

คำชื่นชม

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

— Jeremy Faircloth,

ที่ปรึกษา/สถาปนิกด้านความปลอดภัยไซเบอร์อาวุโส

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

— Chris Devers,

หัวหน้าทีมเทคนิควิศวกรรมบำรุงรักษา, บริษัท EditShare

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

— Dane Grace,

ผู้จัดการผลิตภัณฑ์ด้านความปลอดภัยไซเบอร์อาวุโส

เป็นคู่มือที่ให้กรอบปฏิบัติที่เข้าใจง่าย เพื่อช่วยให้คุณระบุและเข้าใจถึง “พื้นที่การโจมตี” จึงขอแนะนำให้ผู้ที่เกี่ยวข้องกับการลดความเสี่ยง และต้องการปกป้องระบบของตนเอง ได้อ่านหนังสือเล่มนี้อย่างยิ่ง ... เพราะเราไม่สามารถปกป้องสิ่งที่เราไม่รู้ ว่า “มีอยู่” ได้

— Steve Winterfeld,

CISO ในฐานะที่ปรึกษาของบริษัท Cyber Vigilance Advice

คำนำ

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

ASM ไม่ใช่เป็นแค่คำศัพท์ด้านความปลอดภัยที่มักพูดกัน แต่เป็นการเปลี่ยนแปลงระดับรากฐานด้านความปลอดภัยทางไซเบอร์ขององค์กร ในโลกที่การเปลี่ยนแปลงทางดิจิทัลเกิดขึ้นอย่างรวดเร็ว จากการรักษาความปลอดภัยเน็ตเวิร์คและอุปกรณ์แบบเดิมๆ ไปสู่ระบบนิเวศที่กว้างขวางและเชื่อมต่อกันของสภาพแวดล้อมคลาวด์, แอปพลิเคชัน SaaS, API, อุปกรณ์ IoT, พนักงานที่ทำงานจากระยะไกล และการพึ่งพาบนห่วงโซ่อุปทาน พื้นที่ที่เสี่ยงต่อการถูกโจมตีสมัยใหม่จึงกว้างใหญ่, กระจายตัว และเปลี่ยนแปลงอยู่ตลอดเวลา ซึ่งสิ่งเหล่านี้เป็นเป้าหมายหลักสำหรับอาชญากรไซเบอร์ที่มองหาช่องโหว่ในการป้องกันของเรา

ในขณะที่ทีมรักษาความปลอดภัยต้องจมอยู่กับการแจ้งเตือนและช่องโหว่มากมาย และพยายามปกป้องสินทรัพย์ที่บางครั้งก็ไม่รู้ด้วยซ้ำว่ามีอยู่จริง ASM จึงเป็นกรอบการทำงานเชิงกลยุทธ์ที่จะลดความสับสน ช่วยให้องค์กรระบุ, วิเคราะห์ และจัดการความเสี่ยง ได้ก่อนที่ผู้โจมตีจะนำมาใช้ให้เป็นประโยชน์ในการโจมตี

การทำความเข้าใจและจัดการพื้นที่การโจมตี จึงไม่ได้เป็นเพียงแค่การตอบสนองต่อภัยคุกคาม แต่เป็นการคาดการณ์ล่วงหน้า เป็นการลดความเสี่ยงก่อนที่จะเกิดเหตุการณ์ขึ้นจริง และหนังสือเล่มนี้จะช่วยให้ผู้ทำงานด้านความปลอดภัย, ทีมไอที และผู้บริหารทางธุรกิจ สามารถเดินทางไปในโลกดิจิทัลที่ขยายตัวตลอดเวลาได้อย่างมั่นใจ

ตอนนี้เกมได้เปลี่ยนไปแล้ว เพราะ ASM คือวิธีที่ทำให้เราก้าวนำการ
โจมตีอยู่เสมอ

ใครควรอ่านหนังสือเล่มนี้

ความปลอดภัยทางไซเบอร์ไม่ได้เป็นงานที่จำกัดอยู่แค่แผนกเดียว หรือแค่
ทีมเฉพาะทางในศูนย์ปฏิบัติการด้านความปลอดภัยอีกต่อไป แต่ความรับผิดชอบ
ในการรักษาความปลอดภัยสินทรัพย์ขององค์กรนั้นถูกกระจายไปทั่ว ทั้งฝ่ายไอที,
ฝ่ายรักษาความปลอดภัย, ฝ่าย DevOps, ฝ่ายปฏิบัติตามกฎระเบียบ และแม้แต่
ฝ่ายบริหารของธุรกิจ หากคุณกำลังอ่านข้อความนี้อยู่ แสดงว่าคุณมีบทบาทใน
การปกป้องสินทรัพย์ดิจิทัลขององค์กร ไม่ว่าจะคุณจรรู้ตัวหรือไม่ก็ตาม

หนังสือเล่มนี้เหมาะสำหรับผู้ทำงานด้านความปลอดภัย ที่พยายามลด
ความเสี่ยง, ตอบสนองต่อภัยคุกคาม และเพิ่มสถานะความปลอดภัยในสภาพ
แวดล้อมดิจิทัลที่ซับซ้อนมากขึ้นเรื่อยๆ นอกจากนี้ยังเหมาะสำหรับผู้ดูแลระบบ
ไอทีที่จัดการโครงสร้างพื้นฐาน, อุปกรณ์ปลายทาง และสภาพแวดล้อมคลาวด์
เพื่อให้ระบบทำงานได้อย่างราบรื่น และมีความปลอดภัย โดย ASM จะเป็นกรอบ
การทำงานหรือเฟรมเวิร์คที่ช่วยให้มองเห็นภาพรวม, มีการทำงานอัตโนมัติ และ
ควบคุมได้ ทีมไอทีจึงสามารถกำจัดจุดบอดได้ก่อนที่จะเกิดเหตุการณ์ด้านความ
ปลอดภัยขึ้น

ทีม DevOps ก็พบว่าหนังสือเล่มนี้มีประโยชน์เช่นกัน เพราะจะช่วยให้
ฝังความปลอดภัยลงในขั้นตอนการทำงาน เพื่อไม่ให้เรื่องของความปลอดภัยเป็น
เรื่องที่ถูกคิดหลังจากพัฒนาซอฟต์แวร์เสร็จแล้ว แต่ให้กลายเป็นส่วนหนึ่งของการ
พัฒนาซอฟต์แวร์

สำหรับเจ้าหน้าที่ที่ดูแลด้านกฎระเบียบและผู้จัดการความเสี่ยง จะพบ
ว่า ASM เป็นวิธีในการเชื่อมโยงความปลอดภัยเข้ากับการกำกับดูแล การรู้ว่ามี
ข้อมูลอ่อนไหวอยู่ที่ไหน, ใครมีสิทธิ์เข้าถึงได้ และมีการพึ่งพากับภายนอกอย่างไร
มีความสำคัญอย่างยิ่งต่อการรักษาการปฏิบัติตามกฎระเบียบ ซึ่งหนังสือเล่มนี้
จะช่วยให้ผู้ดูแลด้านกฎระเบียบทำงานร่วมกับทีมรักษาความปลอดภัยและทีม

ไอที เพื่อนำมาตรการควบคุมความปลอดภัยไปใช้ในทางปฏิบัติ และยังคงความปลอดภัยคล่องกับกฎระเบียบที่องค์กรต้องปฏิบัติ

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

สิ่งที่ควรรู้อีกก่อน

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

สำรวจเนื้อหา

ASM คือการเดินทาง ไม่ใช่จุดหมาย จึงต้องใช้รากฐานเชิงกลยุทธ์, การปฏิบัติ และการปรับตัวอย่างต่อเนื่อง เพื่อให้ทันต่อภัยคุกคามที่เปลี่ยนแปลงไป

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 ที่อดทนต่อ
ไอเดียด้านความปลอดภัยไซเบอร์ที่ไม่รู้จักของผม ผู้ทำหน้าที่แม่ที่ดีที่สุดให้กับ
Ava Rose ลูกสาวของเรา ความอดทน, การสนับสนุน และกำลังใจของคุณ ทำให้
ผมมีส่วนร่วมในหนังสือเล่มนี้ได้ และผมคงไม่สามารถมายืนอยู่จุดนี้ได้ หากไม่มี
คุณอยู่เคียงข้าง

MJ Kaufmann

ขอขอบคุณอย่างสุดซึ้งต่อ Kurt Kaufmann สามีน้องฉัน สำหรับการ
สนับสนุน, คำแนะนำ และคำวิจารณ์ที่สร้างสรรค์ตลอดการเขียนหนังสือเล่มนี้
ขอบคุณเพื่อนสนิท Andrew Matchett, Blanca Betances, Jaime Lumsden
และ Dionne Lister ที่ช่วยให้ฉันไม่หลงทาง เชื่อมั่นและเป็นแรงบันดาลใจให้
ฉัน และขอบคุณแม่สามีน้องฉัน ผู้ซึ่งเป็นกำลังใจที่ยิ่งใหญ่ที่สุดของฉัน ขอชื่นชม
กลุ่มเพื่อนหญิงของฉันที่คอยสนับสนุน ให้กำลังใจตั้งแต่หน้าแรก และอยู่เคียง
ข้างจนถึงบทสุดท้าย: 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 ที่ช่วยให้ฉันมอง
สิ่งต่างๆ จากมุมมองใหม่ และให้คำแนะนำด้านเทคนิค ที่ช่วยยกระดับหนังสือ
เล่มนี้ให้ดีที่สุด ขอขอบคุณเป็นพิเศษต่อ Nabeel Nizar ที่เป็นพี่เลี้ยงและผลักดัน
ให้ฉันทำได้ดีที่สุดในทุกเรื่อง และขอขอบคุณบรรณาธิการที่ยอดเยี่ยมของเรา
Jill Leonard ซึ่งหากไม่มีเธอ หนังสือเล่มนี้คงไม่เกิดขึ้น รวมถึง Simina Calin
ที่เชื่อมั่นในพวกเรา

สารบัญ

ส่วนที่ 1 พื้นฐานของการจัดการพื้นที่ที่เสี่ยงต่อการถูกโจมตี	21
บทที่ 1 พื้นฐาน: ภาพรวมของการจัดการพื้นที่ที่เสี่ยงต่อการถูกโจมตี	23
ASM คืออะไร และมีความจำเป็นอย่างไร	24
พื้นที่ที่เสี่ยงต่อการถูกโจมตีคืออะไร?	25
Attack Vector และ Attack Surface	27
การจัดการพื้นที่การโจมตีคืออะไร?	33
องค์ประกอบของ ASM	39
การระบุสินทรัพย์	40
การจำแนกประเภท	42
การจัดลำดับความสำคัญ	43
การแก้ไขปัญหา	44
การปรับตัว	45
การเฝ้าติดตาม	45
บทบาทเชิงกลยุทธ์ของ ASM ด้านความปลอดภัยไซเบอร์	46
มองจากมุมมองของผู้โจมตี	46
เปลี่ยนมุมมองความคิด	47
กลยุทธ์เชิงรุก: คิดแบบผู้โจมตี	51
กรณีการใช้งาน ASM และความท้าทายด้านความปลอดภัย	52
ความท้าทายด้านการมองเห็น	52
การจัดการสินทรัพย์	53
ข้อมูลเชิงลึกของสินทรัพย์	53
Shadow IT	54
การจัดการความเสี่ยง	55

การตอบสนองและจัดลำดับความสำคัญของเหตุการณ์	57
การบังคับใช้นโยบาย	58
การปฏิบัติตามกฎระเบียบ	59
สรุป	60
บทที่ 2 ประเภทของพื้นที่การโจมตี	63
พื้นที่การโจมตีที่ขยายตัวอย่างต่อเนื่อง	63
องค์ประกอบไอทีแบบดั้งเดิม	65
ระบบเสมือนจริงแบบดั้งเดิม	66
องค์ประกอบในระบบไอทีสมัยใหม่	67
ระบบเสมือนจริงยุคใหม่	67
IoT	68
เว็บไซต์	69
ไบร่บรอง	70
คลาวด์	71
ผู้ให้บริการคลาวด์	71
เวิร์คโหลดบนคลาวด์	72
คอนเทนเนอร์	73
แอปพลิเคชันบนคลาวด์	74
ข้อมูล	75
การจัดการการตั้งค่า	76
SaaS	76
การจัดการ SaaS	77
ตัวตน	78
ผู้ใช้	79
การเข้าถึงข้อมูลข้ามแพลตฟอร์ม	80
ความท้าทายในการจัดการตัวตนและการเข้าถึง	81

ห่วงโซ่อุปทาน (Supply Chain)	82
การพัฒนาซอฟต์แวร์	83
แอปพลิเคชัน	84
หน่วยงานออกใบรับรอง	84
BYOD และอุปกรณ์เคลื่อนที่	85
ปัญญาประดิษฐ์	86
โมเดล AI และสถาปัตยกรรมนิเวศอินเทอร์เน็ตเวิร์ค	86
ไปป์ไลน์และโครงสร้างพื้นฐานของ AI	87
ยูเซอร์อินเทอร์เฟซ และ API ของ AI	88
สรุป	89
บทที่ 3 พื้นที่การโจมตีเกี่ยวข้องกับความเสี่ยงอย่างไร	91
การวัดความเสี่ยง	91
การประเมินความเสี่ยงเชิงคุณภาพ	95
ตัวอย่าง	95
ประโยชน์ที่ได้	97
ความท้าทาย	98
การประเมินความเสี่ยงเชิงปริมาณ	98
ตัวอย่าง	98
ขั้นตอนปฏิบัติ: การประเมินความเสี่ยงเชิงปริมาณ	99
ประโยชน์	101
ความท้าทาย	102
การเลือกวิธีที่เหมาะสม	102
ข้อควรพิจารณาด้านข้อมูลและความซับซ้อน	102
ข้อควรพิจารณาด้านทรัพยากรและความสามารถ	103
ข้อควรพิจารณาด้านวัตถุประสงค์และผู้มีส่วนได้ส่วนเสีย	104
ควรใช้ทั้ง 2 วิธีร่วมกันหรือไม่?	105

ตัวอย่าง: การเลือกวิธีการที่เหมาะสม	106
เฟรมเวิร์กด้านความเสี่ยง	107
NIST	109
ISO	111
ITIL v4	113
COSO ERM	114
OCTAVE	116
การสื่อสารความเสี่ยงไปยังทีมธุรกิจ	118
รู้จักผู้รับสารของคุณ	119
ศัพท์เทคนิคจะทำให้ทีมธุรกิจสับสน	119
วิธีแปลงความเสี่ยงทางเทคนิคให้เป็นภาษาธุรกิจ	120
จัดการกับข้ออ้างสำหรับการสื่อสารที่ไม่ดี	121
สรุป	122
ส่วนที่ 2 การระบุและจำแนกประเภท	125
บทที่ 4 การระบุและจำแนกประเภทสินทรัพย์	129
การระบุสินทรัพย์	130
รายการสินทรัพย์	130
เหตุใดการดูแลรายการสินทรัพย์จึงเป็นรากฐานของ ASM	132
โซลูชันสำหรับการจัดการสินทรัพย์	134
การค้นพบสินทรัพย์	138
การจำแนกประเภทเพื่อเข้าใจสินทรัพย์มากขึ้น	144
รายละเอียดชนิดของสินทรัพย์	145
ข้อมูลการตั้งค่า	146
การจำแนกประเภทของข้อมูล	147
ข้อมูลการใช้งาน	149

ข้อมูลตำแหน่งและสภาพแวดล้อม	150
การขึ้นต่อกันของสินทรัพย์	151
สถานะความปลอดภัยของสินทรัพย์	152
สถานะวงจรชีวิตของสินทรัพย์	153
การผสมผสานความเข้าใจในสินทรัพย์เข้ากับกลยุทธ์ธุรกิจ	155
จัดลำดับความสำคัญได้ดีขึ้น	156
รายการสินทรัพย์ที่ต้องดูแล	158
การติดตามสิทธิ์การใช้งานซอฟต์แวร์	158
หลักฐานสำหรับการตรวจสอบการทำตามข้อกำหนด	160
สรุป	161
บทที่ 5 การค้นพบสินทรัพย์แบบอัตโนมัติ	163
ความสำคัญของการทำ Asset Discovery แบบอัตโนมัติ	164
ขอบเขตขององค์กร	165
ความซับซ้อนของระบบคลาวด์	168
ประเภทของการค้นหาสินทรัพย์แบบอัตโนมัติ	174
การสแกนเครือข่าย	174
การวิเคราะห์คลาวด์	177
การระบุ API	179
การค้นพบข้อมูล	180
ความท้าทายในการค้นหาอัตโนมัติ	181
คุณสมบัติที่ให้ความคุ้มค่าต่อการลงทุน	184
ความสามารถในการค้นหา	184
การแสดงผลข้อมูล	185
การวิเคราะห์และรายงาน	186
พีเจเออร์ระดับสูง	187
สรุป	188

ส่วนที่ 3 การจัดลำดับความสำคัญและการแก้ไขปัญหา	191
บทที่ 6 การจัดลำดับความสำคัญและการวิเคราะห์ถึงสินทรัพย์ที่สำคัญที่สุด	195
ทำความเข้าใจกับการจัดลำดับความสำคัญ	195
การสนับสนุนต่อกระบวนการเชิงกลยุทธ์อื่นๆ	197
ความสำคัญของการจัดลำดับสินทรัพย์	197
เกณฑ์ในการจัดลำดับความสำคัญ	200
มูลค่าต่อองค์กร	201
ผลกระทบต่อการทำงาน	202
ความอ่อนไหวและการจำแนกประเภทข้อมูล	204
การทำความเข้าใจในบริบททางธุรกิจ	209
การจัดทำแผนผังฟังก์ชันทางธุรกิจ	210
เครื่องมือและเทคนิคสำหรับการทำแผนผัง	211
การประเมินผลกระทบ	213
การหาลำดับความสำคัญที่แท้จริง	214
การระบุถึงสินทรัพย์ที่สำคัญที่สุด	214
การทบทวนและอัปเดตสินทรัพย์สำคัญเป็นระยะ	217
การระบุสินทรัพย์ที่มีมูลค่าสูงอื่นๆ	218
การจัดอันดับสินทรัพย์อื่นๆ	219
สรุป	224
บทที่ 7 การประมาณการพื้นที่ที่เสี่ยงต่อการถูกโจมตี	227
การวิเคราะห์พื้นที่การโจมตี	227
ASA มีขั้นตอนอย่างไร	228
ASA ช่วยเสริมสร้างความปลอดภัยอย่างไร	229
พื้นที่การโจมตีภายในและภายนอก	230

การวิเคราะห์พื้นที่การโจมตีภายใน	230
การวิเคราะห์พื้นที่การโจมตีภายนอก	233
พื้นที่ทับซ้อน	238
เครื่องมือสำหรับการประเมินพื้นที่การโจมตี	240
การสร้างแบบจำลองภัยคุกคาม	241
การสร้างแบบจำลองภัยคุกคามเพื่อช่วยบริหารความเสี่ยง	241
ระเบียบวิธีสร้างแบบจำลองภัยคุกคาม	242
ควรใช้วิธีใด?	245
รวมการสร้างแบบจำลองภัยคุกคามเข้ากับการทำแผนที่	
พื้นที่การโจมตี	248
แบบจำลองภัยคุกคามช่วยปรับปรุง ASM ได้อย่างไร	249
ASM มีส่วนเติมเต็มให้กับแบบจำลองภัยคุกคามอย่างไร	249
สรุป	250
บทที่ 8 การแก้ไขปัญหา	253
ประเมินความต้องการในการแก้ไขปัญหา	253
การระบุความรุนแรงของช่องโหว่	254
การประเมินผลกระทบที่อาจเกิดขึ้น	255
การวิเคราะห์ต้นทุนและประโยชน์ของการแก้ไขปัญหา	257
การจัดลำดับความสำคัญของความเสี่ยง	259
ความง่ายต่อการใช้โจมตี	259
ความสามารถในการค้นพบ	261
ลำดับความสำคัญของผู้โจมตี	262
ความซับซ้อนของการแก้ไขปัญหา	264
กลยุทธ์ในการแก้ไขปัญหา	266
การตรวจสอบการแก้ไขปัญหา	271
พีตแบ็คคูลจากผู้เกี่ยวข้อง	272

การเฝ้าระวังปัญหาที่ไม่คาดคิด	272
การทำเอกสารและการรายงาน	273
สรุป	276
ส่วนที่ 4 การปรับเปลี่ยนและเฝ้าระวัง	279
บทที่ 9 การลดพื้นที่การโจมตี	283
การลดพื้นที่ที่เสี่ยงต่อการถูกโจมตี	284
วิธีการเชิงกลยุทธ์	284
เทคนิคเชิงยุทธวิธี	297
สรุป	304
บทที่ 10 การเฝ้าระวังและจัดการแบบต่อเนื่อง	307
ลักษณะของระบบนิเวศดิจิทัล	307
การเปลี่ยนแปลงทางเทคโนโลยีและการบูรณาการใหม่ๆ	308
ผลกระทบของการเปลี่ยนแปลงองค์กรต่อระบบนิเวศ	311
การกำหนดเกณฑ์ในการแจ้งเตือน	312
การแยกแยะผลลัพธ์ผิดพลาดกับภัยคุกคามจริง	312
การปรับแต่งเกณฑ์	313
การแจ้งเตือนตามบริบท	315
การบูรณาการเข้ากับการตอบสนองต่อเหตุการณ์	316
ประสานการเฝ้าระวังเข้ากับทีมตอบสนองต่อเหตุการณ์	316
การจำลองสถานการณ์การละเมิด	318
กลยุทธ์การตอบสนองอย่างรวดเร็วและการบรรเทาผลกระทบ	321
การทบทวนและตรวจสอบเป็นระยะ	323
การสแกนช่องโหว่ต่อเนื่อง	323

ประเมินการดำเนินงานและประสิทธิภาพในการแก้ไขปัญหา สม่ำเสมอ	324
กลับมาประเมินลำดับความสำคัญของสินทรัพย์เป็นระยะ	326
พีดแบ็คอุป และการปรับปรุงอย่างต่อเนื่อง	326
ส่งเสริมความร่วมมือระหว่างทีมต่างๆ	327
นำบทเรียนจากเหตุการณ์ในอดีตมาใช้ให้เกิดประโยชน์	329
การปรับกลยุทธ์การเฝ้าระวังตามพีดแบ็ค	331
ระบบอัตโนมัติและ AI ในการเฝ้าระวังแบบต่อเนื่อง	332
ประโยชน์ของเครื่องมือเฝ้าระวังอัตโนมัติ	333
บทบาทของ AI ในการตรวจจับและวิเคราะห์ภัยคุกคาม	334
การสร้างสมดุลระหว่างระบบอัตโนมัติและการดูแลด้วยคน	336
สรุป	337
บทที่ 11 อนาคตของการจัดการพื้นที่ที่เสี่ยงต่อการถูกโจมตี	339
แนวโน้มของ ASM	340
AI และ ML ใน ASM	341
การประมวลผลแบบควอนตัม	345
ความท้าทายสำหรับเอเดจคอมพิวติง	347
ความท้าทายด้านความปลอดภัยไซเบอร์ที่เปลี่ยนแปลงไป	348
ก้าวทันแนวทางปฏิบัติและเทคโนโลยีด้าน ASM	349
การเรียนรู้อย่างต่อเนื่อง และการพัฒนาทักษะ	350
อย่าหยุดเรียนรู้ และอย่ายอมแพ้	351