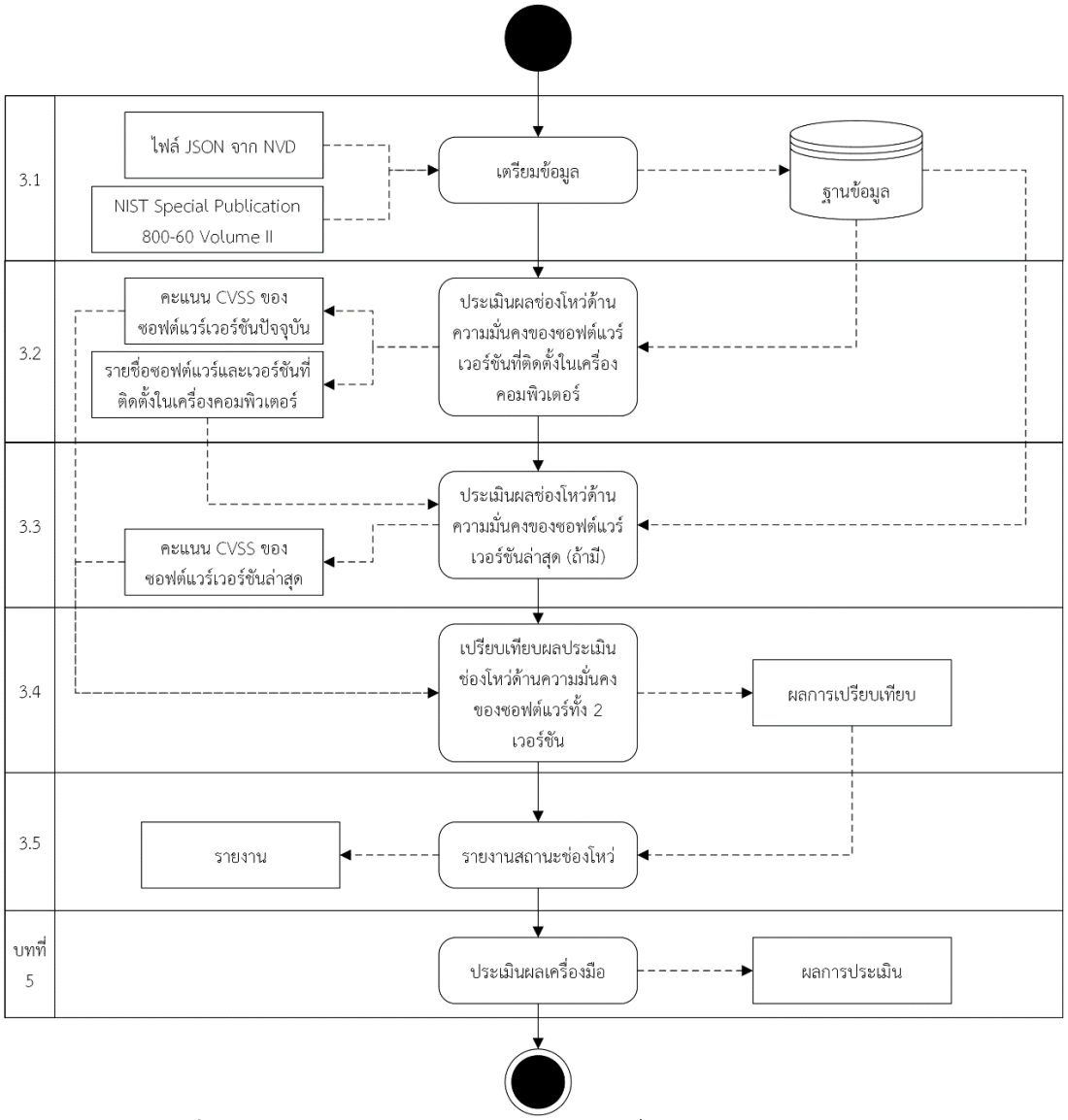
จากงานวิจัยดังกล่าวพบว่าคะแนนซีวีเอสเอสในกลุ่มตัววัดตามเวลาเป็นเพียงคะแนนที่ได้จากการประมาณจากสูตร และคะแนนซีวีเอสเอสในกลุ่มตัววัดตามสภาพแวดล้อมเป็นคะแนนที่ได้จากการ

สัมภาษณ์ผู้จัดการความมั่นคงกลุ่มหนึ่ง ซึ่งอาจสะท้อนสภาพแวดล้อมขององค์กรอื่น ๆ ได้ไม่ดีนัก ดังนั้นในการคำนวณคะแนนซีวีเอสเอสของผู้วิจัย จะนำคะแนนในกลุ่มตัววัดตามเวลามาจากไอบีเอ็ม เอกซ์เอฟอี และคะแนนกลุ่มตัววัดตามสภาพแวดล้อม จะให้ผู้ใช้งานเป็นผู้ระบุเอง หรือให้ผู้ดูแลระบบของแต่ละองค์กรเป็นผู้ระบุโดยมีข้อแนะนำเบื้องต้นตามระดับผลกระทบจากการสูญเสียองค์ประกอบด้านความมั่นคงซึ่งกำหนดโดย NIST

บทที่ 3
แนวคิดและวิธีดำเนินการวิจัย

ผู้วิจัยมีแนวคิดที่จะพัฒนาเครื่องมือช่วยประเมินช่องโหว่ด้านความมั่นคงเพื่อการยกระดับเวอร์ชันของซอฟต์แวร์ โดยจะนำคะแนนซีวีเอสเอสเข้ามาประเมินความรุนแรงของช่องโหว่ในแต่ละซอฟต์แวร์ที่ติดตั้งอยู่ในเครื่องคอมพิวเตอร์ซึ่งอาจเป็นเครื่องคอมพิวเตอร์ของผู้ใช้งาน หรือเป็นเครื่องคอมพิวเตอร์ขององค์กร และเปรียบเทียบกับความรุนแรงของช่องโหว่ในเวอร์ชันล่าสุด เพื่อรายงานคำแนะนำในการเพิ่มความมั่นคงให้กับซอฟต์แวร์ ซึ่งหากเวอร์ชันล่าสุดที่ยังไม่ได้ติดตั้งในเครื่องคอมพิวเตอร์มีความรุนแรงของช่องโหว่น้อยกว่า ผู้ดูแลระบบขององค์กรหรือผู้ใช้งานควรที่จะพิจารณายกระดับเวอร์ชัน การประเมินช่องโหว่จะใช้ตัววัดทั้ง 3 กลุ่มเพื่อสะท้อนความรุนแรงที่แท้จริงของช่องโหว่จากมุมมองขององค์กร โดยคะแนนกลุ่มตัววัดตามสภาพแวดล้อมจะใช้แนวทางผลกระทบที่กำหนดโดย NIST [3] เป็นคะแนนแนะนำให้แก่ผู้ดูแลระบบ หรือให้ผู้ใช้งานเป็นผู้ระบุผลกระทบเอง

กระบวนการทำงานของเครื่องมือและการประเมินผลจะมี 6 ขั้นตอนหลัก ดังภาพรวมการทำงานในรูปที่ 3.1 รายละเอียดแต่ละขั้นตอนที่ 1-5 จะอธิบายถัดไป และขั้นตอนที่ 6 ขั้นตอนประเมินผลเครื่องมือจะอธิบายในบทที่ 5



รูปที่ 3.1 ภาพรวมกระบวนการทำงานของเครื่องมือและการประเมินผล

3.1. ขั้นตอนการจัดเตรียมข้อมูลช่องโหว่และคะแนนกลุ่มตัววัดตามสภาพแวดล้อม

3.1.1. จัดเตรียมข้อมูลช่องโหว่จากเอ็นวีดี

ในขั้นตอนนี้จะดำเนินการรวบรวมและจัดเตรียมข้อมูลช่องโหว่ที่ได้จากเอ็นวีดีลงในฐานข้อมูล ซึ่งในเอ็นวีดี ข้อมูลช่องโหว่จะถูกแบ่งเป็นไฟล์ตามปีที่ค้นพบรายการซีวีอีของช่องโหว่นั้นๆ ดังรูปที่ 3.2 และข้อมูลช่องโหว่นี้จะถูกจัดเก็บในรูปแบบเจสัน (JSON) โดยที่ในแต่ละรายการซีวีอีจะประกอบด้วยข้อมูลหลายๆ อย่าง เช่น รายการซีวีอี ชื่อผู้ขายผลิตภัณฑ์ซอฟต์แวร์ รายชื่อซอฟต์แวร์และเวอร์ชันที่มีช่องโหว่นี้อยู่ คะแนนกลุ่มตัววัดพื้นฐานของซีวีเอสเอสเวอร์ชัน 2 คะแนนกลุ่มตัววัดพื้นฐานของซีวีเอส

เอสเวอร์ชัน 3 และ แหล่งอ้างอิงของรายการช่องโหว่ ซึ่งโครงสร้างของข้อมูลซีวีอีที่ถูกจัดเก็บในเอ็นวีดีสามารถแสดงได้ดังรูปที่ 3.3

Feed	Updated	Download	Size (MB)
CVE-Modified	6/11/2017 6:00:28 AM -04:00	META	
		GZ	0.13
		ZIP	0.13
CVE-Recent	6/11/2017 6:00:11 AM -04:00	META	
		GZ	0.09
		ZIP	0.09
CVE-2017	6/11/2017 3:00:58 AM -04:00	META	
		GZ	0.78
		ZIP	0.78
CVE-2016	6/10/2017 3:04:18 AM -04:00	META	
		GZ	2.45
		ZIP	2.45
CVE-2015	6/10/2017 3:07:05 AM -04:00	META	
		GZ	2.04
		ZIP	2.04

รูปที่ 3.2 รายการซีวีอีแยกตามปีที่เผยแพร่ทางเว็บไซต์เอ็นวีดี


```
"cve" : {
  "CVE_data_meta" : {
    "ID" : "CVE-2016-0001"
  },
"configurations" : {
  "CVE_data_version" : "4.0",
  "nodes" : [ {
    "operator" : "AND",
    "children" : [ {
      "operator" : "OR",
      "cpe" : [ {
        "vulnerable" : true,
        "cpeMatchString" : "cpe:/a:microsoft:jscript:5.7",
        "cpe23Uri" : "cpe:2.3:a:microsoft:jscript:5.7:*:*:*:*:*:*:*"
      }, {
        "vulnerable" : true,
        "cpeMatchString" : "cpe:/a:microsoft:jscript:5.8",
        "cpe23Uri" : "cpe:2.3:a:microsoft:jscript:5.8:*:*:*:*:*:*:*"
      }, {
        "vulnerable" : true,
        "cpeMatchString" : "cpe:/a:microsoft:vbscript:5.7",
        "cpe23Uri" : "cpe:2.3:a:microsoft:vbscript:5.7:*:*:*:*:*:*:*"
      }, {
        "vulnerable" : true,
        "cpeMatchString" : "cpe:/a:microsoft:vbscript:5.8",
        "cpe23Uri" : "cpe:2.3:a:microsoft:vbscript:5.8:*:*:*:*:*:*:*"
      } ]
    }, {
```

```
"impact" : {
  "baseMetricV3" : {
    "cvssV3" : {
      "attackVector" : "NETWORK",
      "attackComplexity" : "HIGH",
      "privilegesRequired" : "NONE",
      "userInteraction" : "REQUIRED",
      "scope" : "UNCHANGED",
      "confidentialityImpact" : "HIGH",
      "integrityImpact" : "HIGH",
      "availabilityImpact" : "HIGH",
      "baseScore" : 7.5,
      "baseSeverity" : "HIGH"
    },
    "exploitabilityScore" : 1.6,
    "impactScore" : 5.9
  },
  "baseMetricV2" : {
    "cvssV2" : {
      "accessVector" : "NETWORK",
      "accessComplexity" : "HIGH",
      "authentication" : "NONE",
      "confidentialityImpact" : "COMPLETE",
      "integrityImpact" : "COMPLETE",
      "availabilityImpact" : "COMPLETE",
      "baseScore" : 7.6
    },
    "severity" : "HIGH",
    "exploitabilityScore" : 4.9,
    "impactScore" : 10.0,
    "obtainAllPrivilege" : false,
    "obtainUserPrivilege" : false,
    "obtainOtherPrivilege" : false,
    "userInteractionRequired" : true
  }
},
```


รูปที่ 3.3 โครงสร้างของรายการซีวีอีที่ถูกจัดเก็บในเอ็นวีดี

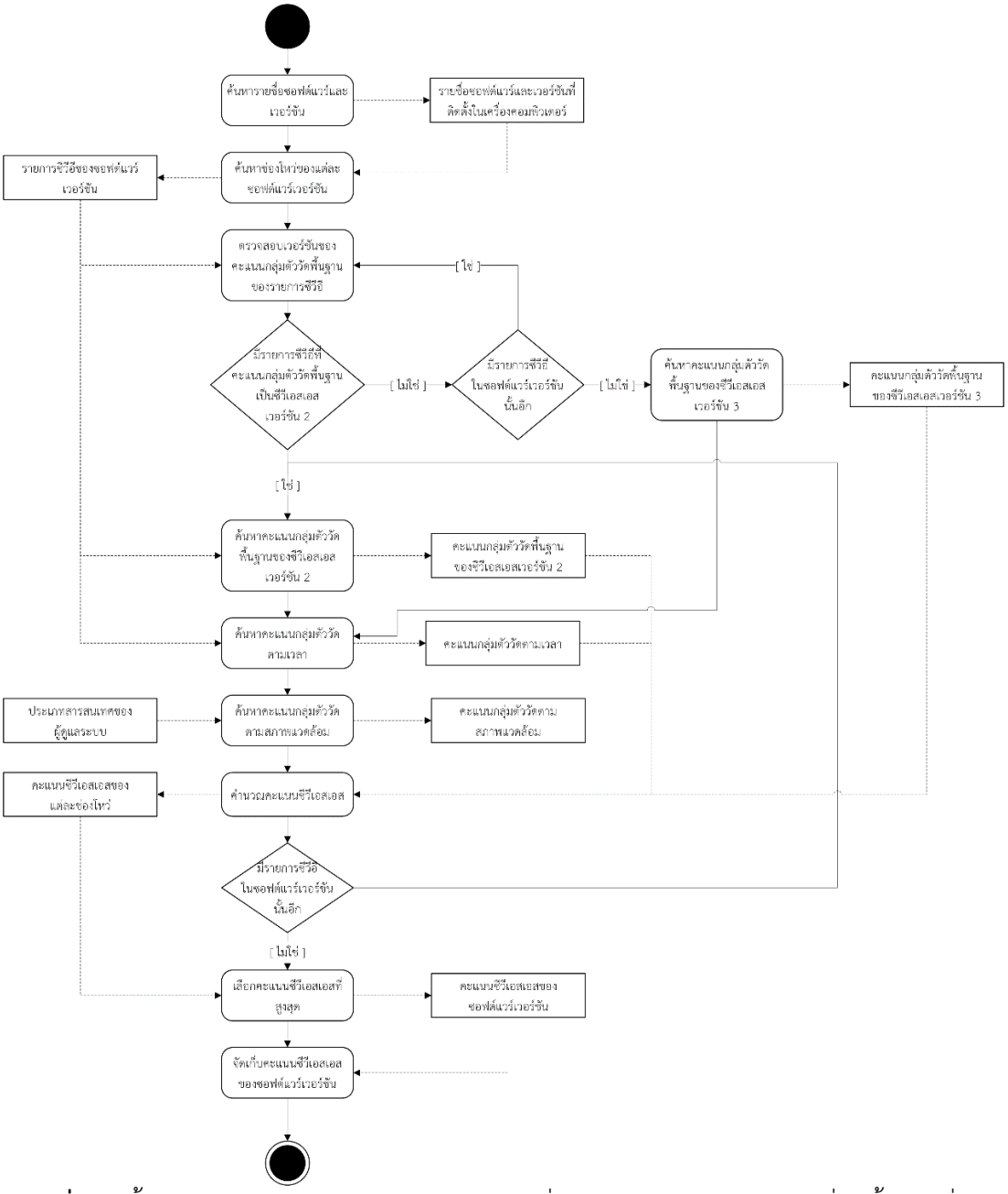
บางรายการซีวีอีที่เอ็นวีดีเริ่มมีการประเมินความรุนแรงของช่องโหว่ด้วยคะแนนกลุ่มตัววัดพื้นฐานของซีวีเอสเอสเวอร์ชัน 3 นั้น ส่วนใหญ่จะเป็นรายการซีวีอีปี 2015 และ 2016

3.1.2. รวบรวมและจัดเก็บข้อมูลกลุ่มตัววัดตามสภาพแวดล้อม

ในส่วนนี้จะจัดเก็บข้อมูลระดับของผลกระทบต่อองค์กรเมื่อสารสนเทศประเภทต่าง ๆ ในระบบสารสนเทศขององค์กรเกิดการสูญเสียการรักษาความลับ บูรณภาพ และสภาพพร้อมใช้งาน ตามแนวทางของ NIST [3] ดังตัวอย่างในตารางที่ 2.2 ในหัวข้อที่ 2.1.4 ตามที่ได้กล่าวไปแล้ว โดยจัดเก็บลงในฐานข้อมูล

3.2. ขั้นตอนประเมินผลช่องโหว่ด้านความมั่นคงของซอฟต์แวร์เวอร์ชันที่ติดตั้งในเครื่องคอมพิวเตอร์

ในขั้นตอนนี้จะดำเนินการตามรูปที่ 3.4 มีรายละเอียดดังนี้



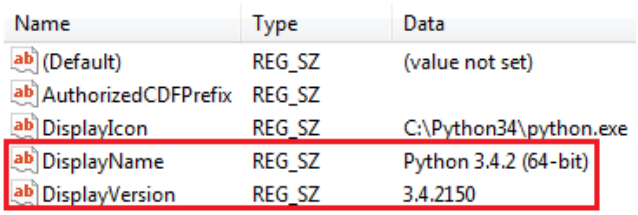
รูปที่ 3.4 ขั้นตอนการประเมินผลช่องโหว่ด้านความมั่นคงของซอฟต์แวร์เวอร์ชันที่ติดตั้งในเครื่องคอมพิวเตอร์

3.2.1. ค้นหาซอฟต์แวร์เวอร์ชันทั้งหมดที่ติดตั้งในเครื่องคอมพิวเตอร์

การค้นหารายชื่อซอฟต์แวร์และเวอร์ชันจะทำการค้นจากวินโดวส์รีจิสทรี (Windows Registry) โดยที่เวอร์ชันของระบบปฏิบัติการวินโดวส์จะถูกเก็บไว้ใน HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion และรายชื่อซอฟต์แวร์และเวอร์ชันที่ติดตั้งในเครื่องคอมพิวเตอร์บนระบบปฏิบัติการวินโดวส์ถ้าหากเป็นซอฟต์แวร์เวอร์ชัน 64 บิตจะถูกเก็บไว้ใน HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall และ ะ

สำหรับซอฟต์แวร์เวอร์ชัน 32 บิตจะถูกเก็บไว้ใน HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall

รายละเอียดของข้อมูลรายชื่อซอฟต์แวร์เวอร์ชันที่เก็บไว้ในวินโดวส์รีจิสทรี เป็นดังรูปที่ 3.5 ซึ่งรายชื่อซอฟต์แวร์จะดึงมาจากฟิลด์ DisplayName และเลขเวอร์ชันจะดึงมาจากฟิลด์ DisplayVersion



Name	Type	Data
(Default)	REG_SZ	(value not set)
AuthorizedCDFPrefix	REG_SZ	
DisplayIcon	REG_SZ	C:\Python34\python.exe
DisplayName	REG_SZ	Python 3.4.2 (64-bit)
DisplayVersion	REG_SZ	3.4.2150

รูปที่ 3.5 ตัวอย่างรายละเอียดของข้อมูลรายชื่อซอฟต์แวร์เวอร์ชันที่เก็บไว้ในวินโดวส์รีจิสทรี

3.2.2. ค้นหาช่องโหว่ของแต่ละซอฟต์แวร์เวอร์ชันจากฐานข้อมูลช่องโหว่

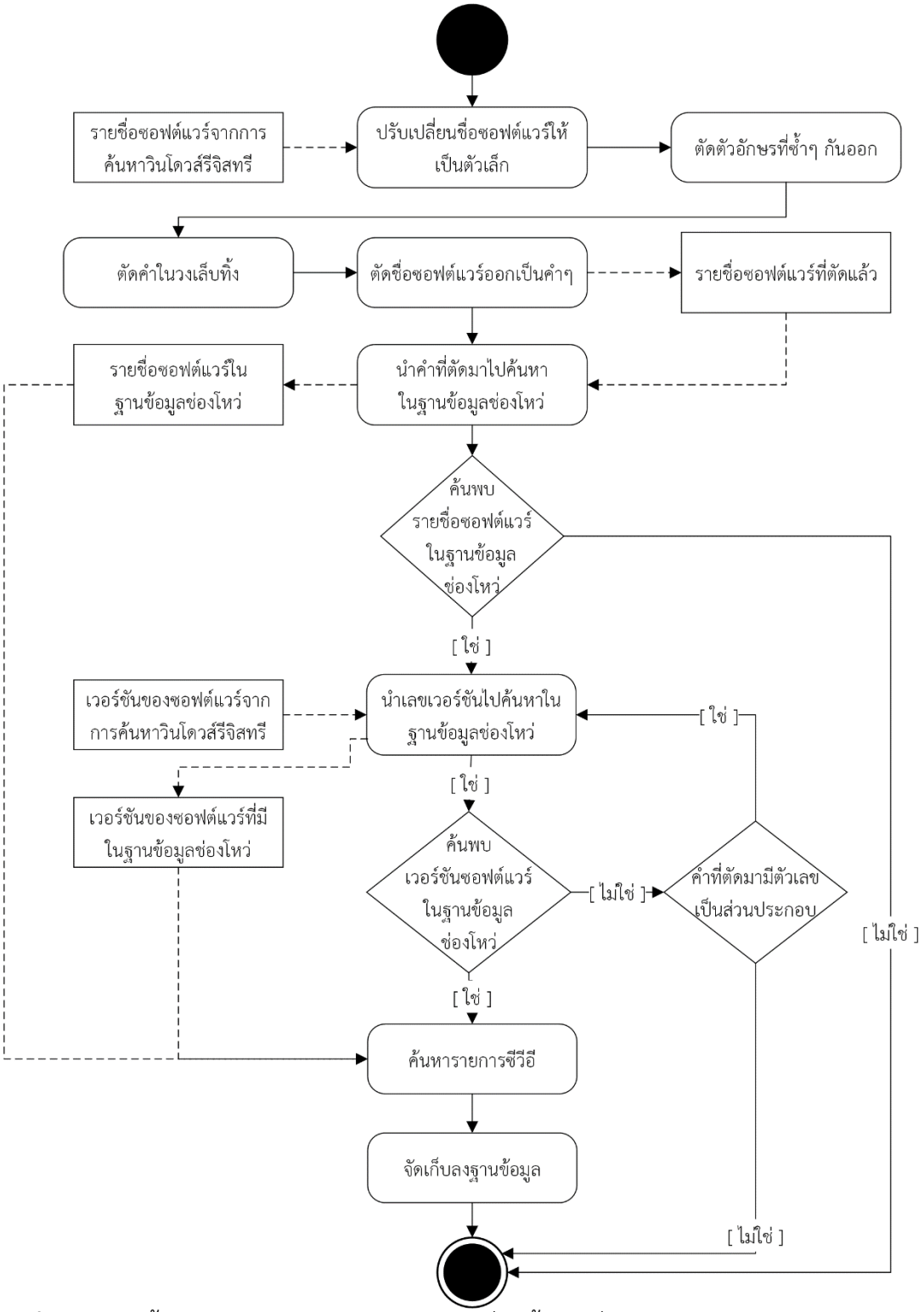
หลังจากได้รายชื่อซอฟต์แวร์และเวอร์ชันของซอฟต์แวร์ที่ติดตั้งในเครื่องคอมพิวเตอร์แล้ว จะนำไปค้นหาช่องโหว่ของแต่ละซอฟต์แวร์เวอร์ชันจากฐานข้อมูลช่องโหว่ที่ได้จากเอ็นวีดีในหัวข้อที่ 3 เพื่อให้ระบุได้ว่าซอฟต์แวร์เวอร์ชันนั้นมีช่องโหว่รายการใดบ้าง ในการจับคู่ชื่อซอฟต์แวร์เวอร์ชันกับฐานข้อมูลช่องโหว่ มีขั้นตอนดังรูปที่ 3.6 รายละเอียดมีดังนี้

1) นำชื่อซอฟต์แวร์ที่ได้มาจากการค้นหาวินโดวส์รีจิสทรีจากฟิลด์ DisplayName มาปรับเปลี่ยนให้เป็นตัวอักษรตัวเล็กทั้งหมดเผื่อในกรณีที่ชื่อซอฟต์แวร์ที่ได้มามีตัวอักษรใหญ่ปน ตัดตัวอักษรซ้ำๆ กันออกเนื่องจากไม่มีนัยสำคัญในการค้นหา เช่น zzzz และตัดคำในวงเล็บทิ้ง เพื่อเตรียมพร้อมสำหรับการนำไปค้นหารายชื่อซอฟต์แวร์ในฐานข้อมูล

2) ตัดชื่อซอฟต์แวร์ที่ได้มาจากข้อ 1) ออกเป็นคำย่อย ๆ โดยใช้ช่องว่างระหว่างคำเป็นตัวแบ่ง เพื่อเพิ่มโอกาสในการจับคู่รายชื่อซอฟต์แวร์ในฐานข้อมูลช่องโหว่ให้มีโอกาสพบมากขึ้น เนื่องจากรายชื่อซอฟต์แวร์ที่ได้มาจากการค้นหาในวินโดวส์รีจิสทรี อาจไม่ตรงกับรายชื่อซอฟต์แวร์ในฐานข้อมูลช่องโหว่ทุกประการ เช่น รายชื่อซอฟต์แวร์ที่ค้นหาได้จากวินโดวส์รีจิสทรีชื่อ Python 3.4.2 (64-bit) แต่ในฐานข้อมูลช่องโหว่ชื่อ “cpe:/a:python:python:3.4.2”

3) นำคำที่ได้จากข้อที่ 2) มาค้นหาในฐานข้อมูลช่องโหว่ ถ้าหากค้นหารายชื่อซอฟต์แวร์พบ จะไปค้นหาในส่วนของเวอร์ชันในข้อ 4) ต่อไป ถ้าหากคำที่ค้นหาไม่พบในฐานข้อมูล แสดงว่ารายชื่อซอฟต์แวร์นั้นไม่มีในฐานข้อมูล

4) นำเลขเวอร์ชันของซอฟต์แวร์ที่ได้จากฟิลด์ DisplayVersion มาค้นหาว่าตรงกันกับเลขเวอร์ชันของซอฟต์แวร์ที่มีช่องโหว่ในฐานข้อมูลหรือไม่ ถ้าไม่พบจะไปพิจารณาจากคำที่ได้จากข้อที่ 2) ว่ามีตัวเลขประกอบอยู่ด้วยหรือไม่ ถ้ามีจะนำไปค้นหาเวอร์ชันของซอฟต์แวร์ในฐานข้อมูลอีกครั้ง



รูปที่ 3.6 ลำดับขั้นตอนในการจับคู่ซอฟต์แวร์เวอร์ชันที่ติดตั้งในเครื่องคอมพิวเตอร์กับฐานข้อมูลช่องโหว่

5) ถ้าค้นพบเลขเวอร์ชันในฐานข้อมูล จะไปค้นหารายการซีวีอีของซอฟต์แวร์เวอร์ชันนั้น เพื่อให้ทราบว่าซอฟต์แวร์เวอร์ชันนี้มีช่องโหว่รายการใดบ้าง

6) จัดเก็บรายการซีวีอีของซอฟต์แวร์เวอร์ชันนั้นลงฐานข้อมูล

3.2.3. คำนวณคะแนนความรุนแรงของช่องโหว่ในซอฟต์แวร์เวอร์ชันที่ติดตั้งในเครื่องคอมพิวเตอร์

เมื่อได้รายการซีวีอีของซอฟต์แวร์เวอร์ชันที่มีช่องโหว่ที่ติดตั้งในเครื่องคอมพิวเตอร์แล้ว การคำนวณคะแนนความรุนแรงของช่องโหว่มีรายละเอียดดังนี้

1) นำรายการซีวีอีของซอฟต์แวร์เวอร์ชันนั้น ๆ ไปตรวจสอบจากฐานข้อมูลช่องโหว่ว่ามีรายการซีวีอีที่มีคะแนนกลุ่มตัววัดพื้นฐานเป็นซีวีเอสเอสเวอร์ชัน 2 หรือไม่ หากมีรายการซีวีอีรายการใดรายการหนึ่งมีคะแนนกลุ่มตัววัดพื้นฐานเป็นซีวีเอสเอสเวอร์ชัน 2 จะหยุดตรวจสอบรายการซีวีอีที่เหลือในซอฟต์แวร์เวอร์ชันนั้น ๆ และดำเนินการตาม ข้อที่ 2) หากยังไม่พบรายการซีวีอีใดมีคะแนนกลุ่มตัววัดพื้นฐานเป็นซีวีเอสเอสเวอร์ชัน 2 จะทำการตรวจสอบจนครบทุกรายการซีวีอีในซอฟต์แวร์เวอร์ชันนั้น ๆ แสดงว่ารายการซีวีอีในซอฟต์แวร์เวอร์ชันนั้นมีคะแนนกลุ่มตัววัดพื้นฐานเป็นซีวีเอสเอสเวอร์ชัน 3

2) นำรายการซีวีอีของซอฟต์แวร์เวอร์ชันนั้น ๆ ไปค้นหาคะแนนกลุ่มตัววัดพื้นฐานโดยจะค้นหาตามเวอร์ชันซีวีเอสเอสที่ได้จากการตรวจสอบรายการซีวีอีในข้อที่ 1)

3) นำรายการซีวีอีของซอฟต์แวร์เวอร์ชันนั้น ๆ ไปค้นหาคะแนนกลุ่มตัววัดตามเวลา ซึ่งคะแนนในกลุ่มนี้จะได้มาจากการเรียกใช้เอพีไอของ ไอบีเอ็ม เอกซ์เอฟอี

4) ผู้ดูแลระบบเลือกประเภทสารสนเทศที่คอมพิวเตอร์เครื่องนั้นๆ ทำงานเกี่ยวข้องอยู่ จากนั้นนำไปค้นหาในฐานข้อมูลคะแนนกลุ่มตัววัดตามสภาพแวดล้อม ซึ่งเป็นไปตามระดับผลกระทบจากการสูญเสียองค์ประกอบด้านความมั่นคงซึ่งกำหนดโดย NIST เพื่อให้ได้คะแนนกลุ่มตัววัดตามสภาพแวดล้อมสำหรับประเภทสารสนเทศนั้น สำหรับในกรณีการใช้งานเครื่องมือโดยผู้ใช้งานทั่วไป ผู้ใช้งานสามารถระบุระดับผลกระทบเองได้

5) เมื่อได้คะแนนครบทั้ง 3 กลุ่มแล้วจะคำนวณคะแนนซีวีเอสเอสของแต่ละรายการซีวีอี

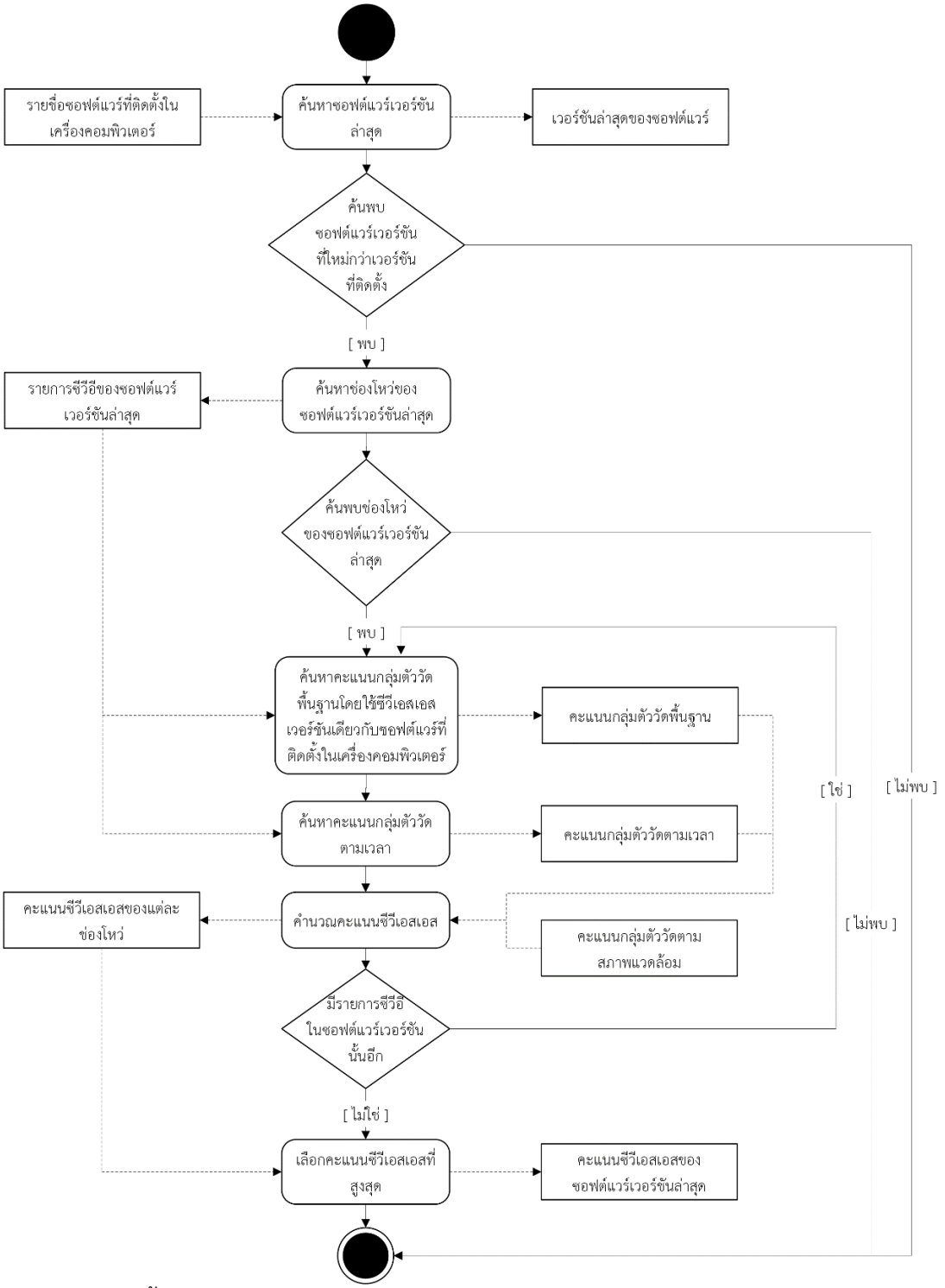
6) เมื่อคำนวณคะแนนซีวีเอสเอสครบทุกรายการซีวีอีในซอฟต์แวร์เวอร์ชันนั้นๆ แล้ว จะเลือกคะแนนซีวีเอสเอสที่สูงที่สุดจากรายการซีวีอีเหล่านั้น ตามหลักการ High Water Mark [13] เพื่อเป็นตัวแทนคะแนนซีวีเอสเอสของซอฟต์แวร์เวอร์ชันนั้น

7) จัดเก็บคะแนนซีวีเอสเอสของซอฟต์แวร์เวอร์ชันนั้น

8) หากยังมีรายชื่อซอฟต์แวร์และเวอร์ชันที่ยังไม่ได้คำนวณคะแนนความรุนแรงของช่องโหว่ในซอฟต์แวร์เวอร์ชันนั้น ๆ จะดำเนินการตามข้อ 1) อีกครั้งจนครบทุกรายการซอฟต์แวร์ที่ติดตั้งในเครื่องคอมพิวเตอร์

3.3. ขั้นตอนประเมินผลช่องโหว่ด้านความมั่นคงของซอฟต์แวร์เวอร์ชันล่าสุด (ถ้ามี)

ในขั้นตอนนี้จะดำเนินการตามรูปที่ 3.7 โดยมีรายละเอียดดังนี้



รูปที่ 3.7 ขั้นตอนการประเมินผลช่องโหว่ด้านความมั่นคงของซอฟต์แวร์เวอร์ชันล่าสุดที่มีในฐานข้อมูลช่องโหว่

3.3.1. ค้นหาเวอร์ชันซอฟต์แวร์ล่าสุด

นำรายชื่อซอฟต์แวร์ที่ได้จากการค้นหาจากวินโดวส์รีจิสทรีในหัวข้อที่ 3.2 ไปค้นหาเวอร์ชันล่าสุดจากฐานข้อมูลช่องโหว่

3.3.2. ค้นหาช่องโหว่ของแต่ละซอฟต์แวร์เวอร์ชันล่าสุดจากฐานข้อมูลช่องโหว่

หากเวอร์ชันล่าสุดใหม่กว่าเวอร์ชันของซอฟต์แวร์ที่ติดตั้งอยู่ จะทำการค้นหาช่องโหว่ของแต่ละซอฟต์แวร์เวอร์ชันล่าสุดจากฐานข้อมูลช่องโหว่ โดยวิธีการหาช่องโหว่จะดำเนินการเช่นเดียวกับในหัวข้อที่ 3.2.2

3.3.3. คำนวณคะแนนความรุนแรงของช่องโหว่ในซอฟต์แวร์เวอร์ชันล่าสุด

เมื่อได้รายการซีวีอีของซอฟต์แวร์เวอร์ชันล่าสุดแล้วจะดำเนินการต่อไปนี้

1) นำรายการซีวีอีไปค้นหาคะแนนกลุ่มตัววัดพื้นฐานจากฐานข้อมูล โดยคะแนนที่ค้นหาจะเป็นซีวีเอสเอสเวอร์ชันเดียวกับรายการซีวีอีของซอฟต์แวร์เวอร์ชันที่ติดตั้งในเครื่องคอมพิวเตอร์
2) นำรายการซีวีอีของซอฟต์แวร์เวอร์ชันล่าสุด ไปค้นหาคะแนนกลุ่มตัววัดตามเวลา ซึ่งคะแนนในกลุ่มนี้จะได้มาจากการเรียกใช้เอพีไอของ ไอบีเอ็ม เอกซ์เอฟอี
3) คะแนนกลุ่มตัววัดตามสภาพแวดล้อมจะเป็นคะแนนเดียวกับที่ผู้ใช้งานหรือผู้ดูแลระบบระบุไว้สำหรับประเภทสารสนเทศที่เครื่องคอมพิวเตอร์ทำงานเกี่ยวข้องอยู่ ดังหัวข้อที่ 3.2.3
4) เมื่อได้คะแนนครบทั้ง 3 กลุ่มแล้วจะคำนวณคะแนนซีวีเอสเอสของแต่ละรายการซีวีอี
5) เมื่อคำนวณคะแนนซีวีเอสเอสครบทุกรายการซีวีอีในซอฟต์แวร์เวอร์ชันนั้น ๆ แล้ว จะเลือกคะแนนซีวีเอสเอสที่สูงที่สุดจากรายการซีวีอีเหล่านั้น ตามหลักการ High Water Mark [13] เพื่อเป็นตัวแทนคะแนนซีวีเอสเอสของซอฟต์แวร์เวอร์ชันล่าสุด
6) จัดเก็บคะแนนซีวีเอสเอสของซอฟต์แวร์เวอร์ชันล่าสุด

3.4. ขั้นตอนเปรียบเทียบผลประเมินช่องโหว่ด้านความมั่นคงของซอฟต์แวร์ทั้งสองเวอร์ชัน

นำคะแนนที่ได้จากการประเมินผลช่องโหว่ด้านความมั่นคงของซอฟต์แวร์เวอร์ชันที่ติดตั้งในเครื่องคอมพิวเตอร์ในหัวข้อที่ 3.2 และคะแนนที่ได้จากการประเมินผลช่องโหว่ด้านความมั่นคงของซอฟต์แวร์เวอร์ชันล่าสุดในหัวข้อที่ 3.3 มาเปรียบเทียบกัน เพื่อพิจารณาว่าซอฟต์แวร์เวอร์ชันใดมีคะแนนซีวีเอสเอสน้อยกว่า แสดงว่าซอฟต์แวร์เวอร์ชันนั้นมีความมั่นคงดีกว่าซอฟต์แวร์อีกเวอร์ชันหนึ่ง

3.5. ขั้นตอนการรายงานสถานะช่องโหว่

ในขั้นตอนนี้จะรายงานสถานะช่องโหว่ที่พบ คะแนนซีวีเอสเอส และระดับความรุนแรงที่สรุปได้จากคะแนนซีวีเอสเอส ตามตารางที่ 2.1 สำหรับแต่ละซอฟต์แวร์เวอร์ชันที่ติดตั้งในเครื่องคอมพิวเตอร์และซอฟต์แวร์เวอร์ชันล่าสุดที่ค้นพบจากฐานข้อมูลช่องโหว่ เพื่อให้ผู้ใช้งานหรือผู้ดูแลระบบสามารถ

ทราบได้ว่า ซอฟต์แวร์ที่ติดตั้งในเครื่องคอมพิวเตอร์และซอฟต์แวร์เวอร์ชันล่าสุดนั้นมีช่องโหว่รายการใดบ้าง และมีคะแนนความรุนแรงของช่องโหว่เป็นเท่าไร มีช่องโหว่รายการใดถูกแก้ไขไปแล้ว มีช่องโหว่รายการใดเพิ่มมาใหม่ในซอฟต์แวร์เวอร์ชันล่าสุด

จากสถานะของช่องโหว่ที่ประเมินได้ เครื่องมือสามารถแนะนำโอกาสในการเพิ่มความมั่นคงได้ หากการยกระดับเวอร์ชันของซอฟต์แวร์จะทำให้มีช่องโหว่ที่มีความรุนแรงน้อยลง ในกรณีที่ซอฟต์แวร์ที่ติดตั้งในเครื่องคอมพิวเตอร์และซอฟต์แวร์เวอร์ชันล่าสุดสามารถเปรียบเทียบคะแนนซีวีเอสเอสได้ ในกรณีนี้เครื่องมือมีแนวทางในการแนะนำตามตารางที่ 3.1

ตารางที่ 3.1 คำแนะนำการระบุโอกาสในการเพิ่มความมั่นคงโดยการยกระดับเวอร์ชันซอฟต์แวร์

ระดับผลประเมินช่องโหว่ด้านความมั่นคงของซอฟต์แวร์เวอร์ชันที่ติดตั้งในเครื่องคอมพิวเตอร์	**ระดับผลประเมินช่องโหว่ด้านความมั่นคงของซอฟต์แวร์เวอร์ชันล่าสุด**	**คำแนะนำ**		
		แนะนำให้ยกระดับเวอร์ชันซอฟต์แวร์	**ไม่แนะนำยกระดับเวอร์ชันซอฟต์แวร์**	**ยกหรือไม่ยกระดับเวอร์ชันซอฟต์แวร์ก็ได้**
None	None			✓
	Low, Medium, High, Critical		✓	
Low	None	✓		
	Low			✓
	Medium, High, Critical		✓	
Medium	None, Low	✓		
	Medium			✓
	High, Critical		✓	
High	None, Low, Medium	✓		
	High			✓
	Critical		✓	
Critical	None, Low, Medium, High	✓		
	Critical			✓

กรณีที่ซอฟต์แวร์เวอร์ชันที่ติดตั้งในเครื่องคอมพิวเตอร์ไม่ปรากฏในฐานข้อมูล แต่มีซอฟต์แวร์เวอร์ชันที่ใหม่กว่าปรากฏในฐานข้อมูล ในกรณีนี้จะเลือกระดับ Medium ซึ่งเป็นค่ากลางของระดับความรุนแรงจากคะแนนซีวีเอสเอส เป็นตัวแทนของผลประเมินช่องโหว่ด้านความมั่นคงของซอฟต์แวร์เวอร์ชันที่ติดตั้งในเครื่องคอมพิวเตอร์ และเครื่องมือมีแนวทางในการแนะนำตามตารางที่ 3.2

ตารางที่ 3.2 คำแนะนำในกรณีที่ซอฟต์แวร์เวอร์ชันที่ติดตั้งในเครื่องคอมพิวเตอร์ไม่ปรากฏในฐานข้อมูล

ระดับผลประเมินช่องโหว่ด้านความมั่นคงของซอฟต์แวร์เวอร์ชันที่ติดตั้งในเครื่องคอมพิวเตอร์	**ระดับผลประเมินช่องโหว่ด้านความมั่นคงของซอฟต์แวร์เวอร์ชันล่าสุด**	**คำแนะนำ**		
		แนะนำให้ยกระดับเวอร์ชันซอฟต์แวร์	**ไม่แนะนำยกระดับเวอร์ชันซอฟต์แวร์**	**ยกหรือไม่ยกระดับเวอร์ชันซอฟต์แวร์ก็ได้**
Medium	None, Low, Medium	✓		
	High, Critical			✓

กรณีที่ซอฟต์แวร์เวอร์ชันที่ติดตั้งในเครื่องคอมพิวเตอร์มีเวอร์ชันสูงกว่าซอฟต์แวร์เวอร์ชันล่าสุดที่ปรากฏในฐานข้อมูลและกรณีที่ไม่พบชื่อซอฟต์แวร์ในฐานข้อมูลเลย ผู้ใช้งานก็ควรยกระดับเวอร์ชันซอฟต์แวร์เนื่องจากเครื่องมือไม่สามารถเปรียบเทียบระดับผลประเมินช่องโหว่ด้านความมั่นคงของซอฟต์แวร์ทั้งสองเวอร์ชันได้ แต่ในทางปฏิบัติแล้ว เมื่อผู้ขายผลิตภัณฑ์ซอฟต์แวร์ได้ออกซอฟต์แวร์เวอร์ชันใหม่ๆ มาแสดงว่าซอฟต์แวร์เวอร์ชันนั้นต้องมีการปรับปรุงด้านใดด้านหนึ่งให้ดีขึ้นกว่าซอฟต์แวร์เวอร์ชันเก่า

บทที่ 4
การออกแบบและพัฒนาเครื่องมือ

ในบทนี้จะกล่าวถึงการออกแบบและพัฒนาเครื่องมือช่วยประเมินช่องโหว่ด้านความมั่นคงเพื่อการยกระดับเวอร์ชันของซอฟต์แวร์

4.1. การกำหนดรายการความต้องการของเครื่องมือ

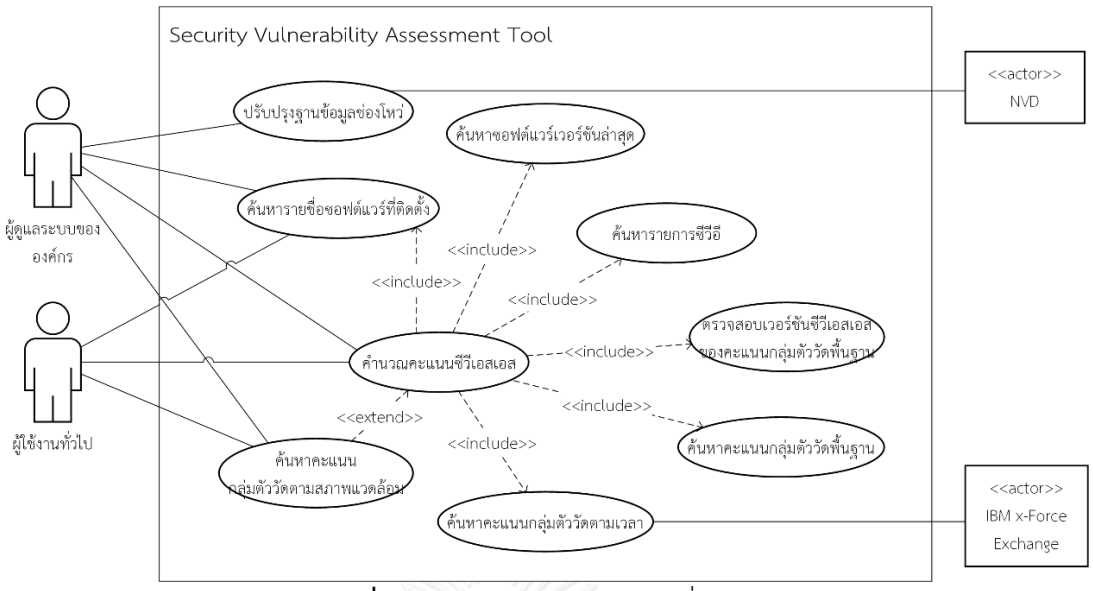
ตามที่ได้กล่าวถึงแนวคิดและวิธีการดำเนินการวิจัยไปแล้วในบทที่ 3 ดังนั้นสามารถระบุความต้องการของเครื่องมือได้ ดังนี้

4.1.1. ความต้องการที่เป็นหน้าที่หลัก (Functional Requirement)

1. ผู้ใช้งานที่เป็นผู้ดูแลระบบสามารถปรับปรุงฐานข้อมูลช่องโหว่จากเอ็นวีดีให้เป็นปัจจุบันได้
2. ผู้ใช้สามารถค้นหารายชื่อซอฟต์แวร์ที่ติดตั้งในเครื่องคอมพิวเตอร์ได้โดยอัตโนมัติ
3. ผู้ใช้งานสามารถเพิ่มรายชื่อซอฟต์แวร์ที่เครื่องมือค้นหาไม่พบจากวินโดวส์รีจิสทรีได้
4. ผู้ใช้งานสามารถเปรียบเทียบคะแนนซีวีเอสเอสระหว่างซอฟต์แวร์ที่ติดตั้งในเครื่องคอมพิวเตอร์กับซอฟต์แวร์เวอร์ชันล่าสุดที่มีในฐานข้อมูลได้
5. ผู้ใช้งานสามารถเลือกชื่อซอฟต์แวร์อื่นที่ต้องการเปรียบเทียบคะแนนซีวีเอสเอสกับซอฟต์แวร์เวอร์ชันที่มีในเครื่องคอมพิวเตอร์ได้

4.2. การออกแบบหน้าที่การทำงานของเครื่องมือ

การออกแบบหน้าที่การทำงานของเครื่องมือมีวัตถุประสงค์ให้เห็นถึงหน้าที่หรือความสามารถในการทำงานของเครื่องมือที่จะถูกพัฒนาขึ้น โดยใช้แบบจำลองยูสเคส (Use case diagram) ในการออกแบบเครื่องมือดังรูปที่ 4.1 และตารางที่ 4.1 ถึง ตารางที่ 4.9



รูปที่ 4.1 แผนภาพยูสเคสของเครื่องมือ

ตารางที่ 4.1 ตารางอธิบายการปรับปรุงฐานข้อมูลช่องโหว่

รหัสยูสเคส	UC01
ชื่อยูสเคส	ปรับปรุงฐานข้อมูลช่องโหว่
ผู้กระทำหลัก	ผู้ดูแลระบบขององค์กร
คำอธิบาย	แผนภาพยูสเคสอธิบายถึงการปรับปรุงฐานข้อมูลช่องโหว่
งานปกติ	1. ผู้ดูแลระบบขององค์กร คลิก ปรับปรุงฐานข้อมูลช่องโหว่ 2. เครื่องมือตรวจสอบข้อมูลในฐานข้อมูลช่องโหว่ 3. เครื่องมือปรับปรุงข้อมูลในฐานข้อมูลช่องโหว่ 4. เครื่องมือแสดงผลทางหน้าจอว่าปรับปรุงเรียบร้อยแล้ว
งานภายใต้เงื่อนไข	2.1 เครื่องมือตรวจสอบข้อมูลในฐานข้อมูลช่องโหว่ และพบว่าข้อมูลในฐานข้อมูลยังไม่ถูกปรับปรุงให้เป็นปัจจุบัน 2.2 เครื่องมือตรวจสอบข้อมูลในฐานข้อมูลช่องโหว่ และพบว่าข้อมูลในฐานข้อมูลเป็นปัจจุบันแล้ว

ตารางที่ 4.2 ตารางอธิบายการค้นหารายชื่อซอฟต์แวร์

รหัสยูสเคส	UC02
ชื่อยูสเคส	การค้นหารายชื่อซอฟต์แวร์
ผู้กระทำหลัก	ผู้ดูแลระบบขององค์กรหรือผู้ใช้งานทั่วไป
คำอธิบาย	แผนภาพยูสเคสอธิบายถึงการค้นหารายชื่อซอฟต์แวร์
งานปกติ	1. ผู้ดูแลระบบขององค์กรหรือผู้ใช้งานทั่วไป คลิก ค้นหารายชื่อซอฟต์แวร์ 2. เครื่องมือค้นหารายชื่อซอฟต์แวร์ที่ติดตั้งในเครื่องคอมพิวเตอร์ 3. เครื่องมือแสดงผลทางหน้าจอว่ามีรายชื่อซอฟต์แวร์ใดบ้าง
งานภายใต้เงื่อนไข	-

ตารางที่ 4.3 ตารางอธิบายการค้นหารายการซีวีอี

รหัสยูสเคส	UC03
ชื่อยูสเคส	การค้นหารายการซีวีอี
ผู้กระทำหลัก	เครื่องมือ
คำอธิบาย	แผนภาพยูสเคสอธิบายถึงการค้นหารายการซีวีอี
งานปกติ	1. เครื่องมือนำรายชื่อซอฟต์แวร์และเวอร์ชันไปค้นหารายการซีวีอีของแต่ละซอฟต์แวร์เวอร์ชัน 2. เครื่องมือแสดงผลทางหน้าจอว่าซอฟต์แวร์เวอร์ชันนั้นมีรายการซีวีอีใดบ้างประกอบอยู่
งานภายใต้เงื่อนไข	-

ตารางที่ 4.4 ตารางอธิบายการตรวจสอบเวอร์ชันซีวีเอสเอสของคะแนนกลุ่มตัววัดพื้นฐาน

รหัสยูสเคส	UC04
ชื่อยูสเคส	การตรวจสอบเวอร์ชันซีวีเอสเอสของคะแนนกลุ่มตัววัดพื้นฐาน
ผู้กระทำหลัก	เครื่องมือ
คำอธิบาย	แผนภาพยูสเคสอธิบายถึงการตรวจสอบเวอร์ชันซีวีเอสเอสของคะแนนกลุ่มตัววัดพื้นฐาน
งานปกติ	1. เครื่องมือนำรายการซีวีอีของแต่ละซอฟต์แวร์เวอร์ชันไปตรวจสอบจากฐานข้อมูล 2. เครื่องมือค้นพบเวอร์ชันของซีวีเอสเอสที่จะนำไปใช้ในการคำนวณคะแนนซีวีเอสเอส
งานภายใต้เงื่อนไข	2.1 เครื่องมือพบว่ามีรายการซีวีอีรายการใดรายการหนึ่งมีคะแนนกลุ่มตัววัดพื้นฐานเป็นซีวีเอสเอสเวอร์ชัน 2 จึงใช้ซีวีเอสเอสเวอร์ชัน 2 2.2 เครื่องมือพบว่าไม่มีรายการซีวีอีรายการใดรายการหนึ่งมีคะแนนกลุ่มตัววัดพื้นฐานเป็นซีวีเอสเอสเวอร์ชัน 2 จึงใช้ซีวีเอสเอสเวอร์ชัน 3

ตารางที่ 4.5 ตารางอธิบายการค้นหาคะแนนกลุ่มตัววัดพื้นฐาน

รหัสยูสเคส	UC05
ชื่อยูสเคส	การค้นหาคะแนนกลุ่มตัววัดพื้นฐาน
ผู้กระทำหลัก	เครื่องมือ
คำอธิบาย	แผนภาพยูสเคสอธิบายถึงการค้นหาคะแนนกลุ่มตัววัดพื้นฐาน
งานปกติ	1. เครื่องมือนำรายการซีวีอีของแต่ละซอฟต์แวร์เวอร์ชันไปค้นหาคะแนนกลุ่มตัววัดพื้นฐานจากฐานข้อมูล โดยจะค้นหาตามเวอร์ชันซีวีเอสเอสที่ตรวจสอบพบ 2. เครื่องมือแสดงคะแนนกลุ่มตัววัดพื้นฐานของแต่ละรายการซีวีอีของแต่ละซอฟต์แวร์เวอร์ชัน
งานภายใต้เงื่อนไข	-

ตารางที่ 4.6 ตารางอธิบายการค้นหาคะแนนกลุ่มตัววัดตามเวลา

รหัสยูสเคส	UC06
ชื่อยูสเคส	การค้นหาคะแนนกลุ่มตัววัดตามเวลา
ผู้กระทำหลัก	เครื่องมือ
คำอธิบาย	แผนภาพยูสเคสอธิบายถึงการค้นหาคะแนนกลุ่มตัววัดตามเวลา
งานปกติ	1. เครื่องมือนำรายการซีวีอีของแต่ละซอฟต์แวร์เวอร์ชันไปค้นหาคะแนนกลุ่มตัววัดตามเวลาโดยการเรียกใช้เอพีไอ ของไอบีเอ็ม เอกซ์เอฟอี 2. เครื่องมือแสดงคะแนนกลุ่มตัววัดตามเวลาแต่ละรายการซีวีอีของแต่ละซอฟต์แวร์เวอร์ชัน
งานภายใต้เงื่อนไข	-

ตารางที่ 4.7 ตารางอธิบายการค้นหาคะแนนกลุ่มตัววัดตามสภาพแวดล้อม

รหัสยูสเคส	UC07
ชื่อยูสเคส	การค้นหาคะแนนกลุ่มตัววัดตามสภาพแวดล้อม
ผู้กระทำหลัก	ผู้ดูแลระบบขององค์กรหรือผู้ใช้งานทั่วไป
คำอธิบาย	แผนภาพยูสเคสอธิบายถึงการค้นหาคะแนนกลุ่มตัววัดตามสภาพแวดล้อม
งานปกติ	1. ผู้ดูแลระบบขององค์กรหรือผู้ใช้งานทั่วไประบุการค้นหาเพื่อนำคะแนนกลุ่มตัววัดตามสภาพแวดล้อมเข้ามาร่วมคำนวณคะแนนซีวีเอสเอสด้วย 2. เครื่องมือนำข้อมูลประเภทสารสนเทศของเครื่องคอมพิวเตอร์จากฐานข้อมูลมาแสดงบนหน้าจอเพื่อให้ผู้ดูแลระบบขององค์กรหรือผู้ใช้งานทั่วไปเลือกประเภทสารสนเทศของเครื่องคอมพิวเตอร์ 3. ผู้ดูแลระบบขององค์กรหรือผู้ใช้งานทั่วไปเลือกประเภทสารสนเทศของเครื่องคอมพิวเตอร์
งานภายใต้เงื่อนไข	-

ตารางที่ 4.8 ตารางอธิบายการคำนวณคะแนนซีวีเอสเอส

รหัสยูสเคส	UC08
ชื่อยูสเคส	การคำนวณคะแนนซีวีเอสเอส
ผู้กระทำหลัก	ผู้ดูแลระบบขององค์กรหรือผู้ใช้งานทั่วไป
คำอธิบาย	แผนภาพยูสเคสอธิบายถึงการคำนวณคะแนนซีวีเอสเอส
งานปกติ	1. ผู้ดูแลระบบขององค์กรหรือผู้ใช้งานทั่วไปเลือกทำการคำนวณคะแนนซีวีเอสเอส 2. เครื่องมือคำนวณคะแนนซีวีเอสเอสของแต่ละรายการซีวีอี โดยนำคะแนนกลุ่มตัววัดพื้นฐาน กลุ่มตัววัดตามเวลา และกลุ่มตัววัดตามสภาพแวดล้อมมาใช้ในการคำนวณคะแนนซีวีเอสเอส
งานภายใต้เงื่อนไข	-

ตารางที่ 4.9 ตารางอธิบายการค้นหาซอฟต์แวร์เวอร์ชันล่าสุด

รหัสยูสเคส	UC09
ชื่อยูสเคส	การค้นหาซอฟต์แวร์เวอร์ชันล่าสุด
ผู้กระทำหลัก	เครื่องมือ
คำอธิบาย	แผนภาพยูสเคสอธิบายถึงการค้นหาซอฟต์แวร์เวอร์ชันล่าสุด
งานปกติ	1. เครื่องมือนำรายชื่อซอฟต์แวร์ที่ติดตั้งในเครื่องคอมพิวเตอร์ไปค้นหาเวอร์ชันล่าสุดจากฐานข้อมูล 2. เครื่องมือแสดงผลทางหน้าจอว่าเวอร์ชันล่าสุดของซอฟต์แวร์มีอะไรบ้าง
งานภายใต้เงื่อนไข	-

4.3. การออกแบบสถาปัตยกรรมของเครื่องมือ

เนื่องจากเครื่องมือที่พัฒนาต้องเป็นเครื่องมือที่ติดตั้งบนเครื่องคอมพิวเตอร์ของผู้ใช้งานหรือของผู้ดูแลระบบขององค์กรได้ เพื่อให้สามารถอ่านรายชื่อซอฟต์แวร์ที่ติดตั้งในเครื่องคอมพิวเตอร์ได้ จึงได้พัฒนาเครื่องมือในรูปแบบเดสก์ท็อป แอปพลิเคชัน (Desktop Application) โดยใช้ภาษาพีเอชพี (PHP) ร่วมกับเฟรมเวิร์ก พีเอชพีเดสก์ท็อป (PHP Desktop) ในการพัฒนาเครื่องมือ และจัดเก็บ

ข้อมูลลงฐานข้อมูลโดยใช้ มายเอสคิวแอล ดาต้าเบส (MySQL Database) ที่ให้บริการอยู่บนเครื่องเซิร์ฟเวอร์ (Server) เพื่อให้เครื่องมือที่ติดตั้งบนเครื่องไคล์เอนต์สามารถเรียกใช้ข้อมูลได้สะดวก

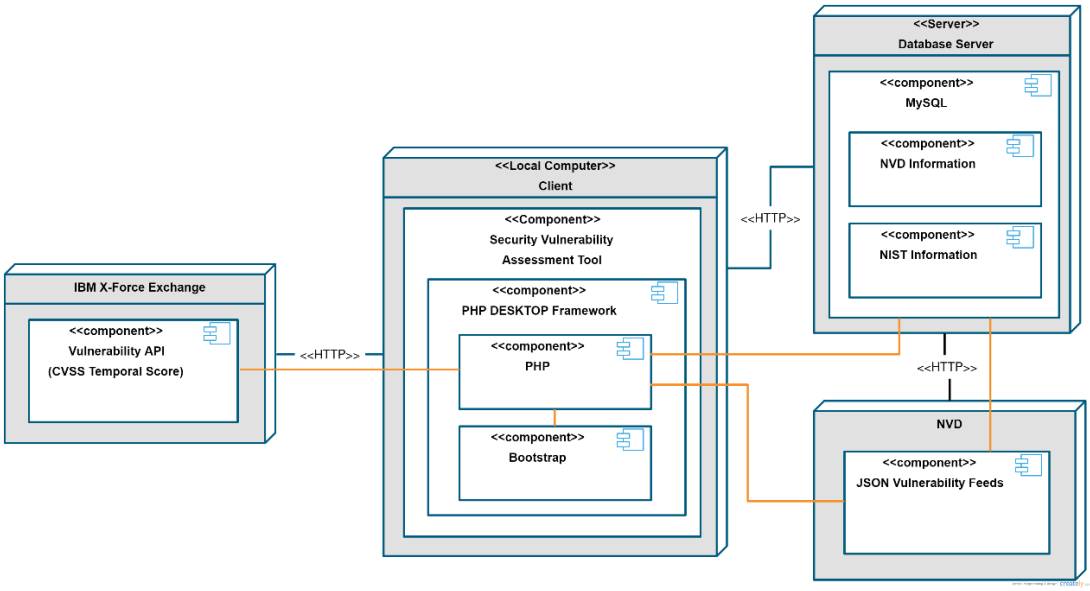
ภาพรวมโครงสร้างสถาปัตยกรรมของเครื่องมือสามารถแสดงได้ดังรูปที่ 4.2 โดยที่เครื่องมือจะแบ่งออกเป็น 2 ส่วนหลักๆ คือ

4.3.1 เครื่องมือที่พัฒนาที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์

ในส่วนนี้จะเป็นส่วนที่ผู้ใช้งานเข้ามาใช้งานเครื่องมือช่วยประเมินช่องโหว่ด้านความมั่นคงเพื่อการยกระดับเวอร์ชันของซอฟต์แวร์ โดยที่เครื่องมือมีหน้าที่ทำการค้นหารายชื่อซอฟต์แวร์ที่ติดตั้งในเครื่องคอมพิวเตอร์ เรียกใช้เอพีไอของไอบีเอ็มเอกซ์เอฟอี และติดต่อฐานข้อมูลที่ติดตั้งอยู่บนเครื่องเซิร์ฟเวอร์ เพื่อประมวลผลการเปรียบเทียบคะแนนซีวีเอสเอสระหว่างซอฟต์แวร์ที่ติดตั้งในเครื่องคอมพิวเตอร์และซอฟต์แวร์เวอร์ชันล่าสุด รวมถึงแสดงรายงานสถานะช่องโหว่บนเครื่องมือ

4.3.2 ฐานข้อมูลที่ให้บริการบนเครื่องเซิร์ฟเวอร์

เครื่องเซิร์ฟเวอร์จะมีหน้าที่ให้บริการฐานข้อมูลช่องโหว่ที่ได้จากเอ็นวีดีและคะแนนกลุ่มตัววัดตามสภาพแวดล้อมที่ได้จากแนวทางของ NIST รวมถึงมีหน้าที่ปรับปรุงข้อมูลช่องโหว่ที่ได้จากเอ็นวีดีให้เป็นปัจจุบันเมื่อผู้ใช้งานที่เป็นผู้ดูแลระบบต้องการปรับปรุงข้อมูลช่องโหว่



รูปที่ 4.2 ภาพรวมโครงสร้างสถาปัตยกรรมของเครื่องมือ

4.4. การพัฒนาเครื่องมือ

สภาพแวดล้อมและเครื่องมือที่ใช้ในการพัฒนาเครื่องมือช่วยประเมินช่องโหว่ด้านความมั่นคงเพื่อการยกระดับเวอร์ชันของซอฟต์แวร์ ประกอบไปด้วยรายการฮาร์ดแวร์และซอฟต์แวร์ดังต่อไปนี้

4.4.1 ฮาร์ดแวร์ที่ใช้ในการพัฒนาเครื่องมือ

1. เครื่องคอมพิวเตอร์ที่ใช้พัฒนาเครื่องมือ

- หน่วยประมวลผล Intel® Core™ i7-3520M CPU ความเร็ว 2.90GHz
- หน่วยความจำ 4 GB
- ฮาร์ดดิสก์ ความจุ 320 GB

2. เครื่องเซิร์ฟเวอร์ (Server)

- หน่วยประมวลผล Intel® Xeon® L5520 ความเร็ว 2.27GHz
- หน่วยความจำ 4 GB
- ฮาร์ดดิสก์ ความจุ 200 GB

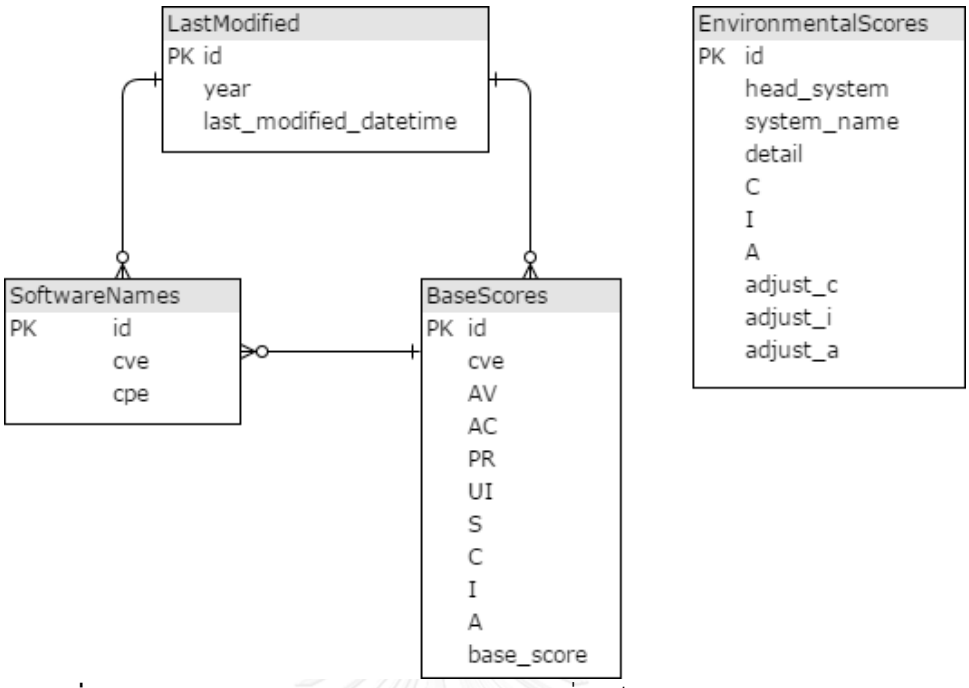
4.4.2 ซอฟต์แวร์ที่ใช้ในการพัฒนาเครื่องมือ

1. เน็ตบีนส์ ไอดีอี (NetBeans IDE 8.0.2)
2. มายเอสคิวแอล ดาต้าเบส 5.5.4 (MySQL Database 5.5.4)
3. พีเอชพีเดสก์ท็อป 47.5 (PHPDESKTOP 47.5)
4. อินโน เซตอัป คอมไพเลอร์ 5.5.9 (Inno Setup Compiler 5.5.9)
5. ระบบปฏิบัติการไมโครซอฟท์วินโดวส์ 7 (Microsoft windows 7) สำหรับเครื่องคอมพิวเตอร์ที่ใช้พัฒนาเครื่องมือ
6. ระบบปฏิบัติการลินุกซ์ (Linux) เวอร์ชัน 3.11.0-15-generic สำหรับเครื่องเซิร์ฟเวอร์

4.5. การพัฒนาเครื่องมือ

4.5.1 การจัดเตรียมข้อมูลช่องโหว่และคะแนนกลุ่มตัววัดตามสภาพแวดล้อม

ในขั้นตอนการจัดเตรียมข้อมูลช่องโหว่และคะแนนกลุ่มตัววัดตามสภาพแวดล้อม ซึ่งข้อมูลเหล่านี้จำเป็นสำหรับการพัฒนาเครื่องมือเป็นอย่างยิ่ง ดังนั้นเพื่อแสดงให้เห็นถึงความสัมพันธ์และรายละเอียดของโครงสร้างแต่ละตารางในฐานข้อมูลที่ใช้จัดเก็บข้อมูลช่องโหว่และคะแนนกลุ่มตัววัดตามสภาพแวดล้อมสามารถแสดงได้โดยใช้แผนภาพความสัมพันธ์ ดังรูปที่ 4.3



รูปที่ 4.3 แผนภาพความสัมพันธ์ของแต่ละตารางที่ใช้เก็บข้อมูลช่องโหว่และกลุ่มตัววัดตามสภาพแวดล้อม

4.5.2 การปรับปรุงฐานข้อมูลช่องโหว่

เมื่อเวลาผ่านไปทางซีวีอีได้มีการเผยแพร่ช่องโหว่ใหม่ออกมา ทางเอ็นวีดีจะให้คะแนนกลุ่มตัววัดพื้นฐานของช่องโหว่นั้นๆ หรือมีการปรับปรุงคะแนนกลุ่มตัววัดพื้นฐานของช่องโหว่เก่าแล้วเผยแพร่ข้อมูลผ่านไฟล์ทางเว็บไซต์ของเอ็นวีดีแล้ว จึงจำเป็นต้องมีการปรับปรุงฐานข้อมูลช่องโหว่ให้เป็นปัจจุบัน โดยวิธีการปรับปรุงฐานข้อมูลช่องโหว่จะเป็นการสั่งรันสคริปต์ไฟล์ (Script File) ที่เครื่องเซิร์ฟเวอร์เพื่อ ตรวจสอบว่าข้อมูลถูกปรับปรุงล่าสุดแล้วหรือไม่จากไฟล์ชื่อว่า .meta ของทางเอ็นวีดี โดยข้อมูลในไฟล์นี้จะบอกข้อมูลเกี่ยวกับ วันเวลาที่ปรับปรุงข้อมูลล่าสุดและขนาดไฟล์เจสัน ดังรูปที่ 4.4

```
lastModifiedDate:2015-09-10T08:40:09-04:00
size:1273382
zipSize:91619
gzSize:91477
sha256:ac782e2db403e2b09ad5dd676501e8755fda3f2bef347b7503491700c6c5eaff
```

รูปที่ 4.4 ข้อมูลภายในไฟล์ .meta

4.5.3 การเรียกใช้เอพีไอของ ไอบีเอ็ม เอกซ์เอฟอี

ในงานวิจัยนี้ต้องการพัฒนาเครื่องมือที่สามารถคำนวณคะแนนซีวีเอสเอสทั้ง 3 กลุ่ม โดยที่ในการค้นหาคะแนนในกลุ่มตัววัดตามเวลา จะได้มาจากการเรียกใช้เอพีไอของ ไอบีเอ็ม เอกซ์เอฟอี ซึ่ง

จะต้องส่งค่าตัวแปรรายการซีวีอี แล้วข้อมูลที่ได้รับตอบกลับมาจะอยู่ในรูปแบบเจสัน โดยข้อมูลที่ได้จะมีทั้งคะแนนกลุ่มตัววัดพื้นฐาน และคะแนนกลุ่มตัววัดตามเวลา ซึ่งในที่นี้จะสนใจเพียงคะแนนกลุ่มตัววัดตามเวลาเท่านั้น ดังตัวอย่างรูปที่ 4.5

```
                [temporal_score] => 4.1
                [remedy] => No remedy available as of October 1, 2014.
                [remedy_fmt] =>

        No remedy available as of October 1, 2014.


                [reported] => 2014-05-22T00:00:00Z
                [tagname] => conversionninja-wordpress-index-xss
                [stdcode] => Array
                    (
                        [0] => BID-67590
                        [1] => CVE-2014-4017
                    )

                [platforms_affected] => Array
                    (
                        [0] => WordPress Conversion Ninja Plugin for WordPress
                    )

                [platforms_dependent] => Array
                    (
                        [0] => WordPress WordPress
                    )

                [exploitability] => High
                [consequences] => Cross-Site Scripting
```

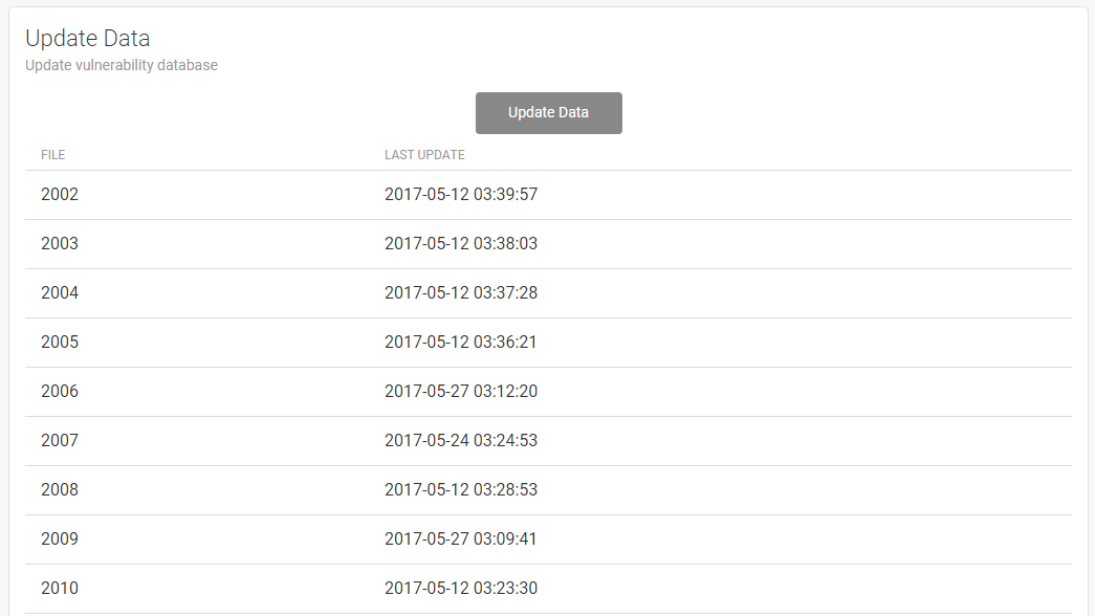
รูปที่ 4.5 ตัวอย่างข้อมูลตอบกลับจากการเรียกใช้เอพีไอของ ไอบีเอ็ม เอกซ์เอฟอี

4.6. การออกแบบและพัฒนาส่วนต่อประสานของผู้ใช้งานเครื่องมือ

การออกแบบและพัฒนาส่วนต่อประสานของผู้ใช้งานเครื่องมือมีวัตถุประสงค์เพื่อแสดงให้เห็นถึงองค์ประกอบของหน้าจอที่ต้องการให้ปรากฏในเครื่องมือที่กำลังจะพัฒนา โดยในปัจจุบันหน้าจอคอมพิวเตอร์มีหลากหลายขนาด จึงได้ออกแบบส่วนต่อประสานโดยใช้เฟรมเวิร์คบูตสแตรป (Bootstrap) และในส่วนของการแสดงผลที่เป็นกราฟ ได้มีการนำฟิวชันชาร์ต (Fusion Charts) เข้ามาใช้งานเพื่อให้สามารถแสดงผลได้ดีขึ้น

4.6.1 หน้าจอขั้นตอนการปรับปรุงฐานข้อมูลช่องโหว่ให้เป็นปัจจุบัน

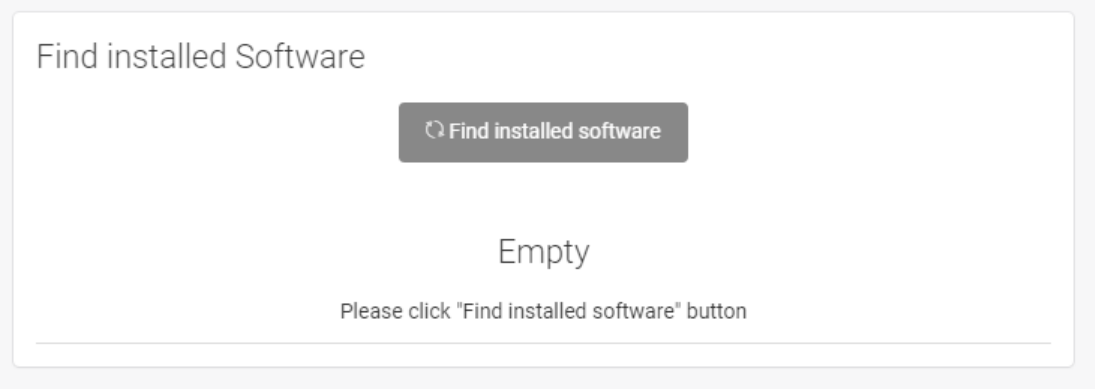
ผู้มีสิทธิ์ในการเข้าใช้ขั้นตอนนี้คือผู้ดูแลระบบขององค์กร โดยที่หน้าจอจะแสดงวันเวลาที่ปรับปรุงฐานข้อมูลช่องโหว่ครั้งล่าสุด จำนวนช่องโหว่ที่มีในฐานข้อมูล จำนวนรายการซีวีอีที่มีในฐานข้อมูล ซึ่งจะแยกแสดงตามปีเหมือนบนเว็บไซต์เอ็นวีดี ดังรูปที่ 4.6



รูปที่ 4.6 หน้าจอแสดงวันเวลาที่ปรับปรุงฐานข้อมูลช่องโหว่ครั้งล่าสุด

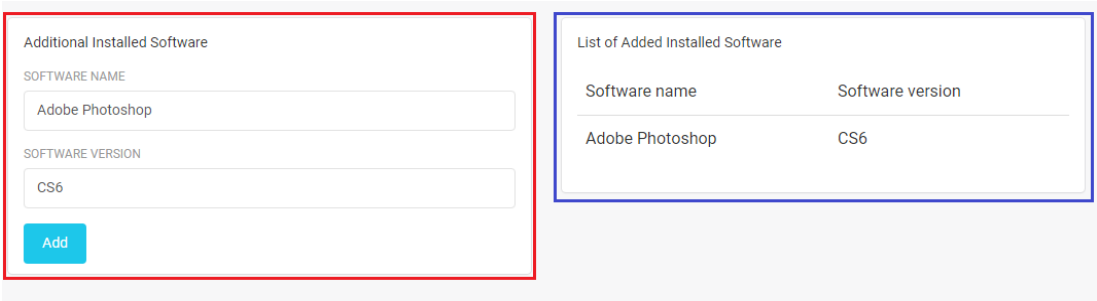
4.6.2 หน้าจอขั้นตอนประเมินผลช่องโหว่ด้านความมั่นคงของซอฟต์แวร์

เมื่อเข้ามาครั้งแรกไม่มีข้อมูลใดๆ แสดงบนหน้าจอ เมื่อกดค้นหารายชื่อซอฟต์แวร์ที่ติดตั้งในเครื่องคอมพิวเตอร์แล้ว เครื่องมือจะทำการค้นหารายชื่อซอฟต์แวร์ที่ติดตั้งในเครื่องคอมพิวเตอร์และแสดงผลว่ามีรายชื่อซอฟต์แวร์รายการใดอยู่บ้างดังรูปที่ 4.7



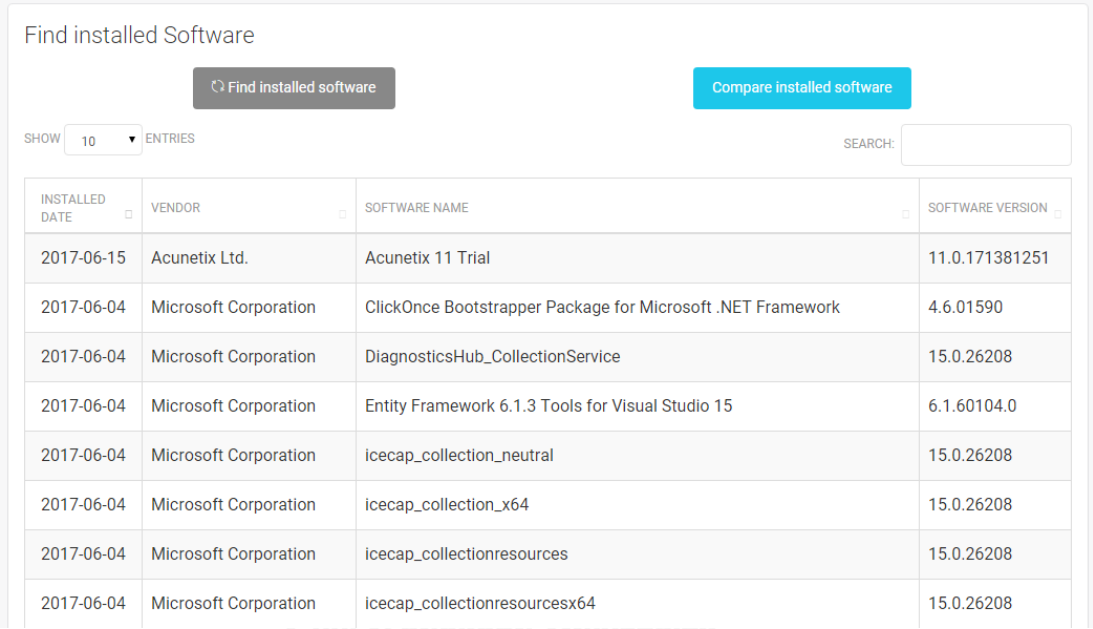
รูปที่ 4.7 หน้าจอก่อนการค้นหารายชื่อซอฟต์แวร์

และเนื่องจากเครื่องมือไม่สามารถค้นหารายชื่อซอฟต์แวร์ที่ไม่มีอยู่ในวินโดวส์รีจิสทรีได้ จึงได้เพิ่มฟังก์ชันในการเพิ่มรายชื่อซอฟต์แวร์และเวอร์ชันที่เครื่องมือไม่สามารถค้นพบได้เอง โดยในกรอบสีแดงด้านซ้ายจะให้กรอกข้อมูลรายชื่อซอฟต์แวร์และเวอร์ชันที่ต้องการ เมื่อกรอกเสร็จแล้วข้อมูลจะไปแสดงที่ตารางด้านขวาในกรอบสีน้ำเงิน ดังรูปที่ 4.8



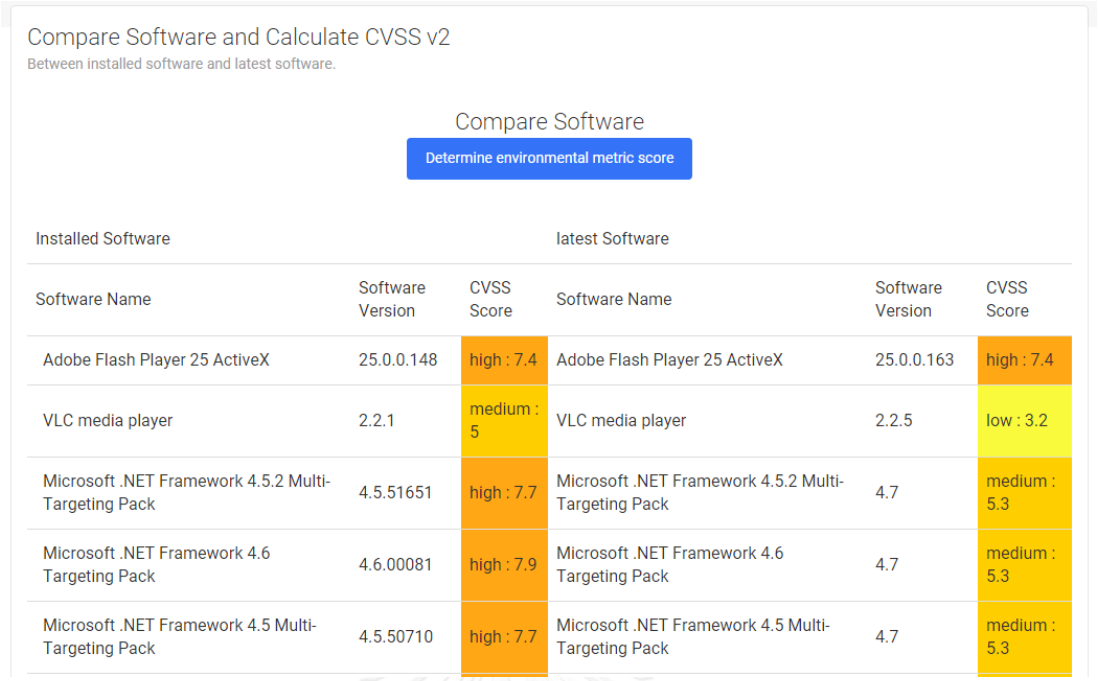
รูปที่ 4.8 หน้าจอแสดงฟังก์ชันการเพิ่มรายชื่อซอฟต์แวร์และเวอร์ชันเอง

เมื่อเครื่องมือค้นหารายชื่อซอฟต์แวร์ที่ติดตั้งในเครื่องคอมพิวเตอร์เรียบร้อยแล้วจะแสดงวันที่ติดตั้งซอฟต์แวร์ ผู้ขายผลิตภัณฑ์ซอฟต์แวร์ รายชื่อซอฟต์แวร์ และเวอร์ชันซอฟต์แวร์ ดังรูปที่ 4.9



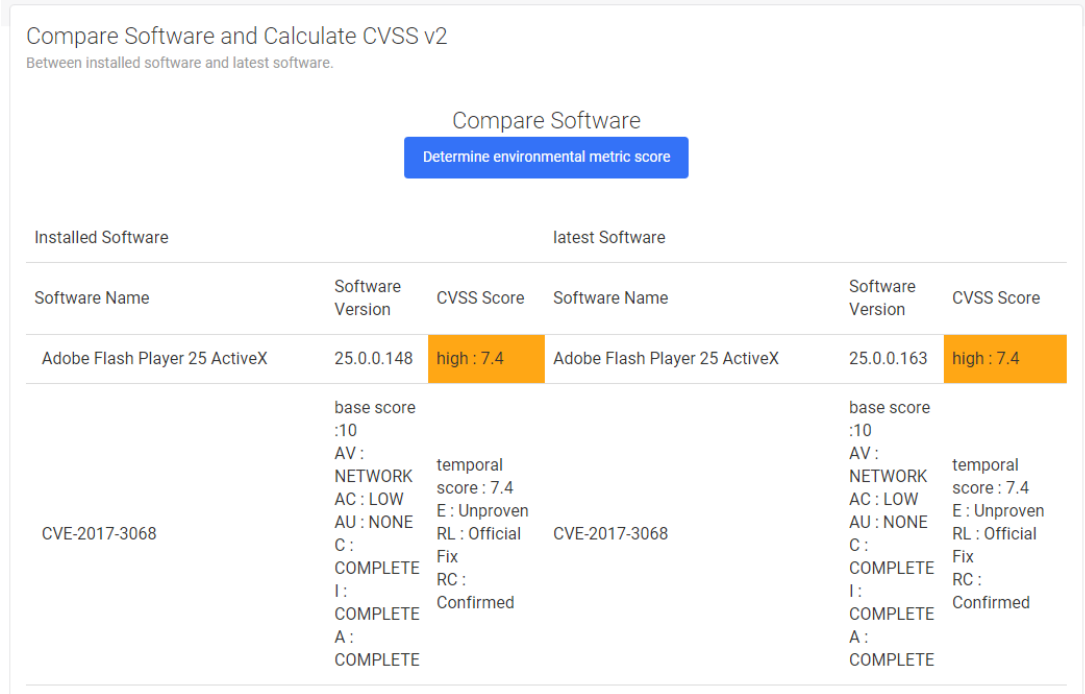
รูปที่ 4.9 หน้าจอแสดงผลหลังจากค้นหารายชื่อซอฟต์แวร์ที่ติดตั้งในคอมพิวเตอร์

หลังจากนั้นเมื่อกดปุ่มเปรียบเทียบซอฟต์แวร์แล้ว เครื่องมือจะแสดงผลการเปรียบเทียบซอฟต์แวร์ระหว่างซอฟต์แวร์เวอร์ชันที่ติดตั้งในเครื่องคอมพิวเตอร์ และซอฟต์แวร์เวอร์ชันล่าสุดที่มีในฐานข้อมูล รวมทั้งยังแสดงรายการซีวีอีของซอฟต์แวร์นั้นๆ และคะแนนซีวีเอสเอสที่ถูกคำนวณโดยกลุ่มตัววัดพื้นฐานและกลุ่มตัววัดตามเวลาดังรูปที่ 4.10



รูปที่ 4.10 หน้าจอแสดงผลการเปรียบเทียบระหว่างซอฟต์แวร์ 2 เวอร์ชัน

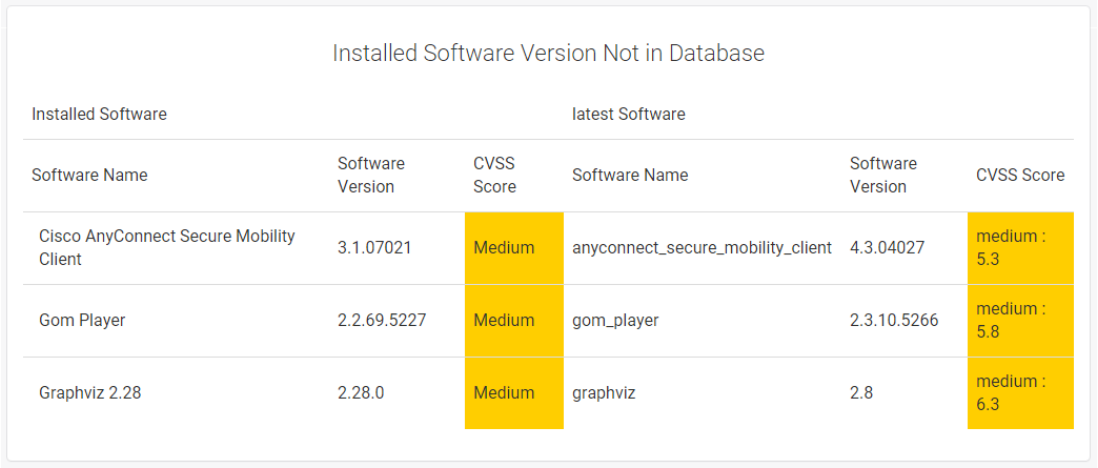
เมื่อคลิกที่ชื่อซอฟต์แวร์จะแสดงรายการซีวีอีของซอฟต์แวร์นั้นๆ และคะแนนกลุ่มตัววัดพื้นฐานและคะแนนในกลุ่มตัววัดตามเวลาดังรูปที่ 4.11



รูปที่ 4.11 หน้าจอแสดงรายการซีวีอีและคะแนนของซอฟต์แวร์

และเมื่อเลื่อนลงมาด้านล่างจะแสดงรายชื่อซอฟต์แวร์ที่ไม่มีข้อมูลช่องโหว่ปรากฏในฐานข้อมูลสำหรับทำการเปรียบเทียบได้ดังรูปที่ 4.13 ซึ่งมี 3 กรณี คือ

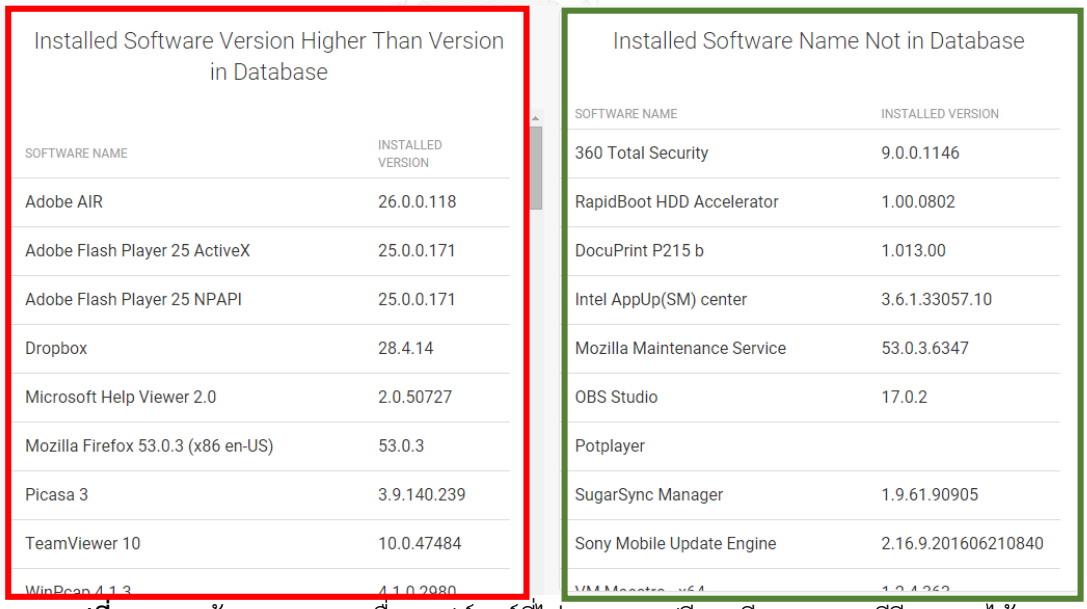
1. ซอฟต์แวร์เวอร์ชันที่ติดตั้งในเครื่องคอมพิวเตอร์ไม่ปรากฏในฐานข้อมูล แต่มีซอฟต์แวร์เวอร์ชันใหม่กว่าปรากฏในฐานข้อมูล ดังรูปที่ 4.12
2. ซอฟต์แวร์เวอร์ชันที่ติดตั้งในเครื่องคอมพิวเตอร์มีเวอร์ชันสูงกว่าซอฟต์แวร์เวอร์ชันล่าสุดที่ปรากฏในฐานข้อมูล ดังรูปที่ 4.13 ในกรอบสีแดง
3. ไม่พบชื่อซอฟต์แวร์ในฐานข้อมูลเลย ดังรูปที่ 4.13 ในกรอบสีเขียว



Installed Software Version Not in Database

Installed Software			latest Software		
Software Name	Software Version	CVSS Score	Software Name	Software Version	CVSS Score
Cisco AnyConnect Secure Mobility Client	3.1.07021	Medium	anyconnect_secure_mobility_client	4.3.04027	medium : 5.3
Gom Player	2.2.69.5227	Medium	gom_player	2.3.10.5266	medium : 5.8
Graphviz 2.28	2.28.0	Medium	graphviz	2.8	medium : 6.3

รูปที่ 4.12 หน้าจอแสดงผลการเปรียบเทียบระหว่างซอฟต์แวร์ 2 เวอร์ชันในกรณีที่ซอฟต์แวร์เวอร์ชันที่ติดตั้งในเครื่องคอมพิวเตอร์ไม่ปรากฏในฐานข้อมูล



Installed Software Version Higher Than Version in Database

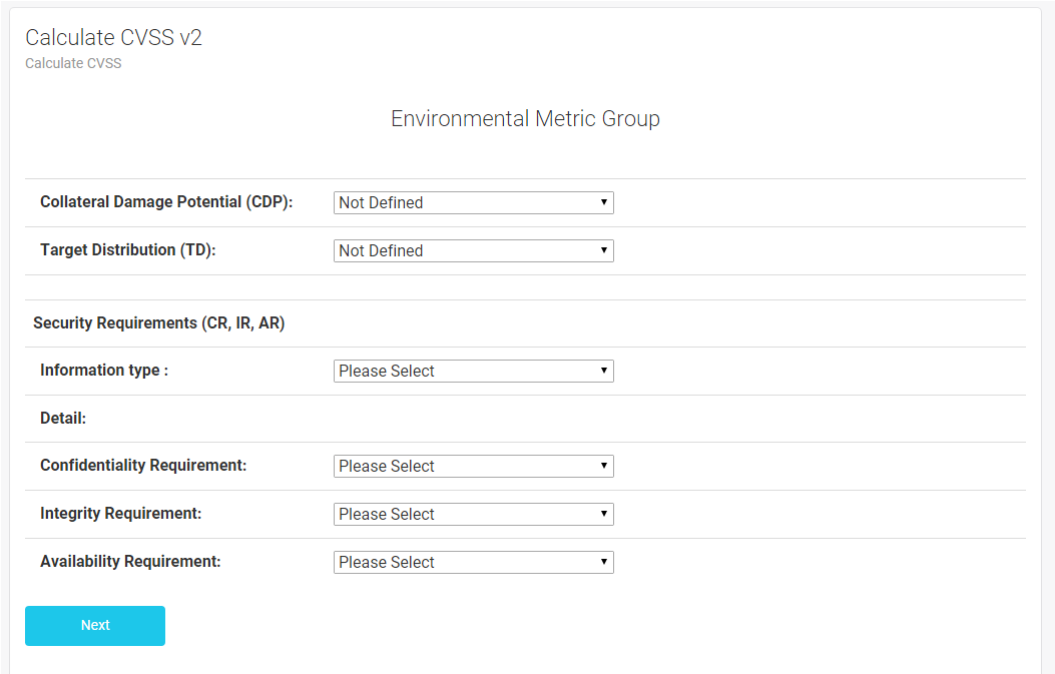
SOFTWARE NAME	INSTALLED VERSION
Adobe AIR	26.0.0.118
Adobe Flash Player 25 ActiveX	25.0.0.171
Adobe Flash Player 25 NPAPI	25.0.0.171
Dropbox	28.4.14
Microsoft Help Viewer 2.0	2.0.50727
Mozilla Firefox 53.0.3 (x86 en-US)	53.0.3
Picasa 3	3.9.140.239
TeamViewer 10	10.0.47484
WinPcap 4.1.3	4.1.0.2980

Installed Software Name Not in Database

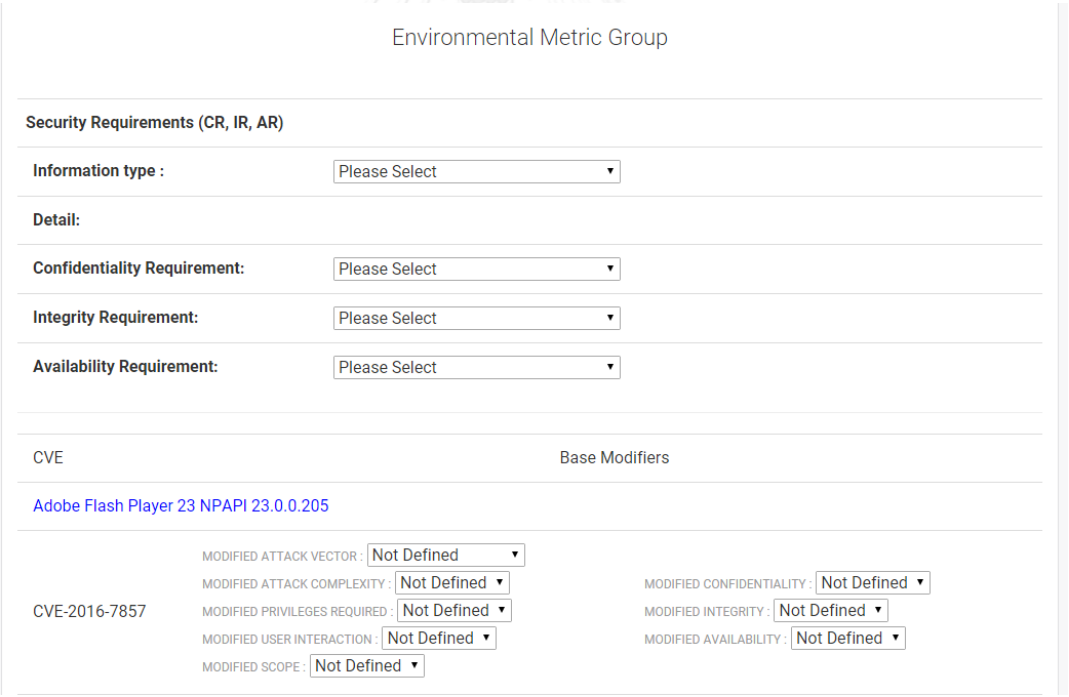
SOFTWARE NAME	INSTALLED VERSION
360 Total Security	9.0.0.1146
RapidBoot HDD Accelerator	1.00.0802
DocuPrint P215 b	1.013.00
Intel AppUp(SM) center	3.6.1.33057.10
Mozilla Maintenance Service	53.0.3.6347
OBS Studio	17.0.2
Potplayer	
SugarSync Manager	1.9.61.90905
Sony Mobile Update Engine	2.16.9.201606210840
VM Maestro x64	1.2.4.262

รูปที่ 4.13 หน้าจอแสดงรายชื่อซอฟต์แวร์ที่ไม่สามารถเปรียบเทียบคะแนนซีวีเอสเอสได้

หลังจากนั้นเมื่อคลิกปุ่มกำหนดคะแนนกลุ่มตัววัดตามสภาพแวดล้อม จะปรากฏหน้าจอให้กรอกข้อมูลกลุ่มตัววัดตามสภาพแวดล้อม โดยในหน้านี้หากเป็นการคำนวณคะแนนซีวีเอสเอสเวอร์ชัน 2 จะแสดงดังรูปที่ 4.14 และหากเป็นการคำนวณคะแนนซีวีเอสเอสเวอร์ชัน 3 จะเป็นดังรูปที่ 4.15



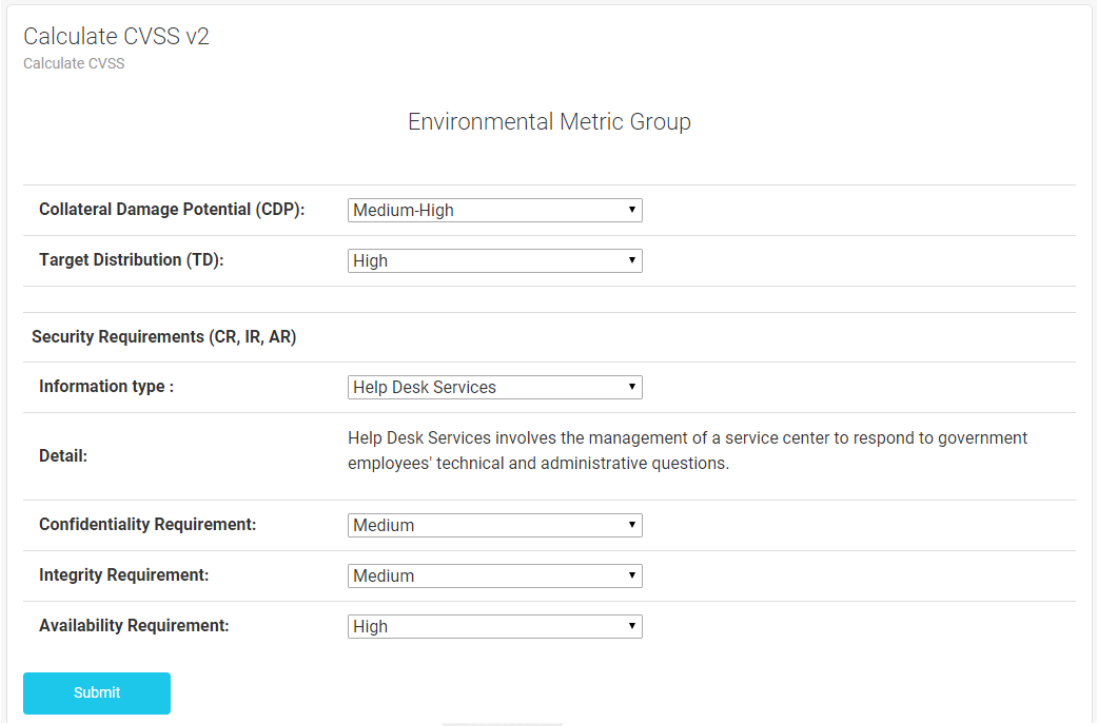
รูปที่ 4.14 หน้าจอการกรอกข้อมูลกลุ่มตัววัดตามสภาพแวดล้อมสำหรับการคำนวณคะแนนซีวีเอสเอสเวอร์ชัน 2



รูปที่ 4.15 หน้าจอการกรอกข้อมูลกลุ่มตัววัดตามสภาพแวดล้อมสำหรับการคำนวณคะแนนซีวีเอสเอสเวอร์ชัน 3

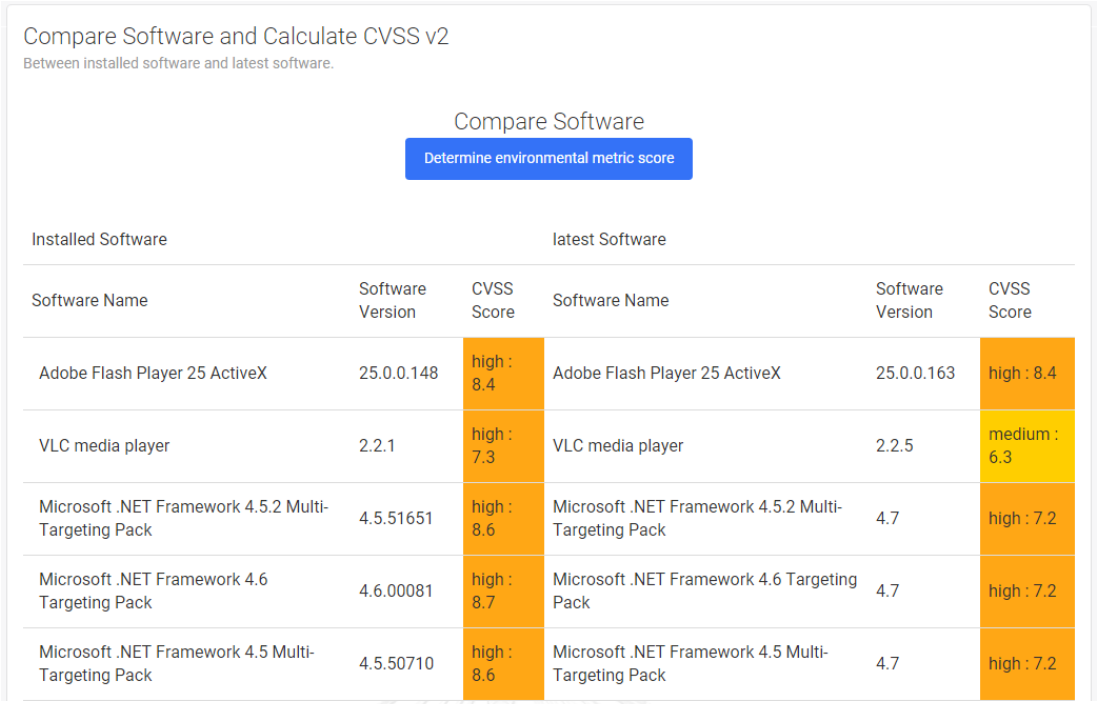
ในการกรอกข้อมูล Security Requirement สำหรับตัววัดตามสภาพแวดล้อม ส่วน Information type จะมีตัวเลือกปรากฏตามประเภทสารสนเทศที่กำหนดโดย NIST เมื่อเลือกประเภทแล้ว หน้าจอ

จะแสดงค่าโดยปริยาย (Default) ของ Confidentiality/Integrity/Availability Requirement ตามค่าระดับผลกระทบของประเภทสารสนเทศที่กำหนดโดย NIST เช่นกัน ทั้งนี้ผู้ดูแลระบบขององค์กรสามารถปรับค่าได้ตามความเหมาะสมขององค์กร



รูปที่ 4.16 หน้าจอแสดงข้อมูลหลักเลือก Security Requirement ตามประเภทสารสนเทศ

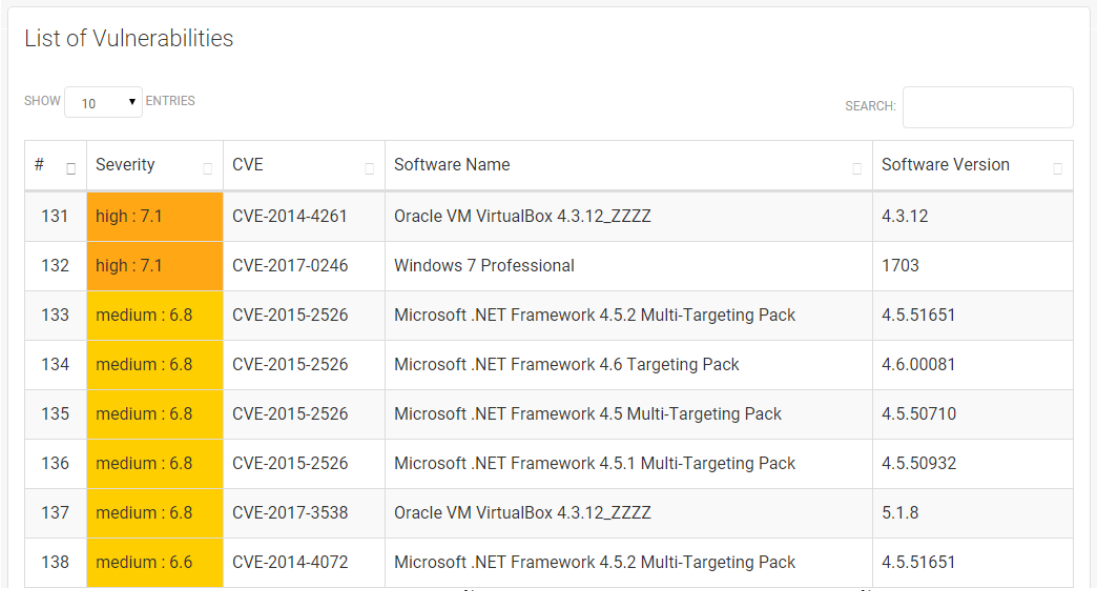
เมื่อกรอกข้อมูลกลุ่มตัววัดตามสภาพแวดล้อมเรียบร้อยแล้ว เครื่องมือจะกลับไปหน้าแสดงผลแสดงผลการเปรียบเทียบซอฟต์แวร์ระหว่างซอฟต์แวร์เวอร์ชันที่ติดตั้งในเครื่องคอมพิวเตอร์ และซอฟต์แวร์เวอร์ชันล่าสุดที่มีในฐานข้อมูลอีกครั้ง โดยในครั้งนี้คะแนนซีวีเอสเอสที่แสดงจะถูกคำนวณทั้ง 3 กลุ่มตัววัด คือ กลุ่มตัววัดพื้นฐาน กลุ่มตัววัดตามเวลาและกลุ่มตัววัดตามสภาพแวดล้อมดังรูปที่ 4.17



รูปที่ 4.17 หน้าจอแสดงรายการซีวีอีและคะแนนของซอฟต์แวร์หลังเพิ่มข้อมูลกลุ่มตัววัดตามสภาพแวดล้อม

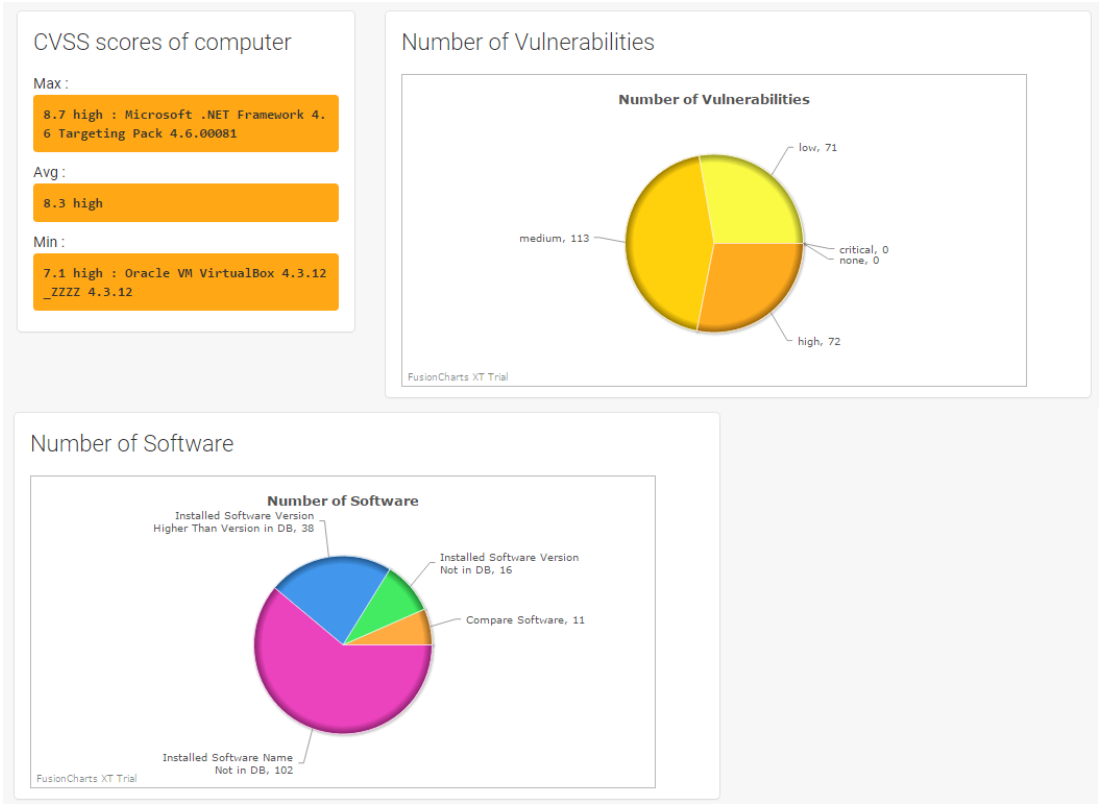
4.6.3 หน้าจอขั้นตอนการรายงานสถานะช่องโหว่

หน้าจอรายงานสถานะช่องโหว่ จะแสดงข้อมูลรายการซีวีอีทั้งหมดที่มีในซอฟต์แวร์เวอร์ชันติดตั้งในเครื่องคอมพิวเตอร์โดยที่ระดับความรุนแรงของช่องโหว่ที่ประเมินได้จะแสดงเป็นระดับสีแทนความรุนแรง สีส้มที่เข้มมากแสดงว่ารุนแรงมากกว่าสีส้มอ่อน ดังรูปที่ 4.18

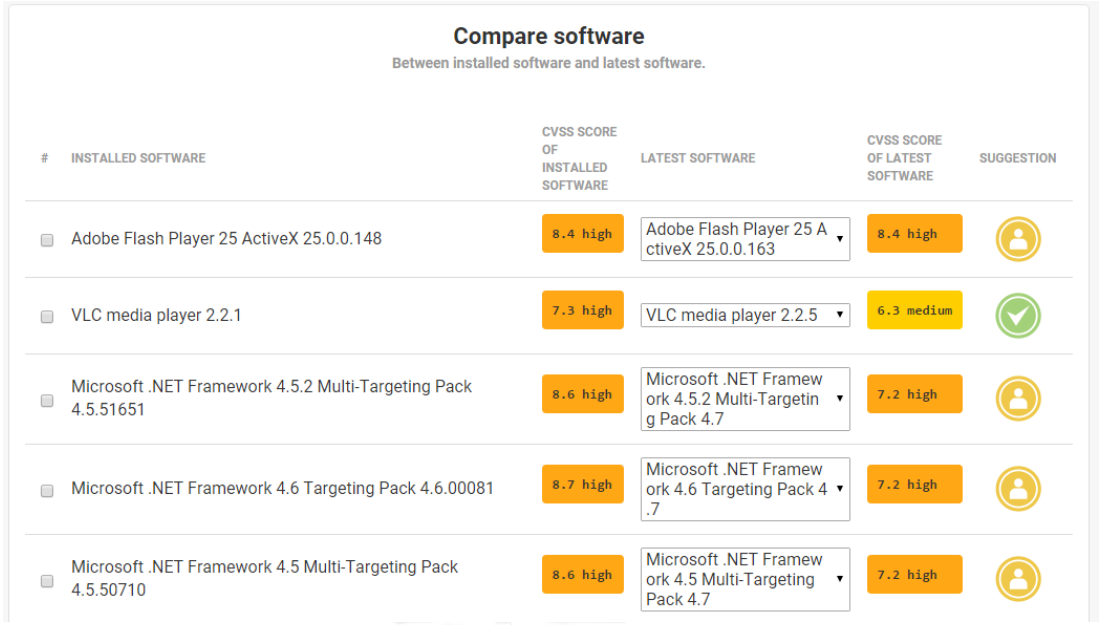


รูปที่ 4.18 หน้าจอแสดงรายการซีวีอีทั้งหมดที่มีในซอฟต์แวร์เวอร์ชันที่ติดตั้งในคอมพิวเตอร์

หน้าแดชบอร์ด (Dashboard) ดังรูปที่ 4.19 จะแสดงข้อมูลสถานะของช่องโหว่ต่างๆ เช่น คะแนนซีวีอีเฉลี่ยของเครื่องคอมพิวเตอร์นั้นๆ จำนวนซีวีอีของแต่ละซอฟต์แวร์เวอร์ชันนั้นที่มีในเครื่องคอมพิวเตอร์และจำนวนซอฟต์แวร์ที่ค้นพบ โดยจะแยกเป็น 4 กรณี ดังที่กล่าวไว้ในหัวข้อที่ 3.5 พร้อมทั้งแสดงผลการแนะนำการยกระดับเวอร์ชันซอฟต์แวร์ ดังรูปที่ 4.20 แต่เนื่องจากเครื่องมือไม่สามารถเปรียบเทียบคะแนนซีวีเอสเอสในกรณีที่มีการเปลี่ยนชื่อซอฟต์แวร์ หรือเป็นซอฟต์แวร์ประเภทเดียวกันแต่ผู้ผลิตต่างรายกันได้ดังนั้นเครื่องมือจึงสามารถให้ผู้ใช้งานเลือกชื่อของซอฟต์แวร์อื่นที่ต้องการเปรียบเทียบคะแนนซีวีเอสเอสกับซอฟต์แวร์เวอร์ชันที่มีในเครื่องคอมพิวเตอร์ได้โดยการคลิกที่ดร็อปดาวน์ (Dropdown) จะมีรายชื่อซอฟต์แวร์ที่มีในฐานข้อมูลแสดงขึ้นมาให้เลือก โดยเวอร์ชันที่แสดงจะเป็นเวอร์ชันล่าสุดของซอฟต์แวร์นั้น



รูปที่ 4.19 หน้าแดชบอร์ด



รูปที่ 4.20 หน้าแสดงผลการแนะนำการยกระดับเวอร์ชันซอฟต์แวร์

บทที่ 5
การทดสอบและประเมินผล

ในบทนี้จะกล่าวถึงการทดสอบและการประเมินผลเครื่องมือที่พัฒนาขึ้น โดยจะแบ่งออกเป็น 2 ส่วน คือ การประเมินผลแบบสอบถามความพึงพอใจจากผู้ใช้งานเครื่องมือ และการประเมินสมรรถนะของเครื่องมือ

5.1. ประเมินผลแบบสอบถามความพึงพอใจจากผู้ใช้งานเครื่องมือ

ประเมินผลแบบสอบถามความพึงพอใจจากผู้ใช้งานเครื่องมือซึ่งเป็นผู้ดูแลระบบขององค์กร 8 ราย และผู้ใช้งานทั่วไป 13 ราย

5.2. ประเมินสมรรถนะของเครื่องมือ

การประเมินสมรรถนะของเครื่องมือในด้านการค้นหารายการซีวีอีของช่องโหว่ของแต่ละซอฟต์แวร์เวอร์ชันจากฐานข้อมูลช่องโหว่ทำโดยเปรียบเทียบกับผลการค้นหารายการซีวีอีด้วยมือโดยผู้วิจัยเอง การวัดค่าสมรรถนะโดยใช้ ค่าเอฟ-เมเชอร์ (F-measure) ซึ่งเป็นค่าสมรรถนะโดยรวมที่พิจารณาจากค่าความเที่ยงตรงและค่าเรียกคืน โดยสูตรที่ใช้คำนวณ คือ

$$F = \frac{2 \times Precision \times Recall}{Precision + Recall}$$

ค่าความเที่ยงตรง (Precision) เป็นค่าที่บ่งบอกว่าเครื่องมือที่พัฒนาขึ้นสามารถค้นหารายการซีวีอีได้เที่ยงตรงเพียงใด โดยสูตรที่ใช้คำนวณ คือ

$$P = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FP}}$$

ค่าเรียกคืน (Recall) เป็นค่าที่บ่งบอกว่าเครื่องมือที่พัฒนาขึ้นสามารถค้นหารายการซีวีอีได้ครบถ้วนเพียงใด โดยสูตรที่ใช้คำนวณคือ

$$R = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}}$$

โดยที่ค่า

TP (True Positive) คือ จำนวนรายการซีวีอีของซอฟต์แวร์เวอร์ชันและเครื่องมือค้นหาพบจากฐานข้อมูลช่องโหว่

FP (False Positive) คือ จำนวนรายการซีวีอีที่ไม่ใช่ของซอฟต์แวร์เวอร์ชันแต่เครื่องมือค้นหาพบจากฐานข้อมูลช่องโหว่

FN (False Negative) คือ จำนวนรายการซีวีอีที่มีในซอฟต์แวร์เวอร์ชันแต่เครื่องมือค้นหาไม่พบจากฐานข้อมูลช่องโหว่

5.3. ผลการทดสอบเครื่องมือ

5.3.1 ผลการประเมินผลแบบสอบถามความพึงพอใจจากผู้ใช้งานเครื่องมือ

หลังจากให้ผู้ดูแลระบบขององค์กรและผู้ใช้งานทั่วไปลองทดสอบเครื่องมือเรียบร้อยแล้ว ได้ทำการประเมินผลความพึงพอใจจากผู้ใช้งานเครื่องมือ โดยจะประเมินจากผู้ดูแลระบบขององค์กร 8 ราย และผู้ใช้งานทั่วไป 13 ราย โดยในแต่ละข้อคะแนนจะอยู่ระหว่าง 1 ถึง 5 โดยที่ 5 คือคะแนนความพึงพอใจมากที่สุด และ 1 คือคะแนนความพึงพอใจน้อยที่สุด พบว่าได้ผลประเมินดังตารางที่ 5.1

ตารางที่ 5.1 ผลการประเมินผลแบบสอบถามความพึงพอใจจากผู้ใช้งานเครื่องมือ

หัวข้อที่ประเมิน	ผลการประเมิน					
	5	4	3	2	1	เฉลี่ย
ความสามารถของเครื่องมือในการค้นหารายชื่อซอฟต์แวร์ที่ติดตั้งในเครื่องคอมพิวเตอร์	9	11	1	0	0	4.38
ความรวดเร็วในการค้นหารายชื่อซอฟต์แวร์ที่ติดตั้งในเครื่องคอมพิวเตอร์	5	14	2	0	0	4.14
เครื่องมือสามารถเปรียบเทียบระหว่างซอฟต์แวร์ที่ติดตั้งในเครื่องคอมพิวเตอร์และซอฟต์แวร์เวอร์ชันล่าสุดในฐานข้อมูลได้จริง	8	12	1	0	0	4.33
ความรวดเร็วในการเปรียบเทียบระหว่างซอฟต์แวร์ที่ติดตั้งในเครื่องคอมพิวเตอร์และซอฟต์แวร์เวอร์ชันล่าสุดในฐานข้อมูล	5	12	4	0	0	4.05
ความรวดเร็วในการค้นหารายการซีวีอีของซอฟต์แวร์	5	15	1	0	0	4.19
ข้อมูลที่ได้รับเป็นประโยชน์ต่อพิจารณาการอัพเดทซอฟต์แวร์	9	11	1	0	0	4.38
ข้อมูลที่ได้รับทำให้เกิดแรงจูงใจในการอัพเดทซอฟต์แวร์	7	13	0	0	0	4.14
เครื่องมือใช้งานง่าย	11	9	1	0	0	4.48
ประสิทธิภาพโดยรวมของเครื่องมือ	6	15	0	0	0	4.29

จากตารางที่ 5.1 หัวข้อเครื่องมือใช้งานง่ายได้คะแนนเฉลี่ยสูงสุดคือ 4.48 รองลงมา คือหัวข้อความสามารถของเครื่องมือในการค้นหารายชื่อซอฟต์แวร์ที่ติดตั้งในเครื่องคอมพิวเตอร์และหัวข้อข้อมูลที่ได้รับเป็นประโยชน์ต่อพิจารณาการอัพเดทซอฟต์แวร์ ได้คะแนนเฉลี่ย 4.38 เท่ากัน ในหัวข้อ

ความรวดเร็วในการเปรียบเทียบระหว่างซอฟต์แวร์ที่ติดตั้งในเครื่องคอมพิวเตอร์และซอฟต์แวร์เวอร์ชันล่าสุดในฐานข้อมูลได้คะแนนเฉลี่ยน้อยสุดคือ 4.05 ซึ่งผู้ประเมินได้มีข้อเสนอแนะว่า เนื่องจากเครื่องมือประมวลผลช้าบ้าง ควรจะมีหน้าจอแสดงว่ากำลังโหลดในขณะที่โปรแกรมกำลังประมวลผลเพื่อตรวจสอบซอฟต์แวร์ภายในเครื่อง และมีข้อแนะนำอื่นๆ อีก เช่น อยากให้โปรแกรมสนับสนุนในหลายๆระบบปฏิบัติการ , น่าจะมีปุ่ม ให้กดเพื่อลิงก์ไปเว็บไซต์เพื่อดาวน์โหลดซอฟต์แวร์ และอยากให้สามารถตรวจสอบโปรแกรมได้มากกว่านี้

5.3.2 ผลการประเมินสมรรถนะของเครื่องมือ

เมื่อลองทดสอบเครื่องมือจากเครื่องของผู้ดูแลระบบขององค์กรและเครื่องของผู้ใช้งานทั่วไปแล้ว ได้ผลการทดลองสำหรับเครื่องของผู้ดูแลระบบขององค์กร จำนวน 8 เครื่อง ดังตารางที่ 5.2 ถึง ตารางที่ 5.9 และผลการทดลองสำหรับเครื่องของผู้ใช้งานทั่วไป จำนวน 13 เครื่อง ดังตารางที่ 5.10 ถึงตารางที่ 5.22

จากผลการทดลองของผู้ดูแลระบบขององค์กรเครื่องที่ 1 พบข้อมูลซอฟต์แวร์เวอร์ชันที่ติดตั้งในฐานข้อมูลจำนวน 6 รายการและไม่พบ 18 รายการ จากตารางที่ 5.2 ได้ค่า F-measure เป็น 0.9944 จะเห็นว่ามีข้อผิดพลาด (False Positive) ในการค้นหาซอฟต์แวร์ Microsoft Visual C++ 2008 Redistributable เนื่องจากในฐานข้อมูลบันทึกไว้ว่า cpe:/a:microsoft:visual_c%2 b%2 b:2 0 0 8 : redistribution_pkg ไม่ใช่ Redistributable เหมือนชื่อซอฟต์แวร์ที่ได้มาจากการค้นหาจากวินโดวส์ รีจิสทรีจึงไม่พบรายการซีวีอีที่ควรพบ 2 รายการ แต่ไปพบรายการซีวีอี 1 รายการที่ไม่ควรพบของ cpe:/a:microsoft:visual_c%2b%2b:2008 แทน

ตารางที่ 5.2 ผลการทดลองเครื่องของผู้ดูแลระบบขององค์กรเครื่องที่ 1

ชื่อซอฟต์แวร์	เวอร์ชันซอฟต์แวร์	TP	FP	FN	F-measure
Microsoft SQL Server 2012	11.1.3128.0	1	0	0	1
Microsoft Visual C++ 2008 Redistributable	9.0.30729.4974	0	1	2	0
Python 3.4.2	3.4.2150	5	0	0	1
Microsoft Visual Studio 2010	10.0.40219	4	0	0	1
Microsoft .NET Framework 4 Multi-Targeting Pack	4.0.30319	57	0	0	1
Windows Server 2012 R2 Standard	-	201	0	0	1
รวม		267	1	2	0.9944

จากผลการทดลองของผู้ดูแลระบบขององค์กรเครื่องที่ 2 พบข้อมูลซอฟต์แวร์เวอร์ชันที่ติดตั้งในฐานข้อมูลจำนวน 3 รายการและไม่พบ 20 รายการ จากตารางที่ 5.3 ได้ค่า F-measure เป็น 1 เนื่องจากหารายการซีวีอีของซอฟต์แวร์เวอร์ชันที่ติดตั้งในเครื่องคอมพิวเตอร์ครบ

ตารางที่ 5.3 ผลการทดลองเครื่องของผู้ดูแลระบบขององค์กรเครื่องที่ 2

ชื่อซอฟต์แวร์	เวอร์ชันซอฟต์แวร์	TP	FP	FN	F-measure
Windows Server 2012 R2 Standard	-	201	0	0	1
VMware vSphere Client 5.5	5.5.0.4216	1	0	0	1
Wireshark 2.2.3 (64-bit)	2.2.3	32	0	0	1
รวม		234	0	0	1

จากผลการทดลองของผู้ดูแลระบบขององค์กรเครื่องที่ 3 พบข้อมูลซอฟต์แวร์เวอร์ชันที่ติดตั้งในฐานข้อมูลจำนวน 4 รายการและไม่พบ 19 รายการ จากตารางที่ 5.4 ได้ค่า F-measure เป็น 0.9763 เนื่องจากเกิดความผิดพลาดในการค้นหาซอฟต์แวร์ Microsoft Visual C++ 2008 Redistributable เช่นเดียวกับที่กล่าวไปแล้วในผลการทดลองเครื่องของผู้ดูแลระบบขององค์กรเครื่องที่ 1

ตารางที่ 5.4 ผลการทดลองเครื่องของผู้ดูแลระบบขององค์กรเครื่องที่ 3

ชื่อซอฟต์แวร์	เวอร์ชันซอฟต์แวร์	TP	FP	FN	F-measure
Microsoft .NET Framework 4 Multi-Targeting Pack	4.0.30319	57	0	0	1
Microsoft SQL Server 2012 (64-bit)	-	1	0	0	1
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4974	9.0.30729.4974	0	1	2	0
Microsoft Visual Studio 2010 Shell (Integrated) - ENU	10.0.40219	4	0	0	1
รวม		62	1	2	0.9763

จากผลการทดลองของผู้ดูแลระบบขององค์กรเครื่องที่ 4 พบข้อมูลซอฟต์แวร์เวอร์ชันที่ติดตั้งในฐานข้อมูลจำนวน 4 รายการและไม่พบ 21 รายการ จากตารางที่ 5.5 ได้ค่า F-measure เป็น 0.9926 เนื่องจากเกิดความผิดพลาดในการค้นหาซอฟต์แวร์ Microsoft Visual C++ 2008 Redistributable เช่นเดียวกับที่กล่าวไปแล้วในผลการทดลองเครื่องของผู้ดูแลระบบขององค์กรเครื่องที่ 1 และเครื่องที่ 3

ตารางที่ 5.5 ผลการทดลองเครื่องของผู้ดูแลระบบขององค์กรเครื่องที่ 4

ชื่อซอฟต์แวร์	เวอร์ชันซอฟต์แวร์	TP	FP	FN	F-measure
Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.4148	9.0.30729.4148	0	1	2	0
VMware vSphere Client 5.5	5.5.0.3165	1	0	0	0
Windows Server 2012 R2 Standard	-	201	0	0	0
OpenVPN 2.3.13-I601	2.3.13-I601	1	0	0	0
รวม		203	1	2	0.9926

จากผลการทดลองของผู้ดูแลระบบขององค์กรเครื่องที่ 5 พบข้อมูลซอฟต์แวร์เวอร์ชันที่ติดตั้งในฐานข้อมูลจำนวน 3 รายการและไม่พบ 57 รายการ จากตารางที่ 5.6 ได้ค่า F-measure เป็น 1 เนื่องจากหารายการซีวีอีของซอฟต์แวร์เวอร์ชันที่ติดตั้งในเครื่องคอมพิวเตอร์ครบ

ตารางที่ 5.6 ผลการทดลองเครื่องของผู้ดูแลระบบขององค์กรเครื่องที่ 5

ชื่อซอฟต์แวร์	เวอร์ชันซอฟต์แวร์	TP	FP	FN	F-measure
Microsoft SQL Server 2012 Native Client	11.0.2100.60	1	0	0	1
Microsoft SQL Server 2014 Transact-SQL ScriptDom	12.0.2000.8	1	0	0	1
Windows Server 2012 R2 Standard	-	201	0	0	1
รวม		203	0	0	1

จากผลการทดลองของผู้ดูแลระบบขององค์กรเครื่องที่ 6 พบข้อมูลซอฟต์แวร์เวอร์ชันที่ติดตั้งในฐานข้อมูลจำนวน 2 รายการและไม่พบ 4 รายการ จากตารางที่ 5.7 ได้ค่า F-measure เป็น 1 เนื่องจากหารายการซีวีอีของซอฟต์แวร์เวอร์ชันที่ติดตั้งในเครื่องคอมพิวเตอร์ครบ

ตารางที่ 5.7 ผลการทดลองเครื่องของผู้ดูแลระบบขององค์กรเครื่องที่ 6

ชื่อซอฟต์แวร์	เวอร์ชันซอฟต์แวร์	TP	FP	FN	F-measure
Windows Server 2012 R2 Standard	-	201	0	0	1
7-Zip 15.14	15.14	1	0	0	1
รวม		202	0	0	1

จากผลการทดลองของผู้ดูแลระบบขององค์กรเครื่องที่ 7 พบข้อมูลซอฟต์แวร์เวอร์ชันที่ติดตั้งในฐานข้อมูลจำนวน 2 รายการและไม่พบ 1 รายการ จากตารางที่ 5.8 ได้ค่า F-measure เป็น 1 เนื่องจากหารายการซีวีอีของซอฟต์แวร์เวอร์ชันที่ติดตั้งในเครื่องคอมพิวเตอร์ครบ

ตารางที่ 5.8 ผลการทดลองเครื่องของผู้ดูแลระบบขององค์กรเครื่องที่ 7

ชื่อซอฟต์แวร์	เวอร์ชันซอฟต์แวร์	TP	FP	FN	F-measure
Microsoft Windows XP	5.2	110	0	0	1
Ipswitch WhatsUp Gold Premium Edition v11	11.00.0004	1	0	0	1
รวม		111	0	0	1

จากผลการทดลองของผู้ดูแลระบบขององค์กรเครื่องที่ 8 พบข้อมูลซอฟต์แวร์เวอร์ชันที่ติดตั้งในฐานข้อมูลจำนวน 5 รายการและไม่พบ 11 รายการ จากตารางที่ 5.9 ได้ค่า F-measure เป็น 0.9820 เนื่องจากมีข้อผิดพลาดในการหารายการซีวีอีของซอฟต์แวร์ PRTG Network Monitor เวอร์ชัน 8 ซึ่งไม่มีเวอร์ชันนี้ในฐานข้อมูล แต่เครื่องมือไปพบรายการซีวีอี 1 รายการของซอฟต์แวร์ cpe:/a:paessler:prtg_network_monitor:14.4.12.3282 เพราะชื่อในฐานข้อมูลมีเลข 8 ประกอบอยู่ด้วย จึงทำให้ค้นหารายการซีวีอีผิดพลาด และมีข้อผิดพลาดในการหารายการซีวีอีของซอฟต์แวร์ Update for Microsoft .NET Framework 3.5 SP1 (KB963707) ซึ่งรายการนี้ไม่มีในฐานข้อมูล แต่เครื่องมือพบรายการซีอีวี 2 รายการของซอฟต์แวร์ cpe:/a:microsoft:forefront_unified_access_gateway:2010:sp1_update1

ตารางที่ 5.9 ผลการทดลองเครื่องของผู้ดูแลระบบขององค์กรเครื่องที่ 8

ชื่อซอฟต์แวร์	เวอร์ชันซอฟต์แวร์	TP	FP	FN	F-measure
Microsoft .NET Framework 4.5.2	4.5.51209	42	0	0	1
PRTG Network Monitor	8	0	1	0	0
Update for Microsoft .NET Framework 3.5 SP1 (KB963707)	1	0	2	0	0
Wireshark 1.4.4	1.4.4	38	0	0	1
Windows Server (R) 2008 Standard	6.0	2	0	0	1
รวม		82	3	0	0.9820

จากผลการทดลองของผู้ใช้งานทั่วไปเครื่องที่ 1 พบข้อมูลซอฟต์แวร์เวอร์ชันที่ติดตั้งในฐานข้อมูลจำนวน 11 รายการและไม่พบ 154 รายการ จากตารางที่ 5.10 ได้ค่า F-measure เป็น 1 เนื่องจากหารายการซีวีอีของซอฟต์แวร์เวอร์ชันที่ติดตั้งในเครื่องคอมพิวเตอร์ครบ

ตารางที่ 5.10 ผลการทดลองเครื่องของผู้ใช้งานทั่วไปเครื่องที่ 1

ชื่อซอฟต์แวร์	เวอร์ชันซอฟต์แวร์	TP	FP	FN	F-measure
Adobe Flash Player 25 ActiveX	25.0.0.148	7	0	0	1
Microsoft .NET Framework 4.5 Multi-Targeting Pack	4.5.50710	42	0	0	1
Microsoft .NET Framework 4.5.1 Multi-Targeting Pack	4.5.50932	23	0	0	1
Microsoft .NET Framework 4.5.2 Multi-Targeting Pack	4.5.51651	28	0	0	1
Microsoft .NET Framework 4.6 Targeting Pack	4.6.00081	23	0	0	1
Microsoft .NET Framework 4.6.1	4.6.01055	8	0	0	1
Microsoft .NET Framework 4.6.1 Targeting Pack	4.6.01055	8	0	0	1

ตารางที่ 5.10 ผลการทดลองเครื่องของผู้ใช้งานทั่วไปเครื่องที่ 1 (ต่อ)

ชื่อซอฟต์แวร์	เวอร์ชันซอฟต์แวร์	TP	FP	FN	F-measure
Oracle VM VirtualBox 4.3.12_ZZZZ	4.3.12	2	0	0	1
Python 3.4.2 (64-bit)	3.4.2150	5	0	0	1
Windows 7 Professional	6.1	1	0	0	1
VLC media player	2.2.1	2	0	0	1
รวม		149	0	0	1

จากผลการทดลองของผู้ใช้งานทั่วไปเครื่องที่ 2 พบข้อมูลซอฟต์แวร์เวอร์ชันที่ติดตั้งในฐานข้อมูลจำนวน 5 รายการและไม่พบ 73 รายการ จากตารางที่ 5.11 ได้ค่า F-measure เป็น 0.1333 เนื่องจากมีข้อผิดพลาดในการหารายการซีวีอีของซอฟต์แวร์ Dota 2 คือ รายชื่อซอฟต์แวร์นี้ไม่มีในฐานข้อมูล แต่เครื่องมือไปค้นพบรายการซีวีอีของซอฟต์แวร์ dota openstats เพราะว่าในฐานข้อมูลบันทึกไว้ว่า cpe:/a:neubivljiv:dota_openstats และในฐานข้อมูลไม่มีรายชื่อซอฟต์แวร์ Microsoft Office Office 64-bit Components 2010 แต่เครื่องมือหารายการซีวีอีของ Microsoft Office Office 2010 เนื่องจากในฐานข้อมูลบันทึกไว้ว่า cpe:/a:microsoft:office:2010 แทน และความผิดพลาดในการหารายการซีวีอีของซอฟต์แวร์ Microsoft Visual C++ 2008 Redistributable ดังที่กล่าวไปแล้วข้างต้น

ตารางที่ 5.11 ผลการทดลองเครื่องของผู้ใช้งานทั่วไปเครื่องที่ 2

ชื่อซอฟต์แวร์	เวอร์ชันซอฟต์แวร์	TP	FP	FN	F-measure
Dota 2	-	0	1	0	0
Microsoft Office Office 64-bit Components 2010	14.0.4763.1000	0	6	0	0
Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.4148	9.0.30729.4148	0	1	2	0
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148	9.0.30729.4148	0	1	2	0
VMware vSphere Client 5.5	5.5.0.3165	1	0	0	1
รวม		1	9	4	0.1333

จากผลการทดลองของผู้ใช้งานทั่วไปเครื่องที่ 3 พบข้อมูลซอฟต์แวร์เวอร์ชันที่ติดตั้งในฐานข้อมูลจำนวน 9 รายการและไม่พบ 73 รายการจากตารางที่ 5.12 ได้ค่า F-measure เป็น 0.8235 เนื่องจากมีข้อผิดพลาดในการหารายการซีวีอีของซอฟต์แวร์ 3CDaemon คือรายชื่อซอฟต์แวร์ 3CDaemon ที่ได้จากการค้นหาจากวินโดวส์รีจิสทรี ค้นหาเวอร์ชันไม่พบ ทำให้เครื่องมือค้นหารายการซีวีอีผิดพลาดไปค้นเจอรายการซีวีอีของ 3CDaemon เวอร์ชัน 2.0 แทน และเครื่องมือค้นพบรายการซีวีอีของ Dota 2, Microsoft Office Office 64-bit Components 2010, Microsoft Visual C++ 2008 Redistributable ดังที่กล่าวไปแล้วข้างต้น

ตารางที่ 5.12 ผลการทดลองเครื่องของผู้ใช้งานทั่วไปเครื่องที่ 3

ชื่อซอฟต์แวร์	เวอร์ชันซอฟต์แวร์	TP	FP	FN	F-measure
3CDaemon	-	0	5	0	0
Dota 2	-	0	1	0	0
Microsoft .NET Framework 4.6.1	4.6.01055	8	0	0	1
Microsoft Office Office 64-bit Components 2010	14.0.4763.1000	0	6	0	0
Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.4148	9.0.30729.4148	0	1	2	0
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148	9.0.30729.4148	0	1	2	0
VMware vSphere Client 5.0	5.0.0.16964	2	0	0	1
Windows 7 Professional	6.1	1	0	0	1
Wireshark 2.2.4 (64-bit)	2.2.4	31	0	0	1
รวม		42	14	4	0.8235

จากผลการทดลองของผู้ใช้งานทั่วไปเครื่องที่ 4 พบข้อมูลซอฟต์แวร์เวอร์ชันที่ติดตั้งในฐานข้อมูลจำนวน 14 รายการและไม่พบ 276 รายการจากตารางที่ 5.13 ได้ค่า F-measure เป็น 0.9962 เนื่องจากมีข้อผิดพลาดในการหารายการซีวีอีของซอฟต์แวร์ Update for Microsoft .NET Framework 4.6.1 (KB4014553) ซึ่งรายการนี้ไม่มีในฐานข้อมูล แต่เครื่องมือพบรายการซีอีวี 2 รายการของซอฟต์แวร์ cpe:/a:microsoft:forefront_unified_access_gateway:2010:sp1_update1

ตารางที่ 5.13 ผลการทดลองเครื่องของผู้ใช้งานทั่วไปเครื่องที่ 4

ชื่อซอฟต์แวร์	เวอร์ชันซอฟต์แวร์	TP	FP	FN	F-measure
Cisco AnyConnect Secure Mobility Client	3.1.07021	4	0	0	1
Microsoft .NET Framework 4 Multi-Targeting Pack	4.0.30319	57	0	0	1
Microsoft .NET Framework 4.5 Multi-Targeting Pack	4.5.50709	42	0	0	1
Microsoft .NET Framework 4.6.1	4.6.01055	8	0	0	1
Microsoft SQL Server 2012 Command Line Utilities	11.0.2100.60	1	0	0	1
Microsoft SQL Server 2012 Data-Tier App Framework	11.0.2316.0	1	0	0	1
Microsoft SQL Server 2012 Native Client	11.0.2100.60	1	0	0	1
Microsoft SQL Server 2012 T-SQL Language Service	11.0.2100.60	1	0	0	1
Microsoft SQL Server 2012 Transact-SQL Compiler Service	11.0.2100.60	1	0	0	1
Microsoft SQL Server 2012 Transact-SQL ScriptDom	11.0.2100.60	1	0	0	1
QuickTime 7	7.78.80.95	92	0	0	1
Update for Microsoft .NET Framework 4.6.1 (KB4014553)	1	0	2	0	0
Windows 7 Professional	6.1	1	0	0	1
Wireshark 1.12.7 (64-bit)	1.12.7	55	0	0	1
รวม		265	2	0	0.9962

จากผลการทดลองของผู้ใช้งานทั่วไปเครื่องที่ 5 พบข้อมูลซอฟต์แวร์เวอร์ชันที่ติดตั้งในฐานข้อมูลจำนวน 3 รายการและไม่พบ 18 รายการ จากตารางที่ 5.14 ได้ค่า F-measure เป็น 0.8571 เนื่องจากมีข้อผิดพลาดในการหารายการซีวีอีของซอฟต์แวร์ Java(TM) 7 คือรายชื่อซอฟต์แวร์ JAVA(TM) 7 ไม่มีในฐานข้อมูล แต่ไปเจอรายการซีวีอีของซอฟต์แวร์ cpe:/a:ibm:java_sdk:7.0.0.0 แทน

ตารางที่ 5.14 ผลการทดลองเครื่องของผู้ใช้งานทั่วไปเครื่องที่ 5

ชื่อซอฟต์แวร์	เวอร์ชันซอฟต์แวร์	TP	FP	FN	F-measure
Java(TM) 7	7.0.0	0	1	0	0
OpenVPN 2.4.0-I602	2.4.0-I602	2	0	0	1
WinSCP 4.3.2	4.3.2	1	0	0	1
รวม		3	1	0	0.8571

จากผลการทดลองของผู้ใช้งานทั่วไปเครื่องที่ 6 พบข้อมูลซอฟต์แวร์เวอร์ชันที่ติดตั้งในฐานข้อมูลจำนวน 10 รายการและไม่พบ 173 รายการ จากตารางที่ 5.15 ได้ค่า F-measure เป็น 0.9993 เนื่องจากมีข้อผิดพลาดในการหารายการซีวีอีของซอฟต์แวร์ Microsoft Visual C++ 2008 Redistributable ดังที่กล่าวไปแล้วข้างต้น

ตารางที่ 5.15 ผลการทดลองเครื่องของผู้ใช้งานทั่วไปเครื่องที่ 6

ชื่อซอฟต์แวร์	เวอร์ชันซอฟต์แวร์	TP	FP	FN	F-measure
Adobe AIR	2.5.1.17730	66	0	0	1
OpenVPN 2.3.13-I601	2.3.13-I601	1	0	0	1
Microsoft Visual C++ 2008 Redistributable	9.0.30729.4974	0	1	2	0
Microsoft Office Visio 2010	14.0.7015.1000	1	0	0	1
Microsoft Excel MUI (English) 2013	15.0.4569.1506	3	0	0	1
Microsoft Word MUI (English) 2013	15.0.4569.1506	1	0	0	1
Microsoft Outlook MUI (English) 2013	15.0.4569.1506	1	0	0	1

ตารางที่ 5.15 ผลการทดลองเครื่องของผู้ใช้งานทั่วไปเครื่องที่ 6 (ต่อ)

ชื่อซอฟต์แวร์	เวอร์ชันซอฟต์แวร์	TP	FP	FN	F-measure
Microsoft Word MUI (English) 2013	15.0.4569.1506	2	0	0	1
Microsoft SQL Server 2005 Compact Edition [ENU]	3.1.0000	1	0	0	1
Windows 8.1 Pro	6.3	669	0	0	1
รวม		745	0	1	0.9993

จากผลการทดลองของผู้ใช้งานทั่วไปเครื่องที่ 7 พบข้อมูลซอฟต์แวร์เวอร์ชันที่ติดตั้งในฐานข้อมูลจำนวน 4 รายการและไม่พบ 39 รายการ จากตารางที่ 5.16 ได้ค่า F-measure เป็น 0.9915 เนื่องจากมีข้อผิดพลาดในการหารายการซีวีอีของซอฟต์แวร์ Java(TM) 7 ดังที่กล่าวไปแล้วข้างต้น

ตารางที่ 5.16 ผลการทดลองเครื่องของผู้ใช้งานทั่วไปเครื่องที่ 7

ชื่อซอฟต์แวร์	เวอร์ชันซอฟต์แวร์	TP	FP	FN	F-measure
Java(TM) 7	7.0.0	0	1	0	0
Microsoft .NET Framework 4 Client Profile	4.0.30319	57	0	0	1
OpenVPN 2.3.4-I003	2.3.4-I003	1	0	0	1
Windows 7 Professional	6.1	1	0	0	1
รวม		59	1	0	0.9915

จากผลการทดลองของผู้ใช้งานทั่วไปเครื่องที่ 8 พบข้อมูลซอฟต์แวร์เวอร์ชันที่ติดตั้งในฐานข้อมูลจำนวน 12 รายการและไม่พบ 100 รายการ จากตารางที่ 5.17 ได้ค่า F-measure เป็น 0.9865 เนื่องจากมีข้อผิดพลาดในการหารายการซีวีอีของซอฟต์แวร์ Microsoft Visual C++ 2008 Redistributable ดังที่กล่าวไปแล้วข้างต้น

ตารางที่ 5.17 ผลการทดลองเครื่องของผู้ใช้งานทั่วไปเครื่องที่ 8

ชื่อซอฟต์แวร์	เวอร์ชันซอฟต์แวร์	TP	FP	FN	F-measure
Foxit Reader	8.0.2.805	1	0	0	1
Mozilla Firefox 48.0 (x86 en-US)	48.0	18	0	0	1
VLC media player	2.2.4	5	0	0	1
Wireshark 1.12.4 (32-bit)	1.12.4	75	0	0	1
VMware vSphere Client 5.5	5.5.0.6352	1	0	0	1
Oracle VM VirtualBox 5.1.10	5.1.10	1	0	0	1
Microsoft Office Excel MUI (Thai) 2010	14.0.7015.1000	3	0	0	1
Microsoft Office PowerPoint MUI (Thai) 2010	14.0.7015.1000	2	0	0	1
Microsoft Office Publisher MUI (Thai) 2010	14.0.7015.1000	2	0	0	1
Microsoft Office Word MUI (Thai) 2010	14.0.7015.1000	1	0	0	1
Microsoft Office OneNote MUI (Thai) 2010	14.0.7015.1000	1	0	0	1
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.17	9.0.30729	0	1	2	0
รวม		110	1	2	0.9865

จากผลการทดลองของผู้ใช้งานทั่วไปเครื่องที่ 9 พบข้อมูลซอฟต์แวร์เวอร์ชันที่ติดตั้งในฐานข้อมูลจำนวน 11 รายการและไม่พบ 129 รายการ จากตารางที่ 5.18 ได้ค่า F-measure เป็น 1 เนื่องจากหารายการซีวีอีของซอฟต์แวร์เวอร์ชันที่ติดตั้งในเครื่องคอมพิวเตอร์ครบ

ตารางที่ 5.18 ผลการทดลองเครื่องของผู้ใช้งานทั่วไปเครื่องที่ 9

ชื่อซอฟต์แวร์	เวอร์ชันซอฟต์แวร์	TP	FP	FN	F-measure
Adobe Flash Player 10 ActiveX	10.0.32.18	194	0	0	1
Microsoft .NET Framework 4.6.1	4.6.01055	8	0	0	1
Windows 7 Professional	6.1	1	0	0	1
Wireshark 2.0.1 (32-bit)	2.0.1	87	0	0	1
Microsoft Office Access MUI (English) 2007	12.0.6612.1000	1	0	0	1
Microsoft Office Excel MUI (English) 2007	12.0.6612.1000	9	0	0	1
Microsoft Office PowerPoint MUI (English) 2007	12.0.6612.1000	3	0	0	1
Microsoft Office Publisher MUI (English) 2007	12.0.6612.1000	4	0	0	1
Microsoft Office Outlook MUI (English) 2007	12.0.6612.1000	1	0	0	1
Microsoft Office Word MUI (English) 2007	12.0.6612.1000	9	0	0	1
Microsoft Office Visio Professional 2007	12.0.6612.1000	1	0	0	1
รวม		318	0	0	1

จากผลการทดลองของผู้ใช้งานทั่วไปเครื่องที่ 10 พบข้อมูลซอฟต์แวร์เวอร์ชันที่ติดตั้งในฐานข้อมูลจำนวน 6 รายการและไม่พบ 76 รายการ จากตารางที่ 5.19 ได้ค่า F-measure เป็น 0.9973 เนื่องจากมีข้อผิดพลาดในการหารายการซีวีอีของซอฟต์แวร์ Dota 2 และ Microsoft Visual C++ 2008 Redistributable ดังที่กล่าวไปแล้วข้างต้น

ตารางที่ 5.19 ผลการทดลองเครื่องของผู้ใช้งานทั่วไปเครื่องที่ 10

ชื่อซอฟต์แวร์	เวอร์ชันซอฟต์แวร์	TP	FP	FN	F-measure
Dota 2	-	0	1	0	0
Mozilla Firefox 43.0.2 (x86 en-US)	43.0.2	1	0	0	1
Wireshark 2.0.1 (64-bit)	2.0.1	87	0	0	1
Steam	2.10.91.91	1	0	0	1
Microsoft Visual C++ 2008 Redistributable	9.0.30729.4974	0	1	2	0
Windows 8.1 Pro	6.3	669	0	0	1
รวม		758	2	2	0.9973

จากผลการทดลองของผู้ใช้งานทั่วไปเครื่องที่ 11 พบข้อมูลซอฟต์แวร์เวอร์ชันที่ติดตั้งในฐานข้อมูลจำนวน 12 รายการและไม่พบ 100 รายการ จากตารางที่ 5.20 ได้ค่า F-measure เป็น 0.9890 เนื่องจากมีข้อผิดพลาดในการหารายการซีวีอีของซอฟต์แวร์ Microsoft Visual C++ 2008 Redistributable ดังที่กล่าวไปแล้วข้างต้น

ตารางที่ 5.20 ผลการทดลองเครื่องของผู้ใช้งานทั่วไปเครื่องที่ 11

ชื่อซอฟต์แวร์	เวอร์ชันซอฟต์แวร์	TP	FP	FN	F-measure
Adobe AIR	18.0.0.144	35	0	0	1
Microsoft .NET Framework 4.5	4.5.50709	42	0	0	1
Mozilla Firefox 43.0.4 (x86 th)	43.0.4	17	0	0	1
Windows 7 Professional	6.1	1	0	0	1
Wireshark 2.2.4 (64-bit)	2.2.4	31	0	0	1
Microsoft Visual C++ 2008 Redistributable	9.0.30729	0	1	2	0
Microsoft Office Excel MUI (English) 2010	14.0.4763.1000	3	0	0	1

ตารางที่ 5.20 ผลการทดลองเครื่องของผู้ใช้งานทั่วไปเครื่องที่ 11 (ต่อ)

ชื่อซอฟต์แวร์	เวอร์ชันซอฟต์แวร์	TP	FP	FN	F-measure
Microsoft Office PowerPoint MUI (English) 2010	14.0.4763.1000	2	0	0	1
Microsoft Office Publisher MUI (English) 2010	14.0.4763.1000	2	0	0	1
Microsoft Office Word MUI (English) 2010	14.0.4763.1000	1	0	0	1
Microsoft Office OneNote MUI (English) 2010	14.0.4763.1000	1	0	0	1
รวม		135	1	2	0.9890

จากผลการทดลองของผู้ใช้งานทั่วไปเครื่องที่ 12 พบข้อมูลซอฟต์แวร์เวอร์ชันที่ติดตั้งในฐานข้อมูลจำนวน 11 รายการและไม่พบ 112 รายการ จากตารางที่ 5.21 ได้ค่า F-measure เป็น 0.9739 เนื่องจากเครื่องมือหารายการซีวีอีของซอฟต์แวร์ Adobe Reader XI (11.0.15) ไม่พบ เพราะในฐานข้อมูลบันทึกไว้ว่า cpe:/a:adobe:acrobat_xi:11.0.15 ไม่ใช่ adobe reader เหมือนชื่อซอฟต์แวร์ที่ได้มาจากการค้นหาจากวินโดวส์รีจิสทรีจึงไม่พบรายการซีวีอีที่ควรพบ 3 รายการ

ตารางที่ 5.21 ผลการทดลองเครื่องของผู้ใช้งานทั่วไปเครื่องที่ 12

ชื่อซอฟต์แวร์	เวอร์ชันซอฟต์แวร์	TP	FP	FN	F-measure
CCleaner	4.11	1	0	0	1
Microsoft .NET Framework 4.5.2	4.5.51209	42	0	0	1
VLC media player	2.2.1	2	0	0	1
Microsoft Office Visio Professional 2007	12.0.4518.1014	1	0	0	1
Microsoft Office Excel MUI (English) 2010	14.0.4763.1000	3	0	0	1

ตารางที่ 5.21 ผลการทดลองเครื่องของผู้ใช้งานทั่วไปเครื่องที่ 12 (ต่อ)

ชื่อซอฟต์แวร์	เวอร์ชันซอฟต์แวร์	TP	FP	FN	F-measure
Microsoft Office Word MUI (English) 2010	14.0.4763.1000	1	0	0	1
Microsoft Office OneNote MUI (English) 2010	14.0.4763.1000	1	0	0	1
Microsoft Office PowerPoint MUI (English) 2010	14.0.4763.1000	2	0	0	1
Microsoft Office Publisher MUI (English) 2010	14.0.4763.1000	2	0	0	1
Adobe Reader XI (11.0.15)	11.0.15	0	0	3	0
Windows 7 Professional	6.1	1	0	0	1
รวม		56	0	3	0.9739

จากผลการทดลองของผู้ใช้งานทั่วไปเครื่องที่ 13 พบข้อมูลซอฟต์แวร์เวอร์ชันที่ติดตั้งในฐานข้อมูลจำนวน 4 รายการและไม่พบ 19 รายการ จากตารางที่ 5.22 ได้ค่า F-measure เป็น 0.9411 เนื่องจากมีข้อผิดพลาดในการหารายการซีวีอีของซอฟต์แวร์ Update for Microsoft .NET Framework 4.6.1 (KB4014553) และ Microsoft Visual C++ 2008 Redistributable ดังที่กล่าวไปแล้วข้างต้น

ตารางที่ 5.22 ผลการทดลองเครื่องของผู้ใช้งานทั่วไปเครื่องที่ 13

ชื่อซอฟต์แวร์	เวอร์ชันซอฟต์แวร์	TP	FP	FN	F-measure
Microsoft .NET Framework 4.6.1	4.6.01055	8	0	0	1
Update for Microsoft .NET Framework 4.6.1 (KB4014553)	1	0	2	0	0
Wireshark 2.2.2 (64-bit)	2.2.2	32	0	0	1
Microsoft Visual C++ 2008 Redistributable	9.0.30729.6161	0	1	2	0
รวม		40	3	2	0.9411

จากผลการทดลองทั้งหมดของเครื่องคอมพิวเตอร์ของผู้ดูแลระบบและผู้ใช้งานทั่วไปสามารถคำนวณค่า F-measure รวมเฉลี่ยเป็น 0.9919 ซึ่งเครื่องมือสามารถหารายการซีวีอีของซอฟต์แวร์ได้แม่นยำในระดับที่น่าพึงพอใจ ได้ดังตารางที่ 5.23

ตารางที่ 5.23 ค่า F-measure ของเครื่องมือ

เครื่องคอมพิวเตอร์	TP	FP	FN	F-measure
เครื่องของผู้ดูแลระบบขององค์กรเครื่องที่ 1	267	1	2	0.9944
เครื่องของผู้ดูแลระบบขององค์กรเครื่องที่ 2	234	0	0	1
เครื่องของผู้ดูแลระบบขององค์กรเครื่องที่ 3	62	1	2	0.9763
เครื่องของผู้ดูแลระบบขององค์กรเครื่องที่ 4	203	1	2	0.9926
เครื่องของผู้ดูแลระบบขององค์กรเครื่องที่ 5	203	0	0	1
เครื่องของผู้ดูแลระบบขององค์กรเครื่องที่ 6	202	0	0	1
เครื่องของผู้ดูแลระบบขององค์กรเครื่องที่ 7	111	0	0	1
เครื่องของผู้ดูแลระบบขององค์กรเครื่องที่ 8	82	3	0	0.9820
เครื่องของผู้ใช้งานทั่วไปเครื่องที่ 1	149	0	0	1
เครื่องของผู้ใช้งานทั่วไปเครื่องที่ 2	1	9	4	0.1333
เครื่องของผู้ใช้งานทั่วไปเครื่องที่ 3	42	14	4	0.8235
เครื่องของผู้ใช้งานทั่วไปเครื่องที่ 4	265	2	0	0.9962
เครื่องของผู้ใช้งานทั่วไปเครื่องที่ 5	3	1	0	0.8571
เครื่องของผู้ใช้งานทั่วไปเครื่องที่ 6	745	0	1	0.9993
เครื่องของผู้ใช้งานทั่วไปเครื่องที่ 7	59	1	0	0.9915
เครื่องของผู้ใช้งานทั่วไปเครื่องที่ 8	110	1	2	0.9865
เครื่องของผู้ใช้งานทั่วไปเครื่องที่ 9	318	0	0	1
เครื่องของผู้ใช้งานทั่วไปเครื่องที่ 10	758	2	2	0.9973
เครื่องของผู้ใช้งานทั่วไปเครื่องที่ 11	135	1	2	0.9890
เครื่องของผู้ใช้งานทั่วไปเครื่องที่ 12	56	0	3	0.9739
เครื่องของผู้ใช้งานทั่วไปเครื่องที่ 13	40	3	2	0.9411
รวม	4045	40	26	**เฉลี่ย** 0.9919

5.4. วิเคราะห์ผลการทดลอง

เนื่องจากรายชื่อซอฟต์แวร์ที่ได้จากการค้นหาวินโดวส์รีจิสทรี ไม่ตรงกับในฐานข้อมูลที่ได้จากเอ็นวีดีทุกประการ ดังนั้นในการค้นหารายชื่อซอฟต์แวร์จะใช้วิธีการตัดคำเป็นคำย่อยๆ แล้วค้นหาจากฐานข้อมูลโดยใช้คำสั่ง like ในการค้นหา ซึ่งคำสั่งนี้จะค้นพบข้อมูลทุกๆ อย่างที่เหมือนกับคำที่นำไปค้นหา ดังนั้นอาจค้นพบรายชื่อซอฟต์แวร์อื่นที่ไม่ต้องการด้วย จึงทำให้เกิดข้อผิดพลาดในการค้นหาอยู่บ้าง แต่จากค่า F-measure เฉลี่ยเป็น 0.9919 และมีคะแนนเฉลี่ยของแบบสอบถามความพึงพอใจจากผู้ใช้งานเครื่องมือเป็น 4.26 ซึ่งอยู่ในระดับที่น่าพึงพอใจ

บทที่ 6
สรุปผลการวิจัย ข้อจำกัดและข้อเสนอแนะ

6.1. สรุปผลการวิจัย

วิทยานิพนธ์นี้ได้นำเสนอเครื่องมือช่วยประเมินช่องโหว่ด้านความมั่นคงเพื่อการยกระดับเวอร์ชันของซอฟต์แวร์ โดยนำคะแนนซีวีเอสเอสเข้ามาประเมินความรุนแรงของช่องโหว่ในแต่ละซอฟต์แวร์เพื่อให้สามารถเปรียบเทียบความรุนแรงของช่องโหว่ในซอฟต์แวร์เวอร์ชันที่ติดตั้งในคอมพิวเตอร์กับซอฟต์แวร์เวอร์ชันล่าสุดที่พบในฐานข้อมูลที่ได้จากเอ็นวีดีได้ โดยที่ในการประเมินช่องโหว่จะใช้ตัววัดทั้ง 3 กลุ่ม คือ กลุ่มตัววัดพื้นฐาน กลุ่มตัววัดตามเวลา และกลุ่มตัววัดตามสภาพแวดล้อม เมื่อนำคะแนนกลุ่มตัววัดตามสภาพแวดล้อมเข้ามาร่วมคำนวณด้วยจะสามารถสะท้อนความรุนแรงที่แท้จริงของช่องโหว่จากมุมมองขององค์กรได้ดีขึ้น นอกจากนี้เครื่องมือยังสามารถแนะนำการยกระดับเวอร์ชันของซอฟต์แวร์ได้ เช่นถ้าหากเวอร์ชันล่าสุดที่ยังไม่ได้ติดตั้งในเครื่องคอมพิวเตอร์มีความรุนแรงของช่องโหว่น้อยกว่าซอฟต์แวร์เวอร์ชันที่ติดตั้งในเครื่องคอมพิวเตอร์แล้ว เครื่องมือจะแนะนำให้ยกระดับเวอร์ชันของซอฟต์แวร์

จากการนำเครื่องมือที่พัฒนาขึ้นไปทดลองใช้งาน พบว่าในส่วนของการจับคู่รายชื่อซอฟต์แวร์และเวอร์ชันกับข้อมูลซอฟต์แวร์ที่มีในฐานข้อมูลที่ได้จากเอ็นวีดี พบว่ามีผลลัพธ์ที่เกิดขึ้นมี 4 กรณี

1. เครื่องมือพบรายการซีวีอีของทั้งซอฟต์แวร์เวอร์ชันที่ติดตั้งในเครื่องคอมพิวเตอร์และซอฟต์แวร์เวอร์ชันล่าสุดที่มีในฐานข้อมูล ทำให้สามารถเปรียบเทียบผลประเมินช่องโหว่ด้านความมั่นคงของระหว่างซอฟต์แวร์ 2 เวอร์ชันได้
2. ซอฟต์แวร์เวอร์ชันที่ติดตั้งในคอมพิวเตอร์ไม่ใช่เวอร์ชันล่าสุด แต่ไม่มีรายการซีวีอีในฐานข้อมูล แต่พบรายการซีวีอีของซอฟต์แวร์เวอร์ชันที่ใหม่กว่าในฐานข้อมูล ทำให้ไม่สามารถเปรียบเทียบผลประเมินช่องโหว่ด้านความมั่นคงของระหว่างซอฟต์แวร์ 2 เวอร์ชันได้
3. ซอฟต์แวร์เวอร์ชันที่ติดตั้งในเครื่องคอมพิวเตอร์ใหม่กว่าเวอร์ชันที่มีในฐานข้อมูลจึงไม่สามารถเปรียบเทียบผลประเมินช่องโหว่ด้านความมั่นคงของระหว่างซอฟต์แวร์ 2 เวอร์ชันได้
4. ไม่มีข้อมูลรายการซีวีอีของชื่อซอฟต์แวร์นี้ในฐานข้อมูลทีได้จากเอ็นวีดีเลย

ทั้งนี้การแนะนำการยกระดับเวอร์ชันของซอฟต์แวร์ ได้สรุปไว้ในหัวข้อที่ 3.5

6.2. ปัญหาและข้อจำกัดของงานวิจัย

จากการพัฒนาเครื่องมือพบปัญหาและข้อจำกัดของงานวิจัยดังนี้

1. เครื่องมือที่พัฒนาขึ้นสามารถใช้ได้ในระบบปฏิบัติการวินโดวส์เท่านั้นเนื่องจากใช้การดึงรายชื่อซอฟต์แวร์จากวินโดวส์รีจิสทรี
2. เครื่องมือที่พัฒนาขึ้นไม่สามารถค้นหารายชื่อซอฟต์แวร์ที่ไม่ปรากฏบนวินโดวส์รีจิสทรีได้โดยอัตโนมัติ ผู้ใช้งานจึงต้องเพิ่มรายชื่อซอฟต์แวร์เหล่านี้เอง
3. รายชื่อซอฟต์แวร์และเวอร์ชันที่มีในเอ็นวีดี อาจมีไม่ครบทุกเวอร์ชันของซอฟต์แวร์นั้นๆ หรือเอ็นวีดียังไม่ได้เพิ่มซอฟต์แวร์เวอร์ชันล่าสุดลงฐานข้อมูล
4. ในการปรับปรุงรายการซีวีอีโดยใช้ข้อมูลล่าสุดจากเว็บไซต์เอ็นวีดี อาจใช้เวลาในการปรับปรุงค่อนข้างมาก หากแบนด์วิดท์ (Bandwidth) ของระบบเครือข่าย (Network) ที่ใช้อยู่ค่อนข้างต่ำ
5. การเรียกเอพีไอของไอบีเอ็ม เอกซ์เอฟอี อาจใช้เวลาค่อนข้างนาน และใช้เรียกเอพีไอของไอบีเอ็ม เอกซ์เอฟอี ได้เพียง 5,000 ครั้ง ต่อเดือน เนื่องจากเป็นบริการฟรี
6. ในการค้นหารายชื่อซอฟต์แวร์โดยการตัดคำออกเป็นส่วนย่อยๆ นั้น อาจเกิดข้อการค้นหารายชื่อซอฟต์แวร์ผิดพลาดและไม่ถูกต้องได้

6.3. ข้อเสนอแนะ

งานวิจัยนี้สามารถพัฒนาเพิ่มเติมได้ในอนาคตดังนี้

1. พัฒนาเครื่องมือให้รองรับกับหลายๆ ระบบปฏิบัติการ
2. พัฒนาเครื่องมือให้มีความแม่นยำในการค้นหารายชื่อซอฟต์แวร์ให้มากขึ้น เพื่อความถูกต้องในการค้นหารายชื่อซอฟต์แวร์ให้มากขึ้น เช่น การใช้การวิเคราะห์ความเหมือนของข้อความ
3. จัดหมวดหมู่ของซอฟต์แวร์เพื่อให้สามารถเลือกเปรียบเทียบระหว่างซอฟต์แวร์ชื่ออื่นๆ ที่อยู่ในหมวดหมู่เดียวกันได้ง่ายขึ้น

รายการอ้างอิง

[1] K.E. Vaniea, E. Rader, and R. Wash. "*Betrayed By Updates: How Negative Experiences Affect Future Security*". *CHI '14 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 2014. ACM New York, NY, USA. pp. 2671-2674.

[2] MITRE. *Common Vulnerabilities and Exposures*. Available from: https://cve.mitre.org/.

[3] *NIST Special Publication 800-60 Volume II*, in *Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*. 2008.

[4] FIRST.Org Inc, *Common Vulnerability Scoring System v3.0*, in *Specification Document*. 2015.

[5] FIRST.Org Inc, *A Complete Guide to the Common Vulnerability Scoring System Version 2.0*. 2007.

[6] NIST. *National Vulnerability Database*. Available from: http://nvd.nist.gov.

[7] IBM Security. *IBM X-Force Exchange*. Available from: https://exchange.xforce.ibmcloud.com.

[8] *ISS X-Force*. Available from: http://xforce.iss.net/.

[9] ปฏิญญา จันฤาชัย, เครื่องมือช่วยบริหารความปลอดภัยโดยใช้ฐานข้อมูลจุดอ่อนระบบเปิด, in วิทยานิพนธ์หลักสูตรวิทยาศาสตร์มหาบัณฑิต สาขาวิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์. 2547, จุฬาลงกรณ์มหาวิทยาลัย.

[10] N. Artaiam and T. Senivongse. "*Enhancing Service-Side QoS Monitoring for Web Services*". *2008 Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing*. 2008. Phuket. pp. 765-770.

[11] C. Fruhwirth and T. Mannisto. "*Improving CVSS-based vulnerability prioritization and response with context information*". *ESEM '09 Proceedings of the 2009 3rd International Symposium on Empirical Software Engineering and Measurement*. 2009. IEEE Computer Society Washington, DC, USA. pp. 535-544.

[12] S. Frei, M. May, U. Fiedler, and B. Plattner. "*Large- scale vulnerability analysis*". *LSAD '06 Proceedings of the 2006 SIGCOMM workshop on Large-scale attack defense*. 2006. Pisa, Italy: ACM New York, NY, USA. pp. 131-138.

[13] *FIPS Publication 199*, in *Standards for Security Categorization of Federal Information and Information Systems*. 2004.

ประวัติผู้เขียนวิทยานิพนธ์

นางสาวศิริขวัญ ตรีทิพยรักษ์ เกิดวันที่ 27 ตุลาคม 2533 สำเร็จการศึกษาระดับปริญญาตรี หลักสูตรวิทยาศาสตรบัณฑิต (วท.บ.) คณะวิทยาศาสตร์ มหาวิทยาลัยเกษตรศาสตร์ ปีการศึกษา 2555

ปัจจุบันเป็นพนักงานรัฐวิสาหกิจที่ บริษัท ทีโอที จำกัด (มหาชน) ตำแหน่งนักคอมพิวเตอร์ เป็นเวลา 4 ปี

เข้าศึกษาต่อระดับปริญญามหาบัณฑิต ปีการศึกษา 2559 หลักสูตรวิทยาศาสตรมหาบัณฑิต (วท.ม.) สาขาวิศวกรรมซอฟต์แวร์ ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรม จุฬาลงกรณ์มหาวิทยาลัย