คำชื่นชม

ในยุคที่โลกไซเบอร์เต็มไปด้วยภัยคุกคาม เราได้รับคำแนะนำและแนวทางมากมาย ซึ่งมักเป็นแนวทางกว้างๆ แต่ Attack Surface Management เป็นคู่มือเชิงปฏิบัติการที่ใช้งานได้จริง เพื่อการระบุ, จัดลำดับความสำคัญ และปกป้องสินทรัพย์สำคัญขององค์กรอย่างเป็นระบบ ตรงตามแนวทางปฏิบัติที่ดีที่สุด และเฟรมเวิร์คการบริหารความเสี่ยง ที่เปลี่ยนจากการทำแค่รายการ checklist ไปสู่การทำงานด้านความปลอดภัยที่ให้คุณค่าอย่างแท้จริง

— Jeremy Faircloth,
ที่ปรึกษา/สถาปนิกด้านความปลอดภัยไซเบอร์อาวุโส

ทุกคนที่เกี่ยวข้องกับความปลอดภัยรู้ว่า มันเป็นภารกิจที่ไม่มีวันจบสิ้น เราพยายามทำให้ระบบมีความแข็งแกร่งและปลอดภัยขึ้นทุกวัน แต่ทุกวันก็มีสิ่งใหม่ๆ มาท้าทายเราเช่นกัน Attack Surface Management เป็นกรอบการทำงานที่ช่วยให้เห็นภูมิทัศน์ใหม่ เพื่อให้ผู้ที่เกี่ยวข้องกับความปลอดภัยข้อมูล (ซึ่งดูเหมือนจะหมายถึงทุกคน) สามารถทำงานได้อย่างยั่งยืนและมีประสิทธิผล ผมได้นำแนวคิดจากหนังสือเล่มนี้ไปใช้กับงานของตัวเองแล้ว และหวังว่า ASM จะแพร่หลายมากขึ้นในอนาคต

— Chris Devers,
หัวหน้าทีมเทคนิควิศวกรรมบำรุงรักษา, บริษัท EditShare

การจัดการพื้นที่การโจมตี (Attack Surface Management) เป็นคำที่ได้ยินบ่อย แต่แทบจะไม่มีการอธิบายอย่างครอบคลุมให้กับผู้ไม่คุ้นเคย แต่ Ron และ MJ สร้างความรู้พื้นฐานเกี่ยวกับ ASM และพาผู้อ่านไปสู่ระดับความเข้าใจที่นำไปใช้ได้จริง ถ้าผมมีหนังสือเล่มนี้เมื่อสิบปีที่แล้ว มันคงช่วยประหยัดเวลาและความพยายามในการลองผิดลองถูกไปได้มาก

— Dane Grace,
ผู้จัดการผลิตภัณฑ์ด้านความปลอดภัยไซเบอร์อาวุโส

เป็นคู่มือที่ให้กรอบปฏิบัติที่เข้าใจง่าย เพื่อช่วยให้คุณระบุและเข้าใจถึง “พื้นที่การโจมตี” จึงขอแนะนำให้ผู้ที่จริงจังกับการลดความเสี่ยง และต้องการปกป้องระบบของตนเอง ได้อ่านหนังสือเล่มนี้อย่างยิ่ง ... เพราะเราไม่สามารถปกป้องสิ่งที่เราไม่รู้ว่า “มีอยู่” ได้

— Steve Winterfeld,
CISO ในฐานะที่ปรึกษาของบริษัท Cyber Vigilance Advice

คำนำ

ความปลอดภัยทางไซเบอร์ (cybersecurity) คือการวิ่งแข่งที่ไม่มีวันสิ้นสุด เป็นการแข่งขันที่เส้นชัยเคลื่อนที่ออกไปเรื่อยๆ ทุกครั้งที่เราคิดว่าปกป้องระบบได้ดีแล้ว ผู้โจมตีก็จะหาวิธีใหม่ๆ โจมตีเข้ามาเสมอ ซึ่งทุกนวัตกรรม, ความสะดวกสบาย, บริการคลาวด์ หรืออุปกรณ์เชื่อมต่อที่เรานำมาใช้ ล้วนเปิดโอกาสใหม่ๆ ให้กับทั้งธุรกิจและผู้ประสงค์ร้ายด้วย นี่คือจุดที่การจัดการพื้นที่การโจมตี (attack surface management - ASM) ได้เข้ามามีบทบาท

ASM ไม่ใช่เป็นแค่คำศัพท์ด้านความปลอดภัยที่มักพูดกัน แต่เป็นการเปลี่ยนแปลงระดับรากฐานด้านความปลอดภัยทางไซเบอร์ขององค์กร ในโลกที่การเปลี่ยนแปลงทางดิจิตอลเกิดขึ้นอย่างรวดเร็ว จากการรักษาความปลอดภัยเน็ตเวิร์คและอุปกรณ์แบบเดิมๆ ไปสู่ระบบนิเวศที่กว้างขวางและเชื่อมต่อกันของสภาพแวดล้อมคลาวด์, แอพพลิเคชัน SaaS, API, อุปกรณ์ IoT, พนักงานที่ทำงานจากระยะไกล และการพึ่งพาบนห่วงโซ่อุปทาน พื้นที่ที่เสี่ยงต่อการถูกโจมตีสมัยใหม่จึงกว้างใหญ่, กระจัดกระจาย และเปลี่ยนแปลงอยู่ตลอดเวลา ซึ่งสิ่งเหล่านี้เป็นเป้าหมายหลักสำหรับอาชญากรไซเบอร์ที่มองหาช่องโหว่ในการป้องกันของเรา

ในขณะที่ทีมรักษาความปลอดภัยต้องจมอยู่กับการแจ้งเตือนและช่องโหว่มากมาย และพยายามปกป้องสินทรัพย์ที่บางครั้งก็ไม่รู้ด้วยซ้ำว่ามีอยู่จริง ASM จึงเป็นกรอบการทำงานเชิงกลยุทธ์ที่จะลดความสับสน ช่วยให้องค์กรระบุ, วิเคราะห์ และจัดการความเสี่ยง ได้ก่อนที่ผู้โจมตีจะนำมาใช้ให้เป็นประโยชน์ในการโจมตี

การทำความเข้าใจและจัดการพื้นที่การโจมตี จึงไม่ได้เป็นเพียงแค่การตอบสนองต่อภัยคุกคาม แต่เป็นการคาดการณ์ล่วงหน้า เป็นการลดความเสี่ยงก่อนที่จะเกิดเหตุการณ์ขึ้นจริง และหนังสือเล่มนี้จะช่วยให้ผู้ทำงานด้านความปลอดภัย, ทีมไอที และผู้บริหารทางธุรกิจ สามารถเดินทางไปในโลกดิจิตอลที่ขยายตัวตลอดเวลาได้อย่างมั่นใจ

ตอนนี้เกมได้เปลี่ยนไปแล้ว เพราะ **ASM คือวิธีที่ทำให้เราก้าวนำการโจมตีอยู่เสมอ**

ใครควรอ่านหนังสือเล่มนี้

ความปลอดภัยทางไซเบอร์ไม่ได้เป็นงานที่จำกัดอยู่แค่แผนกเดียว หรือแค่ทีมเฉพาะทางในศูนย์ปฏิบัติการด้านความปลอดภัยอีกต่อไป แต่ความรับผิดชอบในการรักษาความปลอดภัยสินทรัพย์ขององค์กรนั้นถูกกระจายไปทั่ว ทั้งฝ่ายไอที, ฝ่ายรักษาความปลอดภัย, ฝ่าย DevOps, ฝ่ายปฏิบัติตามกฎระเบียบ และแม้แต่ฝ่ายบริหารของธุรกิจ หากคุณกำลังอ่านข้อความนี้อยู่ แสดงว่าคุณมีบทบาทในการปกป้องสินทรัพย์ดิจิตอลขององค์กร ไม่ว่าคุณจะรู้ตัวหรือไม่ก็ตาม

หนังสือเล่มนี้เหมาะสำหรับผู้ทำงานด้านความปลอดภัย ที่พยายามลดความเสี่ยง, ตอบสนองต่อภัยคุกคาม และเพิ่มสถานะความปลอดภัยในสภาพแวดล้อมดิจิตอลที่ซับซ้อนมากขึ้นเรื่อยๆ นอกจากนี้ยังเหมาะสำหรับผู้ดูแลระบบไอทีที่จัดการโครงสร้างพื้นฐาน, อุปกรณ์ปลายทาง และสภาพแวดล้อมคลาวด์ เพื่อให้ระบบทำงานได้อย่างราบรื่น และมีความปลอดภัย โดย ASM จะเป็นกรอบการทำงานหรือเฟรมเวิร์คที่ช่วยให้มองเห็นภาพรวม, มีการทำงานอัตโนมัติ และควบคุมได้ ทีมไอทีจึงสามารถกำจัดจุดบอดได้ก่อนที่จะเกิดเหตุการณ์ด้านความปลอดภัยขึ้น

ทีม DevOps ก็จะพบว่าหนังสือเล่มนี้มีประโยชน์เช่นกัน เพราะจะช่วยให้ฝังความปลอดภัยลงในขั้นตอนการทำงาน เพื่อไม่ให้เรื่องของความปลอดภัยเป็นเรื่องที่ถูกคิดหลังจากพัฒนาซอฟต์แวร์เสร็จแล้ว แต่ให้กลายเป็นส่วนหนึ่งของการพัฒนาซอฟต์แวร์

สำหรับเจ้าหน้าที่ที่ดูแลด้านกฎระเบียบและผู้จัดการความเสี่ยง จะพบว่า ASM เป็นวิธีในการเชื่อมโยงความปลอดภัยเข้ากับการกำกับดูแล การรู้ว่ามีข้อมูลอ่อนไหวอยู่ที่ไหน, ใครมีสิทธิ์เข้าถึงได้ และมีการพึ่งพากับภายนอกอย่างไร มีความสำคัญอย่างยิ่งต่อการรักษาการปฏิบัติตามกฎระเบียบ ซึ่งหนังสือเล่มนี้จะช่วยให้ผู้ดูแลด้านกฎระเบียบทำงานร่วมกับทีมรักษาความปลอดภัยและทีม

ไอที เพื่อนำมาตรการควบคุมความปลอดภัยไปใช้ในทางปฏิบัติ และยังคงความสอดคล้องกับกฎระเบียบที่องค์กรต้องปฏิบัติ

ท้ายที่สุด หนังสือเล่มนี้เหมาะสำหรับทุกคนที่เกี่ยวข้องกับกลยุทธ์ด้านความปลอดภัยทางไซเบอร์ ไม่ว่าจะเป็นผู้บริหารทางธุรกิจ, ผู้จัดการผลิตภัณฑ์ หรือผู้มีอำนาจตัดสินใจด้านเทคโนโลยี ที่ต้องการความเข้าใจที่ชัดเจนเกี่ยวกับช่องโหว่ในการโจมตี, ความเสี่ยงทางดิจิตอล และการลงทุนด้านความปลอดภัย นั่นคือ ASM ไม่ได้เป็นแค่ความท้าทายทางเทคนิค แต่คือสิ่งจำเป็นทางธุรกิจ ซึ่งผู้บริหารที่เข้าใจถึงความสำคัญของ ASM จะสามารถผลักดันการลงทุนด้านความปลอดภัยที่ชาญฉลาดขึ้น, ปรับปรุงการตอบสนองต่อเหตุการณ์ให้ดีขึ้น และปรับการทำงานด้านความปลอดภัยให้สอดคล้องกับจุดประสงค์ทางธุรกิจได้

สิ่งที่ควรรู้ก่อน

หนังสือเล่มนี้ตั้งอยู่บนสมมติฐานว่า ผู้อ่านมีความเข้าใจพื้นฐานของหลักการด้านความปลอดภัย, สถาปัตยกรรมเครือข่าย และแนวคิดด้านการบริหารความเสี่ยง โดยเนื้อหาถูกออกแบบให้อิงกับการปฏิบัติ, เข้าใจง่าย และนำไปใช้ได้จริง เพื่อให้แม้แต่ผู้ที่เพิ่งเริ่มต้นกับ ASM ก็สามารถเข้าใจ และนำแนวคิดสำคัญไปประยุกต์ใช้อย่างได้ผล

สำรวจเนื้อหา

ASM คือการเดินทาง ไม่ใช่จุดหมาย จึงต้องใช้รากฐานเชิงกลยุทธ์, การปฏิบัติ และการปรับตัวอย่างต่อเนื่อง เพื่อให้ทันต่อภัยคุกคามที่เปลี่ยนไป

หนังสือเล่มนี้ถูกออกแบบมาให้เป็นทั้งคู่มือที่มีโครงสร้าง และเป็นแหล่งอ้างอิงที่ใช้งานได้จริง หากคุณยังใหม่ต่อ ASM ผู้เขียนขอแนะนำให้อ่านส่วนที่ 1 และ 2 เพื่อสร้างพื้นฐาน ก่อนจะลงลึกในรายละเอียดเชิงเทคนิค แต่หากมีความคุ้นเคยกับ ASM อยู่แล้ว และต้องการนำไปใช้งานทันที ก็สามารถข้ามไปยังส่วนที่ 3 และ 4 ได้

- ส่วนที่ 1: ทำความเข้าใจถึงพื้นฐานของการจัดการพื้นที่ที่เสี่ยงต่อการถูกโจมตี
- ส่วนที่ 2: การระบุและจำแนกประเภทของสินทรัพย์ที่ต้องการปกป้อง
- ส่วนที่ 3: การจัดลำดับความสำคัญของช่องโหว่ และการแก้ไขปัญหา
- ส่วนที่ 4: การปรับตัว และการเฝ้าระวัง

แต่ไม่ว่าจะเริ่มต้นจากจุดใด สิ่งหนึ่งที่แน่นอนคือ พื้นที่การโจมตี (attack surface) ยังคงเพิ่มขึ้น, มีการเปลี่ยนแปลง และเผชิญกับภัยคุกคามอยู่เสมอ ดังนั้นการนำหลักการในหนังสือเล่มนี้ไปปรับใช้ จะทำให้สามารถควบคุมและลดความเสี่ยงขององค์กร พร้อมกับก้าวนำผู้โจมตีได้—ทั้งในปัจจุบันและอนาคต

สัญลักษณ์ในเล่ม

 แสดงถึง บันทึกหรือหมายเหตุ

คำขอบคุณ

ผู้เขียนขอขอบคุณผู้ตรวจสอบด้านเทคนิคทุกคน ที่ให้คำแนะนำและคำวิจารณ์ ซึ่งช่วยปรับปรุงให้หนังสือเล่มนี้สมบูรณ์ยิ่งขึ้น

- Chris Devers
- Jeremy Faircloth
- Dane Grace
- Robin Smorenburg
- Josh Summitt
- Sean Sun
- Diana Volere
- Steve Winterfeld

Ron Eddings

ขอขอบคุณ Monika Eddings ภรรยาและเสาหลักของชีวิต ที่อดทนต่อไอเดียด้านความปลอดภัยไซเบอร์ที่ไม่รู้จบของผม ผู้ทำหน้าที่แม่ที่ดีที่สุดให้กับ Ava Rose ลูกสาวของเรา ความอดทน, การสนับสนุน และกำลังใจของคุณ ทำให้ผมมีส่วนร่วมในหนังสือเล่มนี้ได้ และผมคงไม่สามารถมายืนอยู่จุดนี้ได้ หากไม่มีคุณอยู่เคียงข้าง

MJ Kaufmann

ขอขอบคุณอย่างสุดซึ้งต่อ Kurt Kaufmann สามีของฉัน สำหรับการสนับสนุน, คำแนะนำ และคำวิจารณ์ที่สร้างสรรค์ตลอดการเขียนหนังสือเล่มนี้ ขอบคุณเพื่อนสนิท Andrew Matchett, Blanca Betances, Jaime Lumsden และ Dionne Lister ที่ช่วยให้ฉันไม่หลงทาง เชื่อมั่นและเป็นแรงบันดาลใจให้ฉัน และขอบคุณแม่สามีของฉัน ผู้ซึ่งเป็นกำลังใจที่ยิ่งใหญ่ที่สุดของฉัน ขอชื่นชมกลุ่มเพื่อนหญิงของฉันที่คอยสนับสนุน ให้กำลังใจตั้งแต่หน้าแรก และอยู่เคียงข้างจนถึงบทสุดท้าย: Anne Gotay, Michelle Fleming, Sonia Awan, Jen VanAntwerp, Lea Rabinowitz, Gianna Whitver, Karen Walsh และ Joanna Ochoa ขอขอบคุณเป็นพิเศษต่อ Sean Sun, Todd Kamp และ Evan Davis ที่ช่วยให้ฉันมีกำลังใจ และทำให้ฉันหัวเราะได้ แม้ในช่วงเวลาที่ยากลำบาก ขอขอบคุณ Dane Grace, Diana Volere และ Josh Summitt ที่ช่วยให้ฉันมองสิ่งต่างๆ จากมุมมองใหม่ และให้คำแนะนำด้านเทคนิค ที่ช่วยยกระดับหนังสือเล่มนี้ให้ดีที่สุด ขอขอบคุณเป็นพิเศษต่อ Nabeel Nizar ที่เป็นพี่เลี้ยงและผลักดันให้ฉันทำได้ดีที่สุดอย่างแท้จริง และขอขอบคุณบรรณาธิการที่ยอดเยี่ยมของเรา Jill Leonard ซึ่งหากไม่มีเธอ หนังสือเล่มนี้คงไม่เกิดขึ้น รวมถึง Simina Calin ที่เชื่อมั่นในพวกเรา

สารบัญ