Acalvio ShadowPlex Advanced Threat Defense

พลิกสถานการณ์ไปยังฝ่ายตรงข้ามด้วยการป้องกันทางไซเบอร์และการหลอกล่อในระดับองค์กร

เหตุใดศัตรูจึงมีข้อได้เปรียบเหนือการป้องกัน

ความปลอดภัยทางไซเบอร์ในปัจจุบัน บางครั้งดูเหมือนว่าผู้โจมตีจะมีข้อได้เปรียบเหนือผู้ป้องกันอย่างแทบไม่มีอะไรจะเอาชนะได้ หากต้องการเจาะระบบป้องกันรอบนอกขององค์กร ผู้คุกคามสามารถกำหนดเป้าหมายเซิร์ฟเวอร์และอุปกรณ์ที่อาจมีความเสี่ยงได้หลายร้อยเครื่อง ติดตั้งมัลแวร์หรือแรนซัมแวร์ในอุปกรณ์ปลายทางจำนวนหนึ่งจากจำนวนหลายพันเครื่อง หรือขโมยข้อมูลประจำตัวจากพนักงานที่ไม่ระมัดระวังจำนวนเท่าใดก็ได้ เมื่อเข้าไปข้างในองค์กรแล้ว พวกเขาสามารถเข้าถึงข้อมูลด้วยวิธีที่มีโอกาสถูกตรวจพบน้อยมาก โดยเฉพาะอย่างยิ่งหากรวบรวมข้อมูลส่วนตัวที่ถูกต้องไว้แล้ว ผู้โจมตีจำเป็นต้องค้นหาจุดอ่อนเพียงจุดเดียวเพื่อให้ประสบความสำเร็จ ในขณะที่ทีมงานด้านความปลอดภัยต้องปกป้องจุดที่อาจเกิดความล้มเหลวได้ในหลายจุด

พลิกสถานการณ์ด้วยการป้องกันไซเบอร์เชิงรุก

การป้องกันทางไซเบอร์เชิงรุกช่วยพลิกสถานการณ์จากฝ่ายตรงข้าม โดยผสมผสานแนวทางอันทรงพลังสองแนวทางในการรักษาความปลอดภัย:

- **Deception technology**, Wซึ่งทำให้สภาพแวดล้อมการประมวลผลขององค์กรเต็มไปด้วยเครื่องมือล่อลวงและองค์ประกอบการหลอกล่อมากมายที่ดึงดูดและทำให้ผู้โจมตีเข้าใจผิด
- **Predictive analytics**, ซึ่งคาดการณ์การกระทำของผู้โจมตีและวางองค์ประกอบการหลอกล่อที่สร้างขึ้นอย่างระมัดระวังไว้บนเส้นทางของพวกเขาโดยตรง

การป้องกันทางไซเบอร์เชิงรุกช่วยให้ทีมป้องกันสามารถเปลี่ยนแปลงภูมิทัศน์ของศัตรูได้ โดยการใช้องค์ประกอบการหลอกล่อใหม่ๆ อย่างต่อเนื่อง ซึ่งปรับให้เหมาะกับอุตสาหกรรมขององค์กรและโปรไฟล์ภัยคุกคามในสถานที่ที่ผู้ก่อภัยคุกคามมักเข้าไปแฝงตัวมากที่สุด องค์ประกอบการหลอกล่อดึงดูดความสนใจของผู้โจมตีนำพวกเขาออกห่างจากข้อมูลและระบบจริง และแจ้งเตือนทีมรักษาความปลอดภัยถึงทุกการเคลื่อนไหวของพวกเขา

แนวทางเชิงคาดการณ์นี้ทำให้การป้องกันทางไซเบอร์มีมิติเชิงรุกมากขึ้น ช่วยให้ทีมงานด้านความปลอดภัยสามารถตรวจจับภัยคุกคามทางไซเบอร์ได้ในระยะเริ่มต้นและควบคุมภัยคุกคามได้อย่างรวดเร็ว การป้องกันทางไซเบอร์เชิงรุกไม่ได้หมายถึงผู้ป้องกัน แต่เป็นศัตรูที่ต้องเผชิญกับจุดล้มเหลวที่อาจเกิดขึ้นได้หลายร้อยจุด

Acalvio ShadowPlex Advanced Threat Defense

Acalvio นำเสนอเทคโนโลยีป้องกันไซเบอร์อัตโนมัติที่ครอบคลุมในระดับองค์กร ShadowPlex Advanced Threat Defense (ATD) เป็นแพลตฟอร์มการหลอกลวงทางไซเบอร์ชั้นนำของโลก ซึ่งสร้างขึ้นบนแพลตฟอร์ม Active Defense ชั้นนำของอุตสาหกรรมของ Acalvio ซึ่งใช้ประโยชน์จากสิทธิบัตรมากกว่า 25 ฉบับเกี่ยวกับการหลอกลวงโดยอัตโนมัติ

ShadowPlex ATD เติมเต็มสภาพแวดล้อมการประมวลผลขององค์กรด้วยองค์ประกอบการหลอกลวงปลายทางที่หลากหลาย ซึ่งช่วยนำศัตรูออกจากทรัพย์สินข้อมูลที่ถูกต้องและหันไปใช้ข้อมูลจำลองที่สมจริง นอกจากนี้ ยังช่วยให้ทีมป้องกันไซเบอร์สามารถตรวจจับและบันทึกกลวิธีและเทคนิคขั้นสูงของผู้โจมตีสำหรับการลาดตระเวนเครือข่าย persistence การเกระจายตัว การยกระดับสิทธิ์ การหลบเลี่ยงการป้องกัน การขโมยข้อมูล และการกระทำที่เป็นอันตรายอื่นๆ

ชุดการหลอกล่อที่สมจริงและปรับขยายได้

ShadowPlex ATD นำเสนอองค์ประกอบการหลอกล่อที่สร้างไว้ล่วงหน้ามากกว่า 250 องค์ประกอบที่สอดคล้องกับประเภทการโจมตีที่เฉพาะเจาะจง ลูกค้าสามารถปรับแต่งการหลอกล่อของ Acalvio และสร้างองค์ประกอบใหม่ได้

องค์ประกอบการหลอกล่อที่มีใน ShadowPlex ATD ได้แก่:

การหลอกล่อ – เป้าหมายที่น่าดึงดูดและเข้าถึงได้ซึ่งเพิ่มเข้าไปในเครือข่ายเพื่อล่อผู้โจมตีให้ห่างจากข้อมูลและแอปพลิเคชันจริง เช่น เซิร์ฟเวอร์ ปลายทาง โฮสต์ VM แอปพลิเคชัน ฐานข้อมูล ไดเรกทอรี บัคเก็ตที่จัดเก็บข้อมูลบนคลาวด์ และเครือข่าย OT ที่เป็นของปลอมแต่สมจริง Breadcrumbs – ตัวชี้ไปยังการหลอกล่อซึ่งเพิ่มเข้าไปในทรัพย์สินที่ถูกต้องที่มีอยู่ เช่น เส้นทางที่สร้างขึ้นซึ่งแคชไว้ในเซิร์ฟเวอร์ ข้อมูลรับรองการเข้าถึงที่สมมติขึ้นในโปรไฟล์ผู้ใช้และไฟล์บันทึก และลิงก์ FTP, RDP และ SSH

เหยื่อล่อ – วัตถุที่ทำหน้าที่เป็นสายล่อเมื่อเข้าถึงหรือเคลื่อนย้าย เช่น เอกสารและไฟล์ปลอม, honey accounts (บัญชีผู้ใช้และบัญชีบริการที่หลอกลวง), และ honey tokens (ข้อมูลรับรองผู้ใช้สำหรับผู้ใช้ที่มีสิทธิพิเศษที่ไม่มีอยู่จริง)

เมื่อศัตรูโต้ตอบกับองค์ประกอบการหลอกลวงเหล่านี้ เทคโนโลยีของ Acalvio จะ:

- แจ้งเตือนทีมรักษาความปลอดภัยทันทีถึงการโจมตีที่เกิดขึ้น
- เมื่อมีการโจมตีเกิดขึ้น ให้ใช้การวิเคราะห์เชิงคาดการณ์เพื่อปรับใช้องค์ประกอบการหลอกลวงใหม่ในเส้นทางที่ผู้โจมตีมักจะใช้
- รวบรวมข้อมูลนิติวิทยาศาสตร์โดยละเอียดเกี่ยวกับจุดปลายทางที่ถูกบุกรุกและบันทึก TTP ของการโจมตีแต่ละครั้ง
- ดำเนินการตอบสนองอัตโนมัติเพื่อแยกภัยคุกคามและปกป้องทรัพย์สินจริง

การแจ้งเตือนคุณภาพสูงและการกักกันอย่างรวดเร็ว

ShadowPlex ATD ช่วยปรับปรุงความสามารถของ SOC และองค์กรตอบสนองต่อเหตุการณ์ในการค้นหาและกักกันภัยคุกคามอันตรายได้อย่างรวดเร็ว

เมื่อเปรียบเทียบกับเครื่องมือตรวจจับทั่วไป โซลูชันการป้องกันไซเบอร์เชิงรุกจะสร้างการแจ้งเตือนคุณภาพสูงขึ้นโดยมีผลบวกปลอมน้อยกว่ามาก องค์ประกอบการหลอกล่อไม่ได้เป็นส่วนหนึ่งของกระบวนการทางธุรกิจที่ถูกต้อง ดังนั้นการโต้ตอบใดๆ ก็ตามบ่งชี้ถึงกิจกรรมที่เป็นอันตรายได้อย่างชัดเจน

ShadowPlex ATD ให้ความแม่นยำยิ่งขึ้นด้วยการคัดกรองอัตโนมัติโดยใช้ประโยชน์จากแหล่งข้อมูลหลายแหล่ง, AI, และการวิเคราะห์ขั้นสูงเพื่อระบุเหตุการณ์การหลอกล่อที่เกี่ยวข้องกับภัยคุกคามที่ร้ายแรงที่สุดต่อองค์กร

ShadowPlex ATD ยังช่วยให้ทีมงานรักษาความปลอดภัยสามารถควบคุมการโจมตีได้อย่างรวดเร็ว ซึ่งสามารถ:

- กักกันระบบที่ได้รับผลกระทบโดยอัตโนมัติ
- เมื่อมีสัญญาณของกิจกรรมที่เป็นอันตราย ให้สร้างองค์ประกอบการหลอกลวงแบบกำหนดเองใหม่เพื่อเบี่ยงเบนผู้โจมตีออกจากทรัพย์สินจริง
- ให้คำตอบแก่ผู้ตอบสนองต่อเหตุการณ์ที่เกิดขึ้นสำหรับคำถามสำคัญ เช่น "เซสชันและกระบวนการของผู้ใช้ปลายทางใดที่ทำให้เกิดการแจ้งเตือน" "ปลายทางสื่อสารกับทรัพย์สินใด" และ "ปลายทางอื่นใดพบเห็นการดำเนินการที่คล้ายคลึงกัน"

การวิเคราะห์เชิงทำนายและข่าวกรองภัยคุกคาม

ShadowPlex ATD ใช้การวิเคราะห์เชิงทำนายเพื่อคาดการณ์การเคลื่อนไหวครั้งต่อไปที่ผู้โจมตีจะทำและวางองค์ประกอบการหลอกลวงเพิ่มเติมในเส้นทางของพวกมัน นอกจากนี้ยังช่วยให้ทีมตอบสนองต่อเหตุการณ์แยกภัยคุกคามและปกป้องทรัพย์สินที่มีมูลค่าสูงก่อนที่ผู้โจมตีจะพบได้

ShadowPlex ATD ยังช่วยให้ทีมรักษาความปลอดภัยลดความเสี่ยงในระยะยาวอีกด้วย โดยเปิดเผย TTP ของผู้โจมตีเพื่อให้ทีมรักษาความปลอดภัยสามารถระบุมาตรการตอบโต้ที่มีประสิทธิภาพสูงสุดได้ นอกจากนี้ยังมีเครื่องมือวิเคราะห์เพื่อช่วยกำหนดลำดับความสำคัญของการดำเนินการแก้ไข

ระบบอัตโนมัติที่ขับเคลื่อนด้วย AI ซึ่งเพิ่มประสิทธิภาพและลดงาน

ShadowPlex ATD ใช้ระบบอัตโนมัติที่ขับเคลื่อนด้วย AI เพื่อออกแบบ ปรับแต่ง ปรับใช้ และจัดการองค์ประกอบการหลอกลวงนับพันรายการโดยไม่เพิ่มภาระให้กับทีมรักษาความปลอดภัย

ผู้โจมตีมีความฉลาด พวกเขาจะไม่หลงกลโดยตัวล่อที่ดูเรียบง่าย นิ่ง หรืออยู่ผิดที่ เพื่อดึงดูดและหลอกลวงพวกเขา องค์ประกอบการหลอกลวงจะต้องมีจำนวนมาก สมจริง เหมาะสมกับอุตสาหกรรมขององค์กร และสภาพแวดล้อมคอมพิวเตอร์ และต้องเปลี่ยนบ่อยครั้ง แต่กลุ่มรักษาความปลอดภัยไม่มีเจ้าหน้าที่เพียงพอที่จะดำเนินการงานเหล่านี้ด้วยตนเอง

ShadowPlex ATD จัดการกับความท้าทายนี้โดย:

- จัดเตรียมชุดการหลอกลวงที่ครอบคลุมพร้อมตัวล่อ breadcrumbs และเหยื่อล่อเฉพาะมากกว่า 250 ตัวที่สร้างขึ้นบนเครือข่ายจริงและสแต็กแอปพลิเคชัน
- ใช้ AI และระบบอัตโนมัติเพื่อกำหนดค่าและปรับแต่งองค์ประกอบการหลอกลวงสำหรับซับเน็ตและทรัพย์สินแต่ละรายการ
- นำเสนอคู่มือการหลอกลวงที่ปรับแต่งได้ซึ่งใช้งาน, จัดการ, และรีเฟรชตัวล่อ, breadcrumbs, และเหยื่อล่อโดยอัตโนมัติ

การใช้งานที่สำคัญ ได้แก่:

- ตรวจจับภัยคุกคามแบบ zero day threats, APTs, polymorphic และ fileless malware และภัยคุกคามขั้นสูงอื่นๆ ที่หลุดรอดจากเครื่องมือตรวจจับและป้องกันแบบเดิม
- ปกป้อง endpoints รวมถึงเวิร์กสเตชันและเซิร์ฟเวอร์ของผู้ใช้
- ปกป้องเครือข่ายจากภัยคุกคามที่เน้นเครือข่าย
- ปกป้องสินทรัพย์สำคัญ รวมถึงฐานข้อมูลและแอปพลิเคชันที่สำคัญ
- ป้องกัน ransomware
- ปกป้องสภาพแวดล้อม OT/ICS (เทคโนโลยีปฏิบัติการและระบบควบคุมอุตสาหกรรม)
- ปกป้องเวิร์กโหลดบนคลาวด์ในสภาพแวดล้อมคลาวด์แบบ hybrid และ pure-play

การปรับขยาย, การควบคุม, และการใช้งานที่รวดเร็ว

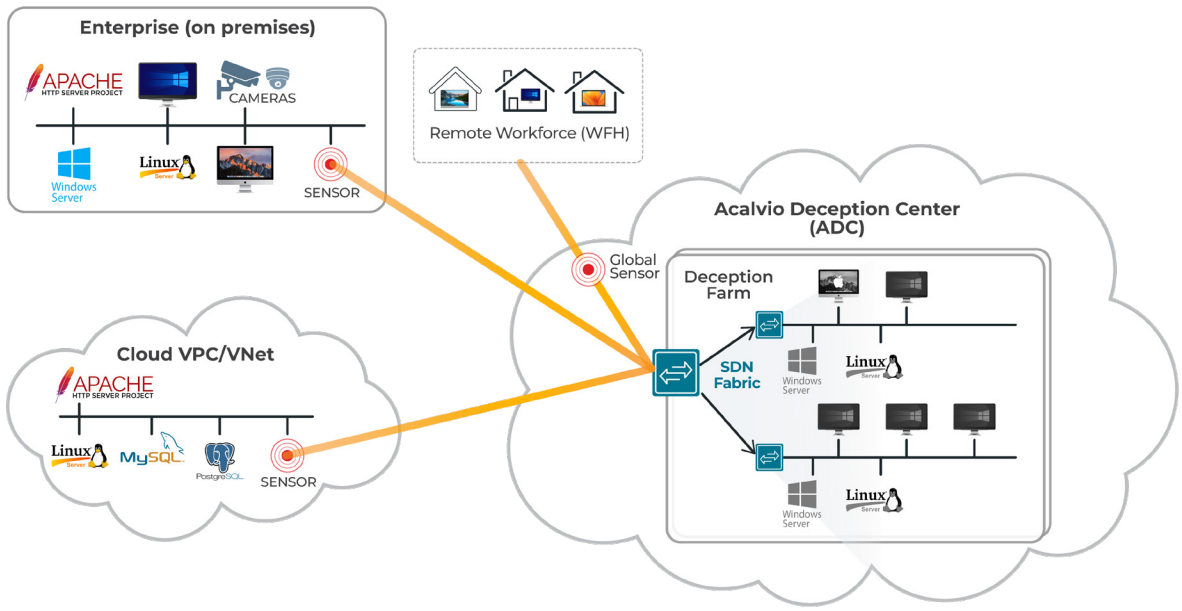
เทคโนโลยีของ Acalvio มอบการป้องกันทางไซเบอร์ที่ครอบคลุมในสภาพแวดล้อมองค์กรขนาดใหญ่ที่หลากหลาย โดยรองรับ:

- On-premises, cloud, และ remote workloads
- ระบบปฏิบัติการ เครือข่าย และประเภทอุปกรณ์ที่หลากหลาย
- Operational technology (OT) รวมถึงสภาพแวดล้อมด้านไอที

ไม่จำเป็นต้องใช้ endpoint agent

ShadowPlex ATD ได้รับการปรับใช้ในสภาพแวดล้อมที่มีปลายทางมากกว่า 100,000 จุดและซับเน็ตจำนวนมากในหลายตำแหน่ง

ตามที่แสดงในรูปที่ 1 ตัวล่อลวง ShadowPlex ATD ทั้งหมดจะถูกโฮสต์ไว้ใน Acalvio Deception Center (ADC) ในระบบคลาวด์ วิธีนี้ช่วยลดความซับซ้อนในการจัดการ นอกจากนี้ แม้ว่าผู้โจมตีจะ "เห็น" ทรัพย์สินบนเครือข่ายที่ตนกำลังโจมตี แต่การโต้ตอบทั้งหมดจะเกิดขึ้นในสภาพแวดล้อมที่ถูกจำกัดซึ่งแยกออกจากข้อมูลจริงและกระบวนการทางธุรกิจ เพื่อเร่งความเร็วในการใช้งานและส่งมอบคุณค่าในทันที ShadowPlex ATD จึงจัดทำคู่มือการหลอกลวงที่รวบรวมความรู้เฉพาะด้านเกี่ยวกับวิธีการใช้งานองค์ประกอบการหลอกลวงที่ปรับแต่งให้เหมาะกับภัยคุกคามเฉพาะ ทีมป้องกันไซเบอร์สามารถใช้คู่มือเหล่านี้เพื่อให้ครอบคลุมกรณีการใช้งานที่เกี่ยวข้องที่สุดได้ทันที และด้วยระบบอัตโนมัติที่ขับเคลื่อนด้วย AI ใน ShadowPlex ATD คุณสามารถใช้งานการหลอกลวงได้หลายพันครั้งในเวลาไม่กี่นาที



รูปที่ 1: สถาปัตยกรรม Acalvio ShadowPlex; ShadowPlex ATD เติมเต็มสภาพแวดล้อมการประมวลผลขององค์กรด้วยองค์ประกอบการหลอกลวงนับพันรายการเพื่อนำผู้โจมตีออกห่างจากทรัพย์สินข้อมูลที่ถูกต้องและแจ้งเตือนทีมงานด้านความปลอดภัยถึงการกระทำของพวกเขา