เครื่องมือด้านความปลอดภัยทางไซเบอร์

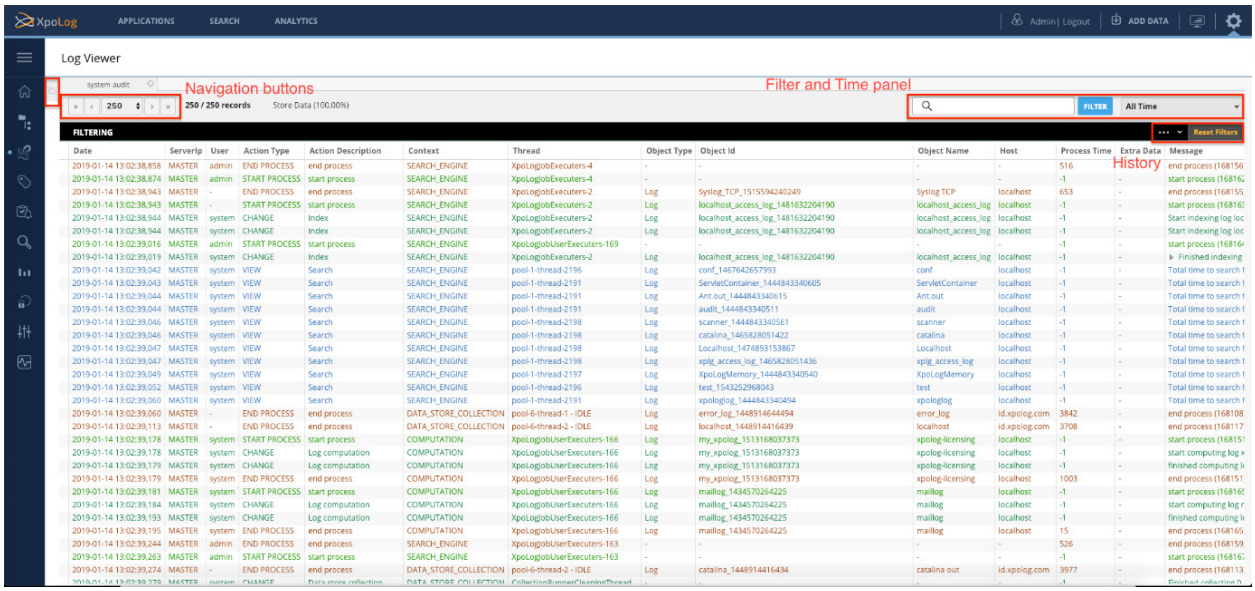
วิษณุ เรืองวิทยานนท์ และพรนภา เจมส์
สถาบันวิจัยวิทยาศาสตร์และเทคโนโลยีแห่งประเทศไทย
35 หมู่ที่ 3 เทคโนธานี ตำบลคลองห้า อำเภอคลองหลวง จังหวัดปทุมธานี 12120

ปัจจุบันภัยคุกคามทางด้านไซเบอร์มีความร้ายแรงมากขึ้น ทั้งกระทำต่อภาครุรกิจ ขนส่ง โทรคมนาคม ตลอดจนถึงการโจมตีทางการทหาร อีกทั้งขณะนี้ได้มีการประกาศพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ยิ่งทำให้หน่วยงานต้องตระหนักถึงความปลอดภัยและความรับผิดชอบที่มากขึ้นเป็นทวีคูณ สาเหตุเนื่องจากพระราชบัญญัติฉบับนี้สามารถดำเนินการครอบคลุมเหตุการณ์ร้ายแรงต่างๆ อาทิ เมื่อมีเหตุร้ายแรงทางไซเบอร์ เจ้าหน้าที่สามารถสอดส่องข้อมูลได้แบบ real-time รวมถึงการมอบอำนาจยึด ค้น เจาะ หรือขอข้อมูลใดๆ จะไม่สามารถอุทธรณ์เพื่อยับยั้งได้ และผู้ใดฝ่าฝืนไม่ปฏิบัติตามคำสั่งมีทั้งโทษปรับและโทษจำคุก

ในอดีตที่ผ่านมาเรามักเห็นเหตุการณ์ที่เกี่ยวกับช่องโหว่และการโจมตีทางไซเบอร์ ในปี พ.ศ. 2561 ธนาคาร HSBC เกิดเหตุช่องโหว่ (Data breach) ทำให้ข้อมูลหมายเลขบัญชี ยอดเงิน ที่อยู่ ประวัติการทำธุรกรรมของลูกค้าหลุดสู่ภายนอก โดยเหตุการณ์นี้เกิดขึ้นจากการที่ผู้ไม่มีสิทธิ์เข้าถึงข้อมูลของลูกค้าลักลอบเข้าระบบระหว่างวันที่ 4-14 ตุลาคม พ.ศ. 2561 ทำให้ธนาคารต้องแก้ไขปัญหาโดยหยุดการให้บริการลูกค้าในลักษณะออนไลน์ รวมถึงการดำเนินการแจ้งเตือนเหตุการณ์ที่เกิดขึ้นให้กับลูกค้าของธนาคารทราบผ่านช่องทางการสื่อสารอื่นๆ และจากเหตุการณ์นี้ส่งผลกระทบกับบัญชีลูกค้าที่อยู่ในประเทศสหรัฐอเมริกาประมาณ 1% จากเหตุการณ์ดังกล่าวทางธนาคารได้ดำเนินการเพิ่มความมั่นคงปลอดภัยในการเข้าใช้งานและการพิสูจน์ตัวตนให้ดียิ่งขึ้น อีกเหตุการณ์ในปีเดียวกันคือธนาคารอินเดียถูกแฮกเกอร์เข้าโจมตี สูญเงินกว่า 400 ล้านบาท ธนาคารดังกล่าวคือ Cosmos Bank ซึ่งเป็นธนาคารอันดับที่ 2 ของประเทศ โดยการโจมตีได้เกิดขึ้นในช่วงวันหยุดประจำสัปดาห์ เหตุการณ์นี้ทำให้สูญเสียเงินไปกว่า 13.5 ล้านเหรียญ (ประมาณ 432 ล้านบาท) โดยธนาคารได้รายงานการโจมตีเป็นการถอนเงินผ่านการทำธุรกรรมทางตู้เบิกถอนเงินสดอัตโนมัติ หรือ ATM จากทั่วโลก รวมถึงการโอนเงินผ่านระบบ SWIFT ไปยังปลายทางที่ประเทศฮ่องกง โดยคาดหมายว่าต้นตอของการโจมตีมาจากประเทศแคนาดา อย่างไรก็ตามต้นทางดังกล่าวอาจไม่ใช่ต้นทางที่แท้จริงเพราะการโจมตีสามารถหลบเลี่ยงผ่านหลายๆ ประเทศดังที่เคยเกิดขึ้นมาก่อน โดยความเสียหายเหล่านี้นอกจากทำให้ลูกค้าทางธุรกิจขาดความเชื่อมั่นแล้วยังทำให้ธนาคารต้องปรับปรุงมาตรการเพื่อรองรับเหตุการณ์ทั้งในเรื่องช่องโหว่และการโจมตีที่อาจเกิดขึ้นในอนาคตได้อีก

ดังนั้นหน่วยงาน และองค์กรต่างๆ ทั้งภาครัฐและเอกชนจึงจำเป็นต้องปรับปรุงเพื่อยกระดับความมั่นคงปลอดภัย เสริมสร้างความแข็งแกร่งของโครงสร้างพื้นฐานและเครือข่าย สำหรับลดความเสี่ยงในการโจมตีทางไซเบอร์ โดยการลดความเสี่ยงดังกล่าวมีเครื่องมือที่ควรนำมาพิจารณาปรับใช้ในระบบป้องกันการโจมตีดังนี้

1. Log Analysis – XpoLog



ที่มา : Technical writer (2019)

ภาพที่ 1 Log Viewer จาก XpoLog

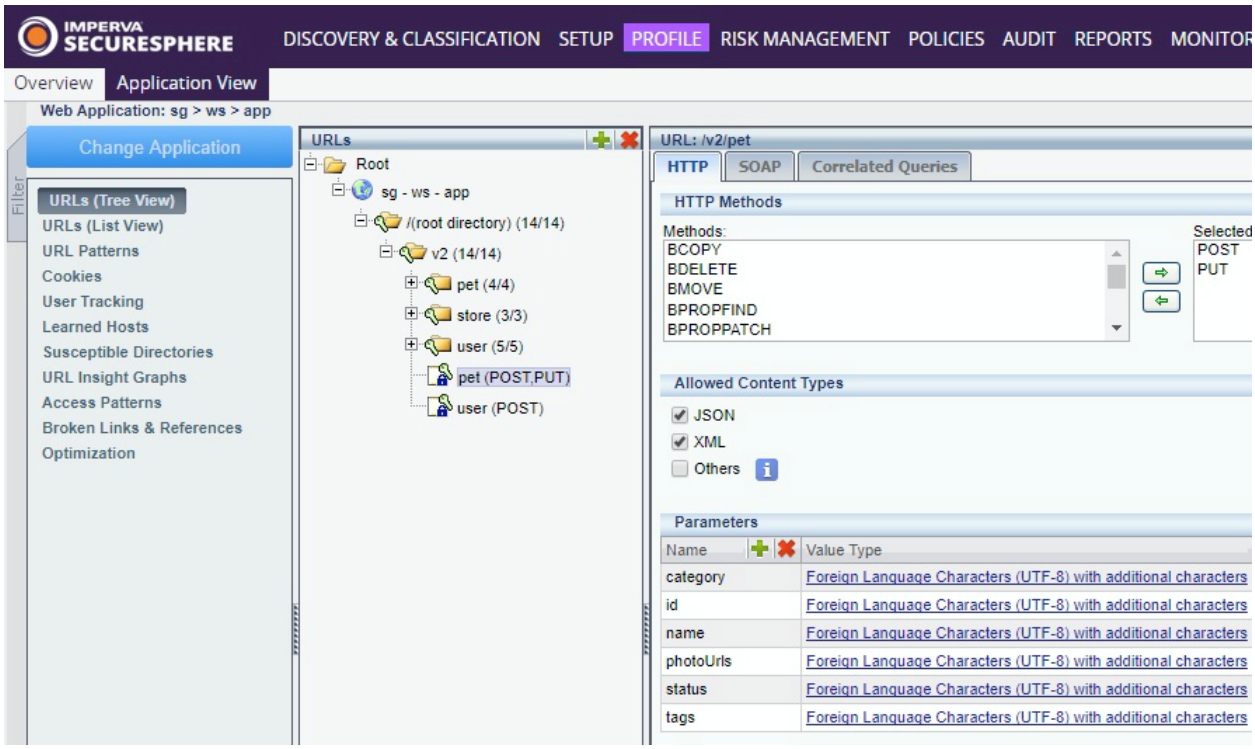
เนื่องจากหน่วยงานหรือองค์กรธุรกิจมีความต้องการติดตามสถานะของระบบโครงสร้างพื้นฐานที่มีอยู่ ซึ่ง XpoLog Center เป็นแพลตฟอร์มการวิเคราะห์ log ของการเข้าสู่ระบบสำหรับการใช้งานเว็บไซต์ สามารถค้นหาและบันทึกข้อมูลเพื่อสอบสวนปัญหา นำไปสร้างรายงาน และใช้ตรวจสอบข้อผิดพลาดโปรแกรม โดยจะมีแดชบอร์ดและแกดเจ็ตที่จะสามารถใช้จัดทำรายงานนำเสนอประสิทธิภาพการทำงานและสิ่งที่ผิดพลาด ในรูปแบบมุมมอง (viewer) สามารถนำไปวิเคราะห์รายงานการค้นหา (search) และนำไปสู่ระบบการบริหารจัดการเรื่องความปลอดภัยต่อไป ทั้งนี้โปรแกรม Xpolog เป็นแพลตฟอร์มสำหรับการจัดการและวิเคราะห์ข้อมูลที่เป็น log ได้หลายรูปแบบ มีความสามารถในการค้นหาและวิเคราะห์ รวมถึงการสร้าง visualization ให้กับ log นั้นๆ ได้อีกด้วย

Xpolog มีวิธีการจัดเก็บข้อมูล log ที่ง่าย สามารถวิเคราะห์และตรวจสอบข้อมูล log ได้จากระบบและจากอุปกรณ์ที่เป็นโครงสร้างพื้นฐานได้เป็นอย่างดี สามารถช่วยแก้ไขปัญหาและยังตรวจสอบสภาพแวดล้อมโดยรวมได้ เพื่อป้องกันปัญหาระบบหยุดชะงักหรือการหยุดให้บริการได้

คุณสมบัติพิเศษของ Xpolog ได้แก่

- มีเครื่องมือสำหรับใช้ในการค้นหาที่ซับซ้อน
- แสดงผล log ผ่านโปรแกรม web browser ได้กับ log ทุกประเภท
- แสดงผลข้อมูลในรูปแบบกราฟ
- รวมรวมข้อมูล log ได้
- คอยตรวจสอบการทำงานของ log
- ตรวจพบข้อผิดพลาดใดๆ ได้ เช่น แนวโน้มพฤติกรรมที่ไม่ปกติ สถานะ เป็นต้น

2. Application and Data Protection – Imperva



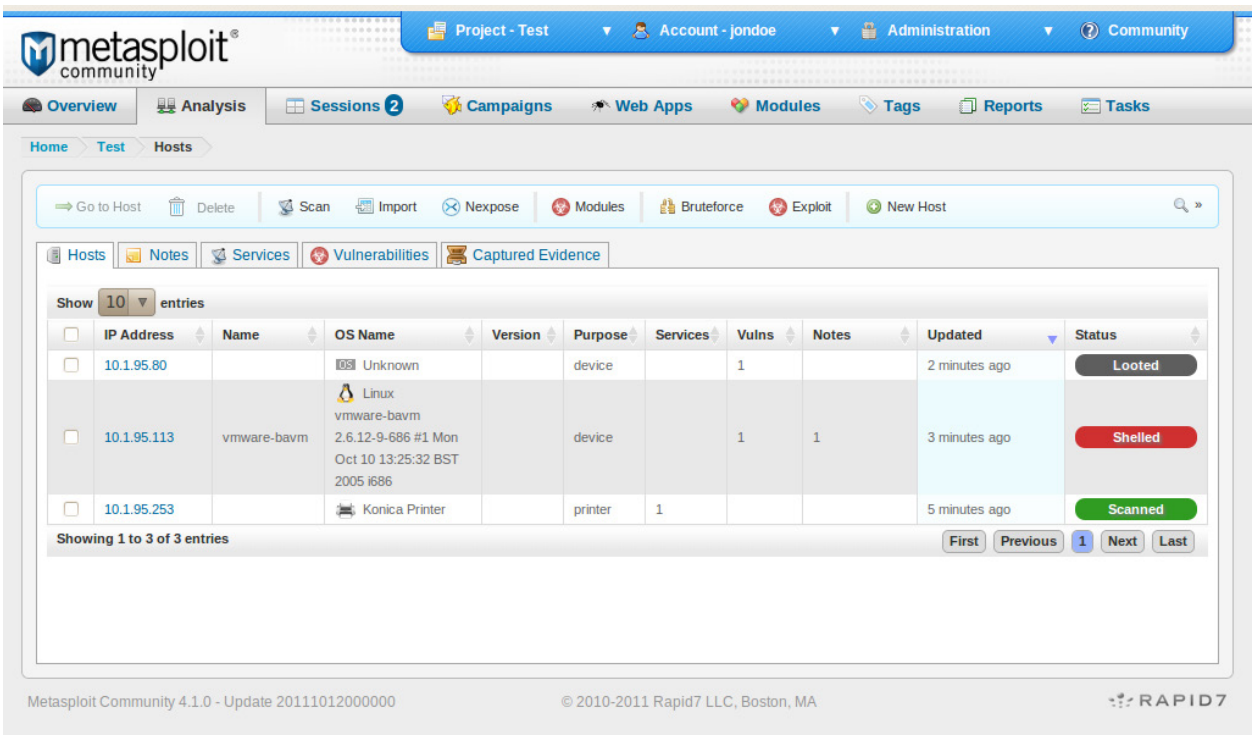
ที่มา : Alok Shukla (2017)

ภาพที่ 2 การสร้างข้อกำหนดบนโปรแกรม Imperva

โดยปกติแล้วผู้ที่ต้องการเจาะระบบมักจะหาข้อมูลเกี่ยวกับโครงสร้างพื้นฐานขององค์กร หรือหน่วยงานที่จะโจมตี ดังนั้นองค์กรควรมีระบบที่สามารถป้องกันการเข้าถึงโครงสร้างต่างๆ ที่สำคัญขององค์กร โดยโปรแกรม Imperva มีเว็บแอปพลิเคชันไฟร์วอลล์ (Web Application Firewall : WAF) เป็นซอฟต์แวร์ที่ช่วยป้องกันการโจมตีผ่านเว็บไซต์โดยทำการวิเคราะห์และค้นหาโปรแกรมหรือสิ่งที่ต้องสงสัย และทำการหยุดการกระทำนั้น เช่น ลดความเสี่ยงเมื่อถูกโจมตีแบบ DDoS

นอกจากนี้ WAF ของ Imperva ยังสามารถสร้างโปรไฟล์ของการจราจรและธุรกรรมที่ผ่านเครือข่าย อีกทั้งช่วยป้องกันการจราจรที่อาจเสี่ยงอันตราย รวมถึงตรวจสอบพฤติกรรมการเข้าถึงที่อาจมีความเสี่ยง

3. Penetration Testing – Metasploit



ที่มา : Saeeddhqan (2019)

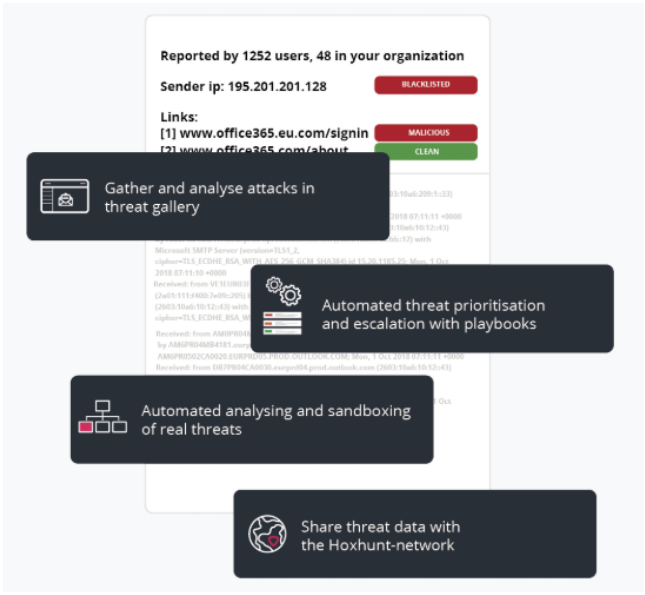
ภาพที่ 3 โปรแกรม Metasploit

Metasploit เป็นโอเพนซอร์ส (project open source) ที่เน้นทางด้านการรักษาความปลอดภัยทางคอมพิวเตอร์ (computer security) โดย Metasploit ถูกใช้สำหรับการทดสอบการเจาะระบบ (penetration testing) โครงการ Metasploit นี้ถูกสร้างโดย HD Moore ในปี ค.ศ. 2003 ปัจจุบันอยู่ภายใต้ Rapid7 โดย Rapid7 ได้พัฒนาเวอร์ชันออกมาอีกคือ Metasploit Express แต่ยังอนุญาตให้ใช้ Metasploit Framework ได้ฟรี

การทดสอบด้านความมั่นคงปลอดภัยของระบบงานหรือระบบเครือข่าย สามารถใช้ Metasploit เป็นเครื่องมือในการทดสอบ โดย Metasploit เป็นซอฟต์แวร์ที่อยู่ในแบบของแพลตฟอร์ม สามารถใช้ค้นหา เข้าถึง และตรวจสอบหาช่องโหว่ที่มีในระบบเครือข่ายคอมพิวเตอร์ อย่างไรก็ตามเนื่องจาก Metasploit มีความสามารถสูงจึงอาจถูกมองว่าเป็นไวรัสคอมพิวเตอร์ ดังนั้นก่อนติดตั้งใช้งานจึงต้องปิดการทำงานของโปรแกรมป้องกันไวรัส (antivirus) และปิดการทำงานของไฟร์วอลล์ (firewall)

4. Anti-Phishing – Hoxhunt

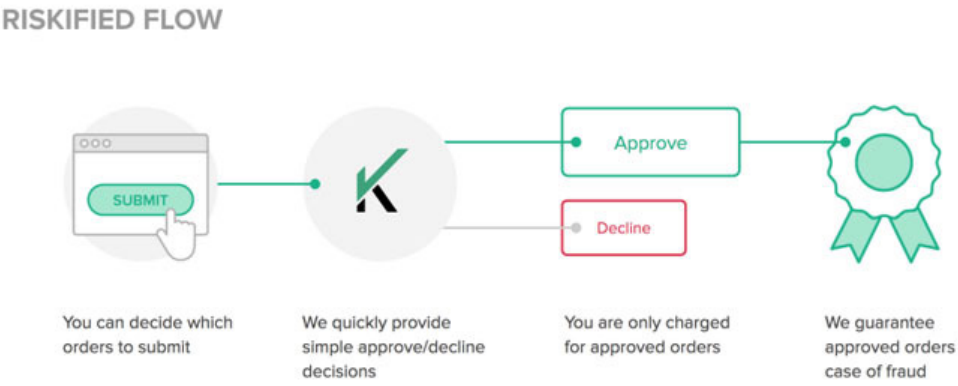
โปรแกรม HoxHunt เป็นซอฟต์แวร์ที่ช่วยวิเคราะห์ภัยคุกคาม และช่วยทดสอบในเรื่องความตระหนักด้านความมั่นคงปลอดภัยของบุคลากรในองค์กร ทั้งในส่วนของการระมัดระวัง Phishing โดยโปรแกรมนี้สามารถส่งจดหมายอิเล็กทรอนิกส์ไปยังเป้าหมายที่ต้องการทดสอบความตระหนัก เช่น พนักงาน หรือผู้บริหาร เพื่อดูว่าเมื่อผู้รับได้จดหมายอิเล็กทรอนิกส์จะให้ความสนใจต่อจดหมายอิเล็กทรอนิกส์ที่หลอกลวงนั้นหรือไม่ อย่างไรก็ตามผู้รับจดหมายอิเล็กทรอนิกส์จะไม่เกิดอันตรายใดๆ จากการส่งของโปรแกรม HoxHunt ดังนั้นประโยชน์ที่จะได้รับจากการใช้งานโปรแกรมดังกล่าวคือการระมัดระวังตัว (awareness) ของบุคลากรในเรื่องของความมั่นคงปลอดภัยทางสารสนเทศ ซึ่งถือเป็นหัวใจหลักขององค์กรในปัจจุบัน



ที่มา : Hoxhunt (2019)

ภาพที่ 4 โปรแกรม Hoxhunt

5. Fraud Detection – Riskified



ที่มา : Ghananewsline (2019)

ภาพที่ 5 Riskfield flow

การป้องกันการทำทุจริต (fraud detection) โดยปกติแบ่งออกเป็น 2 ประเภท ได้แก่

1. การตรวจจับการใช้ในทางที่ผิด (misuse detection) เป็นการตรวจจับโดยอาศัยลักษณะหรือรูปแบบที่ได้กำหนดไว้แล้วว่าเป็นการบุกรุกแล้วนำมาเปรียบเทียบหรือค้นหากับเหตุการณ์ที่เกิดขึ้นในระบบเพื่อตรวจจับการบุกรุกโดยตรง

2. การตรวจจับการใช้งานที่ผิดไปจากปกติวิสัย (anomaly detection) โดยอาศัยการสังเกตพฤติกรรมการใช้ทรัพยากรของระบบคอมพิวเตอร์ที่ผิดไปจากสภาวะการใช้งานปกติ โดยสังเกตที่ตัวผู้ใช้หรือจากระบบงานที่ใช้งาน

ภัยจากการหลอกลวงหรือฉ้อโกงในระบบคอมพิวเตอร์เป็นภัยหนึ่งที่นอกเหนือจากการโจมตีโดยอาศัยช่องโหว่ของระบบ แต่สามารถส่งผลลัพธ์ที่ร้ายแรงต่อระบบงานหรือข้อมูลขององค์กรได้เป็นอย่างสูง โปรแกรม Riskified เป็นโปรแกรมที่ใช้ป้องกันการหลอกลวงโดยอาศัยการเรียนรู้ของเครื่องจักร (Machine Learning : ML) ในการวิเคราะห์พฤติกรรมและจะอนุญาตเฉพาะพฤติกรรมที่ไม่เข้าข่ายในการทุจริตให้สามารถดำเนินการได้ เช่น เมื่อพบว่ามีรายการใดในระบบอิเล็กทรอนิกส์ที่ลูกค้ากระทำแล้ว พบว่าไม่เป็นพฤติกรรมที่ปกติ มีโอกาส หรือมีความเสี่ยงสูง ลูกค้าอาจถูกขอให้ปฏิบัติตามขั้นตอนการตรวจสอบเพิ่มเติมจากปกติมากยิ่งขึ้น หรืออาจถูกปฏิเสธการทำรายการนั้นๆ โดยโปรแกรม Riskfied มีเป้าหมายที่จะจัดการการทุจริต หรือฉ้อโกง โดยมีคุณสมบัติทั้งการป้องกันบัญชีผู้ใช้งาน, ควบคุมอำนาจการจ่ายเงิน, การออกจากระบบแบบอัตโนมัติ ฯลฯ ซึ่งสิ่งเหล่านี้ช่วยให้ผู้ใช้งานและองค์กรมีความปลอดภัยและสามารถดำเนินงานธุรกรรมด้านอิเล็กทรอนิกส์ได้อย่างมั่นใจมากยิ่งขึ้น

เอกสารอ้างอิง

สมหวัง, ปรีชา และ โทศิริกุล, ศิริวัฒน์. 2562. ระบบตรวจจับการใช้งานคอมพิวเตอร์ในทางที่ผิด. [ออนไลน์]. เข้าถึงได้จาก: http://lexitron.nectec.or.th/public/NCIT_2010_Bangkok%20_Thailand/index_files/papers/76-p123.pdf, [เข้าถึงเมื่อ 31 พฤษภาคม 2562],

@KBenZ. 2562. ผ่านแล้ว ‘พ.ร.บ.ไซเบอร์ฯ’ ให้อำนาจเจ้าหน้าที่ สามารถค้น ติดตาม และยึดคอมฯ ได้แทบทันที. [ออนไลน์]. เข้าถึงได้จาก: https://www.aripfan.com/de-laws-cyber-security-protection-act-in-thailand-now-v3/, [เข้าถึงเมื่อ 31 พฤษภาคม 2562].

Abrams, L., 2019. HSBC Bank Data Breach Exposed Account Numbers, Balances, and More. [online]. Available at: https://www.bleepingcomputer.com/news/security/hsbc-bank-data-breach-exposed-account-numbers-balances-and-more/, [accessed 31 May 2019].

Admin, 2562. 5 ทูลด้านความปลอดภัยทางไซเบอร์ ที่ทุกธุรกิจจำเป็นต้องรู้. [ออนไลน์]. เข้าถึงได้จาก: https://www.enterpriseitpro.net/5-cybersecurity-tools-every-business-needs-to-know/?fbclid=IwAR0vNhb2vjg6wVGAnXbjMdIJXEX4F2JlQUG4VD3H86NBEEcNgYrr1G05BnI, [เข้าถึงเมื่อ 31 พฤษภาคม 2562].

Cimpanu, C., 2019. Hackers steal $13.5 million across three days from Indian bank. [online]. Available at: https://www.bleepingcomputer.com/news/security/hackers-steal-135-million-across-three-days-from-indian-bank/, [accessed 31 May 2019].

Ghananewsline, 2019. 5 Cybersecurity Tools Every Business Needs to Know [online]. Available at: https://ghananewsline.com/, [accessed 31 May 2019].

Hoxhunt, 2019. Automated phishing training and response. [online]. Available at: https://www.hoxhunt.com/, [accessed 31 May 2019].

Riskified, 2019. Maximize conversions and prevent fraud from login to checkout. [online]. Available at: https://www.riskified.com/solution/, [accessed 31 May 2019].

Saeeddhqan. 2019. Metasploit Project. [online]. Available at: https://en.wikipedia.org/wiki/Metasploit_Project, [accessed 31 May 2019].

Shukla A., 2019. Six Ways to Secure APIs. [online]. Available at: https://www.imperva.com/blog/six-ways-to-secure-apis/, [accessed 31 May 2019].

Technical Writer, 2019. Log viewer. [online]. Available at: http://wiki.xpolog.com/display/XPOL/Log+Viewer, [accessed 31 May 2019].