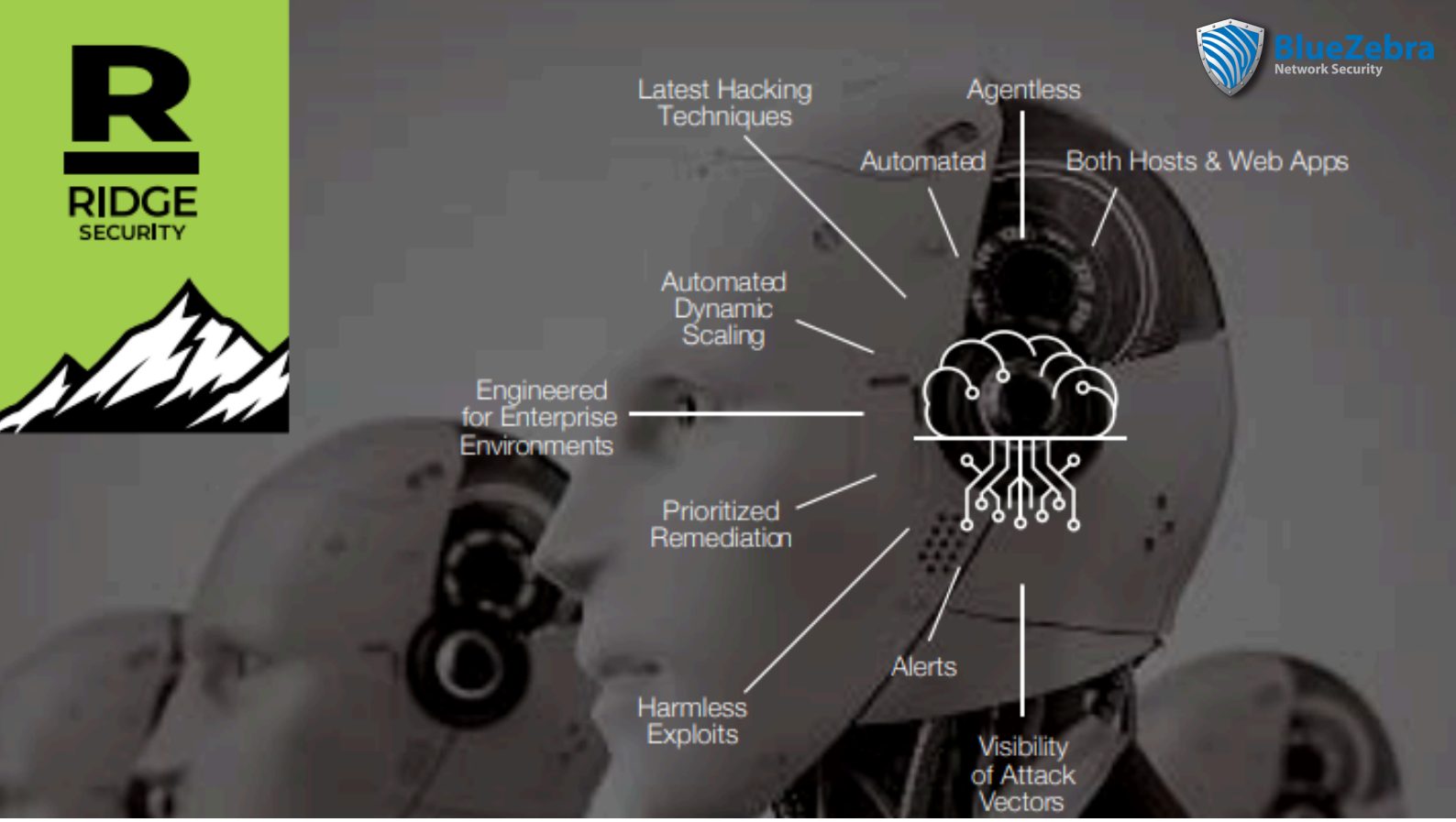
RIDGE SECURITY

BlueZebra Network Security



การจัดการความเสี่ยง ระบบอัตโนมัติ จากภัยคุกคามอย่างต่อเนื่อง

RidgeBot® AI Agent for Continuous Security Validation

RidgeBot® เป็นตัวแทน AI ที่ออกแบบมาเพื่อการตรวจสอบความปลอดภัยอย่างต่อเนื่อง มันดำเนินการโดยอัตโนมัติ การทดสอบตามเป้าหมายที่กำหนดโดยทีมรักษาความปลอดภัยของคุณ RidgeBot® สามารถค้นพบพื้นผิวการโจมตี จัดลำดับความสำคัญของช่องโหว่ตามความสามารถในการใช้ประโยชน์ ทำการทดสอบการเจาะระบบอัตโนมัติและจำลอง การโจมตีของฝ่ายตรงข้าม กระบวนการที่ต่อเนื่องนี้จะตรวจสอบสถานะความปลอดภัยทางไซเบอร์ขององค์กรของคุณและ เสนอข้อแนะนำในการแก้ไข

RidgeBot® ให้ภาพที่ชัดเจนยิ่งขึ้นเกี่ยวกับช่องว่างด้านความปลอดภัยของคุณ โดยการเพิ่มความถี่ของ การทดสอบการเจาะระบบ การจัดการช่องโหว่ตามความเสี่ยง และการฝึกอบรมทีมป้องกันของคุณด้วย แบบฝึกหัดที่มีประสิทธิภาพ RidgeBot® ช่วยป้องกันผู้โจมตีที่เป็นอันตราย มันช่วยเหลือทีมรักษาความปลอดภัยของคุณ ในการเอาชนะข้อจำกัดด้านความรู้และประสบการณ์ ปฏิบัติงานในระดับสูงสุดอย่างต่อเนื่อง

RidgeBot® บรรเทาปัญหาการขาดแคลนผู้เชี่ยวชาญด้านความปลอดภัยโดยเปลี่ยนจากการใช้แรงงานคนและต้องใช้แรงงานคนมาก การทดสอบระบบอัตโนมัติแบบใช้เครื่องจักรช่วย ช่วยให้ผู้เชี่ยวชาญด้านความมั่นคงของมนุษย์สามารถทุ่มเทพลังงานของตนได้ ในการค้นคว้าภัยคุกคามและเทคโนโลยีใหม่ๆ

ทางออกโซลูชั่น และประโยชน์ที่สำคัญ

RidgeBot® เป็นระบบครบวงจรที่ทำการทดสอบการเจาะระบบอัตโนมัติ ประมวลผลและจำลองการโจมตีของฝ่ายตรงข้ามเพื่อตรวจสอบความถูกต้องขององค์กร ท่าทีการรักษาความปลอดภัยทางไซเบอร์ ช่วยให้เห็นภาพช่องว่างด้านความปลอดภัยของคุณได้ชัดเจนยิ่งขึ้น และปิดหน้าต่างแห่งโอกาสสำหรับผู้โจมตีที่เป็นอันตรายด้วย การเพิ่มความถี่ของการทดสอบการเจาะระบบ ความเปราะบางตามความเสี่ยง การจัดการและการฝึกอบรมทีมป้องกันของคุณด้วยแบบฝึกหัดที่มีประสิทธิภาพ RidgeBot® ช่วยเหลือทีมรักษาความปลอดภัยในการเอาชนะความรู้และประสบการณ์ ข้อจำกัดและดำเนินการในระดับบนสุดที่สอดคล้องกันเสมอ การเปลี่ยนแปลงจาก การทดสอบแบบแมนนวลและใช้แรงงานเข้มข้นกับระบบอัตโนมัติที่ใช้เครื่องช่วย บรรเทาปัญหาการขาดแคลนผู้เชี่ยวชาญด้านความปลอดภัยอย่างรุนแรงในปัจจุบัน มันช่วยให้ ผู้เชี่ยวชาญด้านความมั่นคงของมนุษย์จะละทิ้งงานที่ใช้แรงงานเข้มข้นในแต่ละวันและอุทิศตนพลังงานมากขึ้นในการวิจัยภัยคุกคามและเทคโนโลยีใหม่ ๆ

- **ปรับปรุงความครอบคลุมการทดสอบความปลอดภัยและประสิทธิภาพ**
- **ลดค่าใช้จ่ายในการรักษาความปลอดภัยการตรวจสอบ**
- **ปกป้องระบบไอทีอย่างต่อเนื่องด้วยโครงสร้างพื้นฐาน**
- **ผลิตได้จริงและเชื่อถือได้ผลลัพธ์สำหรับผู้มีส่วนได้เสียที่แตกต่างกัน**

การทดสอบการเจาะระบบอัตโนมัติ

การจำลองทางไซเบอร์ของฝ่ายตรงข้าม (ACE)

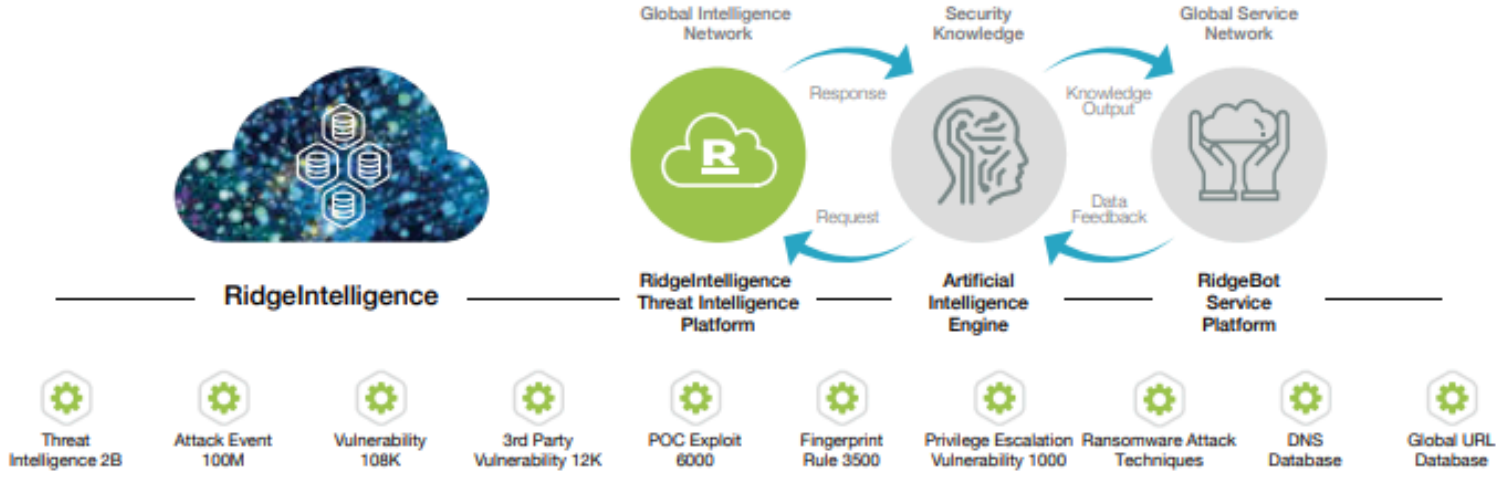
การควบคุมความปลอดภัยด้านไอทีเป็นกลไกที่ใช้ป้องกัน ตรวจจับ และบรรเทาภัยคุกคามและการโจมตีทางไซเบอร์ RidgeBot® ACE เลียนแบบฝ่ายตรงข้ามโดยเลียนแบบเส้นทางและเทคนิคการโจมตีที่เป็นไปได้เพื่อสร้างการประเมินอย่างต่อเนื่อง ข้อมูลเพื่อช่วยระบุความล้มเหลวในการควบคุมความปลอดภัย แก้ไขจุดอ่อนเชิงโครงสร้าง และเปิดใช้งานการเพิ่มประสิทธิภาพการควบคุมความปลอดภัย RidgeBot® ACE ได้ปรับตัวเองให้สอดคล้องกับกรอบงาน MITER ATT&CK และแมปสคริปต์ทดสอบการประเมินกับ MITER กลยุทธ์และเทคนิคของ ATT&CK สิ่งนี้จะเพิ่มการมองเห็นเวกเตอร์การโจมตีที่อาจเกิดขึ้นและปรับปรุงการสื่อสารของการวัดผลการควบคุมความปลอดภัย

การจัดการสินทรัพย์

RidgeBot® มอบพื้นที่เก็บข้อมูลแบบรวมศูนย์เพื่อจัดการสินทรัพย์ไอทีขององค์กรสำหรับการตรวจสอบความปลอดภัย รวมถึง IP ของสินทรัพย์ ที่อยู่, ชื่อโฮสต์, เวอร์ชันของระบบปฏิบัติการ, พอร์ตบริการที่เปิดอยู่, แอปพลิเคชันที่ใช้งานอยู่พร้อมเวอร์ชัน, ชื่อโดเมนเว็บไซต์, ความละเอียด DNS และเวอร์ชันของเว็บเซิร์ฟเวอร์

ความแม่นยำที่สูงขึ้นและการค้นพบที่มากขึ้นด้วย AI Brain

RidgeBot® มีแกน AI ที่ทรงพลังพร้อมฐานความรู้ของผู้เชี่ยวชาญที่จะแนะนำการเลือกเส้นทางการโจมตี มันเปิดตัว การโจมตีซ้ำตามการเรียนรู้ตลอดเส้นทาง บรรลุผลการทดสอบที่ครอบคลุมและการตรวจสอบเชิงลึก



On-Premise Deployment

สำหรับสภาพแวดล้อมองค์กร—ปรับใช้ RidgeBot® บนสถานที่ของลูกค้าช่วยลดความเสี่ยงของ Infosec ข้อมูลรั่วไหล

Cloud Deployment

สำหรับลูกค้า Cloud และ SMB—ปรับใช้ RidgeBot® ใน คลาวด์ (AWS EC2, Microsoft Azure และ Google Cloud) มีความยืดหยุ่นที่ดีขึ้นในขณะที่ลดการลงทุน CapEx เริ่มต้นให้เหลือน้อยที่สุด

Ridge Security มอบโซลูชันการตรวจสอบความปลอดภัยที่มีจริยธรรม มีประสิทธิภาพ และราคาไม่แพงให้กับองค์กรทั้งขนาดเล็กและขนาดใหญ่ เราตรวจสอบให้แน่ใจว่าลูกค้าของเราปฏิบัติตาม แจ้งเตือน และปลอดภัยตลอดเวลาในโลกไซเบอร์ ทางฝ่ายบริหารก็ได้ ประสบการณ์ด้านเครือข่ายและความปลอดภัยหลายปี Ridge Security ตั้งอยู่ในใจกลางของ Silicon Valley และขยายไปสู่พื้นที่อื่นๆ เช่น ละตินอเมริกา เอเชีย และยุโรป RidgeBot® ซึ่งเป็นระบบตรวจสอบความปลอดภัยของหุ่นยนต์ทำให้กระบวนการทดสอบเป็นอัตโนมัติเต็มรูปแบบโดยผสมผสานหลักจริยธรรมขั้นสูงเข้าด้วยกันเทคนิคการแฮ็กและการจำลองทางไซเบอร์ของฝ่ายตรงข้าม RidgeBots ค้นหา ใช้ประโยชน์ และบันทึกความเสี่ยงทางธุรกิจ และพบช่องโหว่ ความปลอดภัยด้านไอทีควบคุมความล้มเหลวในระหว่างกระบวนการทดสอบ โดยเน้นถึงผลกระทบที่อาจเกิดขึ้นหรือความเสียหาย

กรณีศึกษา :

สนามบินนานาชาติโทกุเมนเลือก RidgeBot Pentesting เพื่อระบบที่คล่องตัวและยืดหยุ่นการปฏิบัติการรักษาความปลอดภัยในการทำงานได้มากขึ้น

Ridge Security Technology Inc. www.ridgesecurity.ai
© 2024 All Rights Reserved Ridge Security Technology Inc. RidgeBot is a trademark of Ridge Security Technology Inc.

จากลูกค้าจริงที่ใช้งาน

ในเมืองปานามาซิตี้ ประเทศปานามา สนามบินนานาชาติโทกุเมนเป็นสนามบินหลักของภูมิภาคซึ่งบริหารจัดการสนามบินระดับภูมิภาค 4 แห่ง โดยทำหน้าที่เป็นศูนย์กลางที่สำคัญทั้งภายในประเทศและระหว่างประเทศ มีเที่ยวบินและมีพนักงานมากกว่า 1,700 คน สนามบินนี้จึงรับประกันได้ถึงการดำเนินงานที่มีประสิทธิภาพ

อาคารสนามบินที่กว้างขวางมีบทบาทสำคัญในการเดินทางทางอากาศและการขนส่งสินค้าเนื่องด้วยการให้บริการผู้โดยสารกว่า 17,820,000 ราย สายการบินกว่า 31 สาย และการขนส่งสินค้าจำนวนกว่า 208,000 ตันต่อปี

ความท้าทาย

สนามบินเผชิญกับความท้าทายด้านความปลอดภัยที่สำคัญในการปรับใช้ระบบใหม่ๆเข้ากับการทำงาน และการเปลี่ยนแปลงระบบที่มีอยู่ และเนื่องจากมีการใช้แอปพลิเคชันที่สำคัญมากมายทำให้สนามบินโดนการโจมตีทางไซเบอร์ทุกวัน จึงจำเป็นต้องมีโซลูชันเพื่อจัดลำดับความสำคัญของช่องโหว่กว่าร้อยรายการ และสามารถระบุตัวการสำคัญเพื่อให้ทีมสามารถมุ่งเน้นไปที่การขจัดความเสี่ยงก่อนแล้วจึงย้อนมาตัวที่รุนแรงน้อยกว่า

เพื่อจัดการกับความท้าทายเหล่านี้ สนามบินนานาชาติโทกุเมนได้ว่าจ้างบริษัททดสอบการเจาะแบบ manual เพื่อทำการทดสอบระบบ แต่กระบวนการแบบ manual นี้ทำให้เกิดความล่าช้าอย่างมากและขาดความคล่องตัวในการให้บริการ การดำเนินการทดสอบการเจาะระบบหนึ่งครั้ง ต้องใช้เวลาถึงสามเดือนในการทำสัญญา, หกสัปดาห์สำหรับการทดสอบ, และหนึ่งเดือนสำหรับรายงานขั้นสุดท้าย สนามบินจำเป็นต้องลดขั้นตอนและลดต้นทุนการทดสอบ ค่าธรรมเนียมรายปีสำหรับการทดสอบการเจาะแบบ manual อยู่ที่กว่า 130,000 ดอลลาร์ สนามบินต้องการลดต้นทุนดังกล่าวลงครึ่งหนึ่ง

ความต้องการของสนามบิน Tocumen ที่ต้องการจะทำการทดสอบแบบเจาะลึกภายในองค์กรเมื่อใดก็ได้ จำเป็นต้องมีโซลูชันแบบอัตโนมัติและใช้งานง่าย จุดมุ่งหมายคือเพื่อขจัดความล่าช้าในการทำงาน และสร้างมาตรการรักษาความปลอดภัยที่คล่องตัวและสม่ำเสมอมากขึ้น

ปัญหาสำคัญคือการทดสอบทำได้ไม่บ่อยนัก โดยสามารถดำเนินการได้เพียงปีละหนึ่งครั้งเท่านั้น เมื่อไม่มีการทดสอบสม่ำเสมอ ภัยคุกคามทางไซเบอร์ก็ยิ่งทวีความรุนแรงมากขึ้น การปรับปรุงโครงสร้างพื้นฐานทั้งหมดถือเป็นสิ่งสำคัญ การทำ Pentest แบบ manual นั้นจำกัดไว้เฉพาะ serversและ workstation เท่านั้น สนามบินต้องการความคุ้มครองที่กว้างโดยสามารถทดสอบอะไรก็ได้จาก IP address ซึ่งได้แก่เว็บเซิร์ฟเวอร์ อุปกรณ์กล้องวงจรปิด, ระบบควบคุมการเข้าออก, Firewall, เครื่องพิมพ์, โทรศัพท์แบบ IP, ระบบแสดงข้อมูลเที่ยวบิน, อุปกรณ์สื่อสาร และอุปกรณ์รักษาความปลอดภัย เป็นต้น

การแก้ไขปัญหา

สนามบินได้เลือก RidgeBot ซึ่งเป็นแพลตฟอร์มตรวจสอบความปลอดภัยที่ขับเคลื่อนด้วย AI ที่ทำงานเชิงรุก ค้นพบและกำจัดภัยคุกคามด้วยการเจาะระบบอัตโนมัติได้บ่อยครั้งและต่อเนื่อง การทดสอบ แตกต่างจากการทดสอบแบบ manual เพราะ RidgeBot ทำงานอย่างไม่รู้จักเหน็ดเหนื่อย และสามารถดำเนินการได้อย่างสม่ำเสมอ สามารถเจาะลึกแบบรายสัปดาห์หรือรายวัน และจัดทำรายงานแนวโน้มของปัญหาที่ผ่านมาเพื่อการวิเคราะห์อีกด้วย

Ridgebot ปกป้องแอปพลิเคชันทั้งหมดของสนามบิน ซึ่งมีความสำคัญอย่างยิ่งต่อการบำรุงรักษา ประสิทธิภาพในการดำเนินงาน ความปลอดภัย และประสบการณ์ของผู้โดยสาร ใดยมีแอปพลิเคชันหลัก 3 แอปพลิเคชัน ที่สำคัญในการใช้งาน

ระบบขนย้ายสัมภาระ: ระบบที่มีความยาวถึง 4 กิโลเมตร อาจโดนโจมตีได้ทุกเมื่อ RidgeBot ทดสอบทั้งระบบเพื่อค้นหาช่องโหว่ที่อาจถูกโจมตีได้

ระบบกล้องวงจรปิดรักษาความปลอดภัย: ระบบที่สำคัญต่อสนามบินและความมั่นคงของชาติ ระบบนี้ใช้การจดจำใบหน้าผู้คนในการยับยั้งการก่อการร้าย RidgeBot ทดสอบกล้องวงจรปิดโดยใช้ IP address และเซิร์ฟเวอร์ที่รันระบบ ในระหว่างการแฮกแบบสมมุติ RidgeBot ใช้เว็บอินเทอร์เฟซของกล้อง เพื่อจำลองแฮกเกอร์ที่เข้าควบคุม ซึ่งช่วยให้พนักงานของสนามบินเข้าใจจุดอ่อนและแก้ไขได้อย่างรวดเร็ว

ระบบการจัดการสนามบินโดยรวม: นี่เป็นภารกิจที่สำคัญอย่างยิ่งในการประสานงานการปฏิบัติงานและกิจกรรมของสนามบินทั้งหมด และความมั่นใจในการทำงานทั่วทั้งสนามบินอย่างราบรื่น ทุกสัปดาห์ RidgeBot จะทดสอบเซิร์ฟเวอร์หลายสิบเครื่องที่สนับสนุนระบบเพื่อหาช่องโหว่เพื่อให้แน่ใจว่ามีความพร้อมใช้งาน

สนามบินใช้ประโยชน์จากการรายงานที่ชัดเจนและภาพตัวช่วยของ RidgeBot เช่น KillChain เพื่อการแก้ไข ซึ่งจะช่วยให้ทีมของสนามบิน Tocumen สามารถแสดงภาพกราฟิกและมุมมองเชิงตรรกะของขั้นตอนทั้งหมดที่ RidgeBot ใช้ เพื่อใช้ประโยชน์จากช่องโหว่ของระบบ ตัวอย่างเช่น หากเซิร์ฟเวอร์ถูกโจมตีได้สำเร็จในระหว่างการทดสอบ ระบบอื่นอาจถูกใช้เพื่อเข้าถึงเซิร์ฟเวอร์นั้น RidgeBot ระบุช่องโหว่บนระบบเหล่านั้นโดยไม่รบกวนเซิร์ฟเวอร์ที่รองรับการปฏิบัติงานของสนามบิน

นอกจากนี้ Tocumen ยังใช้การประเมินความปลอดภัยกับแรนซัมแวร์ การประเมินการรั่วไหลของข้อมูล การตรวจสอบความปลอดภัยของ Active Directory และการตรวจสอบการใช้รหัสผ่านที่ไม่รัดกุม คุณสมบัติเหล่านี้มีความสำคัญในการเสริมสร้างมาตรการรักษาความปลอดภัยของสนามบินและรับประกันการป้องกันที่แข็งแกร่ง

สิทธิประโยชน์

RidgeBot ได้รับการพิสูจน์แล้วว่าเป็นเครื่องมือในการระบุช่องโหว่ที่สามารถใช้ประโยชน์ได้ในระบบที่มักถูกมองข้าม เช่น เครื่องพิมพ์ หรืออุปกรณ์ CCTV และอุปกรณ์ IoT เมื่อเปรียบเทียบกับการทดสอบแบบ manual โดยผู้เชี่ยวชาญ RidgeBot มีความรวดเร็วและแม่นยำกว่าในการค้นหา เพิ่มความสามารถของสนามบินในการจัดการกับจุดอ่อนด้านความปลอดภัยได้อย่างมีประสิทธิภาพมากขึ้น

สนามบินได้ปรับปรุงมาตรการรักษาความปลอดภัยอย่างมีนัยสำคัญโดยการลดระยะเวลาการเปิดเผยของช่องโหว่ใหม่ที่สามารถแสวงหาประโยชน์ได้ นอกจากนี้ ยังปรับใช้บริการใหม่ๆ ในการทำงานได้ทันทีอีกด้วย RidgeBot ได้ปรับปรุงประสิทธิภาพการทำงานของเจ้าหน้าที่รักษาความปลอดภัยของสนามบิน ช่วยให้พวกเขามุ่งเน้นไปที่ช่องโหว่ที่สามารถแสวงหาประโยชน์ และจัดลำดับความสำคัญของช่องโหว่ที่สำคัญที่สุดรวมถึงความเสี่ยงที่อาจเกิดขึ้น

ผู้ให้บริการ Pentest รายอื่นได้รับการประเมิน อย่างไรก็ตาม โซลูชันอื่นๆ จำเป็นต้องมี server agents ซึ่งทำให้การติดตั้งและการดำเนินงานมีความซับซ้อนมากขึ้น นอกจากนี้ ไม่มีผลิตภัณฑ์อื่นที่ทำงานได้ดีสำหรับหน้าเว็บ และไม่มีการทดสอบเว็บเซิร์ฟเวอร์เลย พวกเขายังขาดอินเทอร์เฟซที่ใช้งานง่าย ทำให้การนำทางและทำความเข้าใจมีความลำบาก ท้ายที่สุดแล้วปัจจัยเหล่านี้ทำให้ Tocumen เลือก RidgeBot

> “เราชื่นชมผล false positiveของ Ridgebot เป็นพิเศษ ที่สามารถระบุจุดอ่อนที่แสวงหาประโยชน์ได้ ตรวจสอบ และแสดงหลักฐานเพื่อยืนยันความเสี่ยงเหล่านั้น นอกจากนี้ การรายงานแบบเรียลไทม์ของ RidgeBots ยังให้ผลลัพธ์ทันที แทนที่จะต้องรอเป็นสัปดาห์ ”
>
> *Abdy Sanjur* ผู้จัดการนวัตกรรมภายในเทคโนโลยี
> รองประธานสนามบินนานาชาติโทกุเมน

ข้อมูลเพิ่มเติมอื่นๆ จากประสบการณ์ของพนักงานสนามบิน ถึงประโยชน์ในการใช้ RidgeBot

- Interface ที่ใช้งานง่าย ช่วยลดความยุ่งยากในการทดสอบและสะดวกในการใช้งานโดยรวม
- การรายงานแบบเรียลไทม์ให้ข้อมูลเชิงลึกที่เกี่ยวกับช่องโหว่ด้านความปลอดภัยในทันที ช่วยให้แก้ไขได้รวดเร็ว
- ประหยัดเวลาได้มาก และมีประสิทธิภาพเพิ่มขึ้นเมื่อเทียบกับการทดสอบแบบ manual
- มีการตรวจสอบอย่างต่อเนื่อง ช่วยรักษาความยืดหยุ่นด้านความปลอดภัย และป้องกันการละเมิด
- ความแม่นยำและประสิทธิผลในการเจาะระบบอัตโนมัติของการระบุช่องโหว่ช่วยเพิ่มมาตรการรักษาความปลอดภัยของสนามบิน Tocumen
- การทำงานแบบ agentless ทำให้แตกต่างจากโซลูชันอื่นๆ
- มีความเป็นเลิศในการทดสอบเว็บที่ให้บริการ

RidgeBot เป็นส่วนสำคัญในการรักษาความปลอดภัยแบบหลายชั้นที่ครอบคลุมของ Tocumen ช่วยให้สนามบินสามารถทดสอบการรักษาความปลอดภัยของโครงสร้างพื้นฐานด้านไอทีทั้งหมดได้ ทำให้มีความมั่นใจมากขึ้นเมื่อโครงสร้างพื้นฐานด้านไอทีได้รับการทดสอบตรวจสอบ และรักษาความปลอดภัยในเชิงรุกก่อนที่สิ่งใดๆ จะสามารถถูกนำไปใช้ในการแสวงหาประโยชน์ได้

สนามบินนานาชาติโทกุเมน วางแผนที่จะใช้ RidgeBot ในศูนย์ปฏิบัติการด้านความปลอดภัยแห่งใหม่ โดยทำหน้าที่เป็นทีมสำคัญที่จะดำเนินป้องกันการโจมตีอย่างแม่นยำและไวต่อการตอบสนองในทุกเหตุการณ์

เกี่ยวกับ Ridge Security

Ridge Security เป็นผู้นำในด้านการจัดการความเสี่ยง (Risk Management) และทุ่มเทในการพัฒนาผลิตภัณฑ์ความปลอดภัยทางไซเบอร์ที่เป็นนวัตกรรมซึ่งเป็นประโยชน์ต่อ CISO และทีมรักษาความปลอดภัยโดยการลดความเสี่ยงผ่านการตรวจสอบและใช้ระบบอัตโนมัติเพื่อปรับปรุงประสิทธิภาพ ผลิตภัณฑ์ของ Ridge Security ได้รวมเอาปัญญาประดิษฐ์ขั้นสูง (AI) เพื่อมอบการตรวจสอบความปลอดภัยที่ครอบคลุม การป้องกันปริมาณงานที่มีประสิทธิภาพ และการตรวจสอบความปลอดภัยของระบบคลาวด์

© 2024 All Rights Reserved Ridge Security Technology Inc. RidgeBot is a trademark of Ridge Security Technology Inc.

RIDGE SECURITY