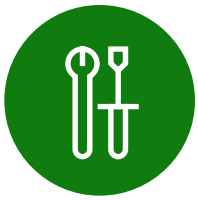
Microsoft Security

3 เหตุผลในการเปลี่ยนแปลงไปสู่การป้องกันภัยคุกคามแบบผสานรวม

สารบัญ

ข้อมูลเบื้องต้น



ในปัจจุบัน โดยเฉลี่ยแล้วองค์กรใช้เครื่องมือรักษาความปลอดภัยที่แตกต่างกันมากกว่า 30 รายการ ซึ่งมักจะแยกส่วนและ “เพิ่มเติมเข้ามา”

การรักษาความปลอดภัยอยู่ในจุดต่ำสุด การโจมตีทางไซเบอร์มีความซับซ้อนมากขึ้น ซึ่งองค์กรต่างๆ ยังคงต่อสู้กับความท้าทายอย่างต่อเนื่อง ตั้งแต่การขาดแคลนบุคลากรที่มีความสามารถและการสร้างความสมดุลของต้นทุน ไปจนถึงการรับมือกับแรงกดดันของการทำงานแบบไฮบริด

ในขณะเดียวกัน ตลาดการรักษาความปลอดภัยนั้นแยกส่วนและซับซ้อนกว่าที่เคย ในปัจจุบัน โดยเฉลี่ยแล้วองค์กรใช้เครื่องมือรักษาความปลอดภัยที่แตกต่างกันมากกว่า 30 รายการ ซึ่งมักจะแยกส่วนและ “เพิ่มเติมเข้ามา” ทำให้มองเห็นได้อย่างจำกัดและมีข้อมูลเชิงลึกไม่เพียงพอสำหรับศูนย์ปฏิบัติการด้านความปลอดภัย (SOC)

ผู้นำด้านการรักษาความปลอดภัยและการปฏิบัติตามกฎระเบียบต้องการความเข้าใจที่ดีขึ้นเกี่ยวกับความเสี่ยงและภัยคุกคามล่าสุด ซึ่งยังต้องรู้อีกด้วยว่าอะไรได้ผล อะไรไม่ได้ผล และมีช่องว่างอยู่ที่ใด

แม้ว่าขอบเขตของความท้าทายด้านการรักษาความปลอดภัยในปัจจุบันอาจดูแน่นขนัด แต่ก็มีสาเหตุในเชิงบวกสำหรับ CISO ที่ต้องการปรับปรุงประสิทธิภาพและประสิทธิผลของการดำเนินงานด้านความปลอดภัย คำตอบอยู่ในแนวทางการป้องกันภัยคุกคามทางไซเบอร์แบบผสานรวมที่ครบวงจรซึ่งจะช่วยให้องค์กร:

เหตุผลที่ 1: ทำสิ่งต่างๆ ได้มากขึ้นโดยใช้ต้นทุนที่ต่ำลง

รวมโซลูชันเฉพาะจุดและลดค่าใช้จ่ายด้านการดำเนินการรักษาความปลอดภัย (SecOps)

เหตุผลที่ 2: เพิ่มขีดความสามารถให้ SecOps เพื่อมุ่งเน้นไปที่งานที่มีมูลค่าสูง

ใช้เครื่องมือที่เพิ่มประสิทธิภาพและทำให้แม้แต่นักวิเคราะห์มือใหม่ก็มีความสามารถมากกว่าที่เคย

เหตุผลที่ 3: เพิ่มประสิทธิภาพการทำงานของพนักงาน

ปกป้องค์กรของคุณด้วยวิธีที่ทำให้พนักงานของคุณไม่ต้องกลัวเมื่อต้องสร้างสรรค์นวัตกรรมใหม่ๆ

วิธีการนี้เกิดขึ้นได้โดยการรวมโซลูชันการตรวจหาและการตอบสนองแบบขยาย (XDR) เข้ากับระบบข้อมูลด้านการรักษาความปลอดภัยและการจัดการเหตุการณ์ (SIEM) แบบคลาวด์เนทีฟที่ใช้ปัญญาประดิษฐ์ (AI) และความสามารถของระบบอัตโนมัติ โซลูชันแบบผสานรวมสามารถช่วยให้ SOC ของคุณคาดการณ์ล่วงหน้า ดำเนินการเชิงรุก และป้องกันการโจมตีทั่วทั้งองค์กรได้มากขึ้น

เหตุผลข้อที่ 1

ทำสิ่งต่างๆ ได้มากขึ้น โดยใช้ต้นทุนที่ต่ำลง

ด้วยการรวมเครื่องมือเข้ากับโซลูชันแบบผสานรวมของ Microsoft ทำให้คุณสามารถประหยัดได้โดยจ่ายเฉพาะส่วนที่คุณใช้เท่านั้น

องค์กรหลายแห่งเข้าหาเครื่องมือรักษาความปลอดภัยโดยเน้นที่โซลูชันเฉพาะจุดที่ดีที่สุด แต่น่าเสียดายที่แนวทางดังกล่าวอาจทำให้ผู้เชี่ยวชาญด้านการรักษาความปลอดภัยระบุและตอบสนองต่อภัยคุกคามอย่างรวดเร็วได้ยากขึ้น นอกจากนี้ อาจจบลงด้วยผลกระทบด้านลบต่อการใช้จ่ายด้านไอทีและประสิทธิภาพการทำงานของผู้ใช้ปลายทาง

จากการที่องค์กรต่างๆ ต้องการทำสิ่งต่างๆ ได้มากขึ้นโดยใช้ต้นทุนที่ต่ำลง ซึ่งวิธีการแบบผสานรวม เช่น SIEM และ XDR ของ Microsoft สามารถช่วยได้ สามารถลดความซับซ้อนได้ด้วยการรวมเครื่องมือแต่ละอย่างเข้าด้วยกัน และเนื่องจากเป็นแบบคลาวด์เนทีฟ โซลูชันแบบผสานรวมจึงสามารถปรับปรุงประสิทธิภาพและปรับขนาดได้

ด้วยการรวมเครื่องมือเข้ากับโซลูชันแบบผสานรวมของ Microsoft ทำให้คุณสามารถประหยัดได้โดยจ่ายเฉพาะส่วนที่คุณใช้เท่านั้น คุณยังสามารถลดค่าใช้จ่ายด้าน SecOps ที่จำเป็นในการจัดการโซลูชันโดยการเพิ่มระบบอัตโนมัติและการผสานรวม

> การเริ่มต้นกระบวนการนำเครื่องมือรักษาความปลอดภัยใหม่ๆ มาใช้นั้นเป็นเรื่องง่าย เพราะคุณคาดว่าช่องว่างจะกว้าง แต่จากจุดนั้นในไม่ช้าคุณจะทราบว่าเครื่องมือจากผู้จัดจำหน่ายแต่ละรายอาจมีหน้าที่ที่ทับซ้อนกัน การทับซ้อนดังกล่าวอาจเป็นที่ต้องการสำหรับการตรวจสอบและหาสมดุล **แต่ก็อาจมาพร้อมกับต้นทุนทางการเงินที่สูงมาก**”
>
> **Jonathan Cassar**
> Chief Technology Officer, MITA

1.6 ล้านดอลลาร์

ประหยัดได้ในแต่ละปีจากการรวมผู้จัดจำหน่าย

Microsoft มอบหมายให้ Forrester Consulting ดำเนินการศึกษา Total Economic Impact™ (TEI) และตรวจสอบผลตอบแทนจากการลงทุน (ROI) ที่องค์กรอาจได้รับจากการปรับใช้ Microsoft SIEM และ XDR สิ่งเหล่านี้เป็นข้อค้นพบที่สำคัญบางส่วนสำหรับองค์กรสมมุติที่มีพนักงานทั้งหมด 8,000 คนและผู้เชี่ยวชาญด้านการรักษาความปลอดภัย 10 คน:

- **ประหยัดเงินได้เกือบ 1.6 ล้านดอลลาร์ต่อปีจากการรวมผู้จัดจำหน่าย** การลงทุนใน Microsoft SIEM และ XDR ช่วยให้การรวมกันนั้นสามารถลดต้นทุนของ SIEM ก่อนหน้าได้ ($560,000) โครงสร้างพื้นฐานภายในองค์กรที่เกี่ยวข้อง (มากกว่า $360,000) โซลูชัน XDR สามจุด ($192,000) และต้นทุนแรงงานต่อเนื่องเพื่อจัดการสิ่งเหล่านี้ ($480,000)
- **ลดความเสี่ยงของการผิดสัญญาอย่างร้ายแรงลง 60%** ด้วยการตรวจสอบความปลอดภัยและเวิร์กโฟลว์การตอบสนองที่มีประสิทธิภาพมากขึ้น การตอบสนองด้านความปลอดภัยอัตโนมัติที่ได้รับการปรับปรุง และความสามารถที่เพิ่มขึ้นในการปกป้องสภาพแวดล้อมการประมวลผลทั้งหมด รวมถึงการปกป้องมัลติคลาวด์ การผสานรวมนี้ช่วยลดความเสี่ยงของการละเมิดโดยส่งผลให้ประหยัดได้ถึง 1.6 ล้านดอลลาร์ต่อปี
- **สร้าง ROI ได้ถึง 207%** การสัมภาษณ์ตัวแทนและการวิเคราะห์ทางการเงินพบว่าองค์กรที่ผสานรวมได้รับประโยชน์ 17.68 ล้านดอลลาร์ในช่วงสามปี เทียบกับต้นทุน 5.76 ล้านดอลลาร์ รวมกันเป็นมูลค่าปัจจุบันสุทธิ (NPV) ที่ 11.92 ล้านดอลลาร์

เหตุผลข้อที่ 2

เพิ่มขีดความสามารถให้ SecOps เพื่อมุ่งเน้นไปที่งานที่มีมูลค่าสูง

ซึ่งจำเป็นต้องผสานรวม SIEM และ XDR ให้สัมพันธ์กับการแจ้งเตือน จัดลำดับความสำคัญของภัยคุกคามที่ใหญ่ที่สุด และร่วมมือกันดำเนินการทั่วทั้งองค์กร

ทีม SecOps จะพบกับกับจำนวนสัญญาณที่ต้องวิเคราะห์จำนวนมาก ซึ่งรวมถึงสัญญาณที่มีความเที่ยงตรงต่ำจำนวนมากที่ยากหรือเป็นไปไม่ได้ในการตรวจจับและบรรเทาด้วยตนเอง เมื่อภัยคุกคามเพิ่มขึ้น เป็นเรื่องยากสำหรับ SOC ที่มีภาระมากเกินไปในการตามให้ทัน โดยเฉพาะอย่างยิ่งเมื่อพยายามวิเคราะห์ข้อมูลจากโซลูชันหลายจุด การจัดสรรทรัพยากรเพิ่มเติมเพื่อเติมเต็มช่องว่างนั้นไม่ใช่คำตอบ เนื่องจากการหาผู้เชี่ยวชาญด้านการรักษาความปลอดภัยที่มีทักษะเพียงพอนั้นเป็นความท้าทายอย่างต่อเนื่อง

นั่นเป็นเหตุผลว่าทำไมการผสานรวม SIEM และ XDR เข้าด้วยกันจึงมีความสำคัญอย่างยิ่ง เพื่อเชื่อมโยงการแจ้งเตือน จัดลำดับความสำคัญของภัยคุกคามที่ใหญ่ที่สุด และประสานงานการดำเนินการทั่วทั้งองค์กรด้วย AI ขั้นสูงและระบบอัตโนมัติเพื่อตรวจจับและแก้ไขภัยคุกคามในเชิงรุก

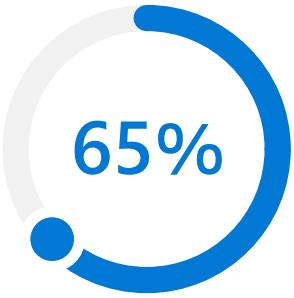
ตัวอย่างเช่น สัญญาณระดับต่ำเพียงสัญญาณเดียวอาจไม่ได้รับความสนใจจาก SIEM แบบเดิมมากนัก แต่การใช้ AI ทำให้ SIEM ที่ทำงานแบบคลาวด์เนทีฟสามารถเปรียบเทียบสัญญาณนั้นกับสัญญาณจากแหล่งอื่นทั่วทั้งองค์กรที่เชื่อมโยงกันระหว่างชุดข้อมูลหลายชุดได้โดยอัตโนมัติเพื่อค้นหาการโจมตีแบบหลายขั้นตอน

SIEM และ XDR ที่ผสานรวมช่วยเพิ่มทรัพยากรของ SecOps ในขณะเดียวกันก็เพิ่มขีดความสามารถให้กับนักวิเคราะห์มือใหม่ด้วยความสามารถและความมั่นใจที่มีมากขึ้น

ระบบจะทำให้ข้อมูลเป็นปกติ วิเคราะห์ และเชื่อมโยงข้อมูล พร้อมกับระบุบริบทเกี่ยวกับวิธีการที่การโจมตีทางไซเบอร์เข้าสู่โครงสร้างพื้นฐาน พร้อมกับไทม์ไลน์ของการแพร่กระจาย ซึ่งช่วยให้ทีม SOC เห็นภาพการละเมิดจากคอนโซลเดียว และจัดการได้อย่างมีประสิทธิภาพ

> CISO จำนวนมากไม่ได้ตระหนักถึง **ค่าใช้จ่ายที่พวกเขากำหนดให้กับทีมของตนด้วยบานกระจกที่แตกต่างกัน 20 แบบ** หรือโซลูชันเฉพาะจุด และค่าใช้จ่ายรายปีที่เกี่ยวข้อง... เราได้ขจัดความล้าสมัยของเครื่องมือจำนวนมากด้วยผู้จัดจำหน่ายเพียงรายเดียว”
>
> **Terence Jackson**
> Chief Information Security and Privacy Officer, Thycotic

องค์กรไม่ควรต้องการความเชี่ยวชาญเชิงลึกเพื่อปลดล็อกมูลค่าของโซลูชันการรักษาความปลอดภัย SIEM และ XDR ที่ผสานรวมช่วยเพิ่มทรัพยากรของ SecOps ในขณะเดียวกันก็เพิ่มขีดความสามารถให้กับนักวิเคราะห์มือใหม่ด้วยความสามารถและความมั่นใจที่มีมากขึ้น



วิธีการแบบผสานรวมของ Microsoft SIEM และ XDR ช่วยลดเวลาในการตรวจสอบภัยคุกคามได้ถึง 65%

การศึกษา Forrester Total Economic Impact™ (TEI) ที่จัดทำโดย Microsoft แสดงให้เห็นถึงประสิทธิภาพของ SecOps ในองค์กรแบบผสมผสาน:

- **ลดเวลาในการตรวจสอบภัยคุกคามได้ถึง 65% และลดเวลาในการตอบสนองต่อภัยคุกคามได้ถึง 88%** วิธีการแบบผสานรวมของ Microsoft SIEM และ XDR ในการตรวจสอบและตอบสนองต่อภัยคุกคามด้านความปลอดภัย ทำให้เวิร์กโฟลว์เหล่านี้มีประสิทธิภาพมากขึ้นสำหรับผู้เชี่ยวชาญด้านการรักษาความปลอดภัยขององค์กรแบบผสมผสาน ไม่จำเป็นต้องข้ามไปยังเครื่องมือหลายตัวเพื่อระบุภัยคุกคามอีกต่อไป จากการที่คุณสมบัติด้านการรักษาความปลอดภัยแบบอัตโนมัติช่วยปรับปรุงเวิร์กโฟลว์การตอบสนอง

- **ลดเวลาในการสร้างสมุดงานใหม่ได้ถึง 90% และเวลาในการเตรียมความพร้อมให้กับผู้เชี่ยวชาญด้านการรักษาความปลอดภัยคนใหม่ได้ถึง 91%** วิธีการแบบผสานรวมของ Microsoft SIEM และ XDR ทำให้เวิร์กโฟลว์ของผู้เชี่ยวชาญด้านการรักษาความปลอดภัยอื่นๆ มีประสิทธิภาพมากขึ้นเช่นกัน เนื่องจากบันทึก SIEM ได้รับการผสานรวมไว้ทั่วทั้งชุดโซลูชัน การสร้างสมุดงานจึงเกือบจะเป็นไปโดยอัตโนมัติ ในขณะที่การเข้าสู่ระบบแบบครั้งเดียวช่วยให้ผู้เชี่ยวชาญด้านการรักษาความปลอดภัยคนใหม่เริ่มงานได้เร็วขึ้นเกือบ 16 สัปดาห์

เหตุผลข้อที่ 3

เพิ่มประสิทธิภาพการทำงานของพนักงาน

โซลูชัน SIEM และ XDR แบบผสานรวมสามารถช่วยให้องค์กรของคุณปรับปรุงประสิทธิภาพการทำงานสำหรับผู้ใช้ปลายทางได้

นอกเหนือจากการทำสิ่งต่างๆ ได้มากขึ้นด้วยต้นทุนที่ต่ำลงและเพิ่มประสิทธิภาพ SecOps แล้ว โซลูชัน SIEM และ XDR แบบผสานรวมสามารถช่วยองค์กรของคุณในการปรับปรุงประสิทธิภาพการทำงานสำหรับผู้ใช้ปลายทางได้ด้วย

อย่างที่ทีม SecOps ทราบดี เมื่อคุณทำให้การรักษาความปลอดภัยเป็นเรื่องยาก ผู้คนจะต้องใช้เวลากับมัน ดังนั้น เมื่อประสบการณ์ของผู้ใช้ปลายทางเป็นอุปสรรค แทนที่จะช่วยประสิทธิภาพการทำงานของพนักงาน นั่นอาจทำให้องค์กรเปิดรับความเสี่ยงด้านความปลอดภัยและค่าใช้จ่ายที่สูงขึ้น รหัสผ่านที่ไม่รัดกุมหรือสูญหาย การเข้าถึงที่ไม่ปลอดภัยผ่านอุปกรณ์ส่วนตัว หรือการแชร์ข้อมูลที่ละเอียดอ่อนอย่างไม่จำกัดเป็นเพียงส่วนหนึ่งของความท้าทาย

> [ในอดีต] เราจะใช้เครื่องมือที่ไม่มีประสิธิภาพเมื่อมีคนสงสัยว่าจะมีปัญหา เราจะปิดการทำงานและปิดการเข้าถึง ซึ่งส่งผลเสียต่อธุรกิจของเรา ซึ่งก็ก็ชัดเจนมากสำหรับทุกคน เพราะสิ่งต่างๆ จะหยุดทำงานชั่วคราว ใน Microsoft Sentinel เรามีเครื่องมือที่ทันสมัยซึ่งเราสามารถตอบสนองต่อสิ่งที่เกิดขึ้นได้ **ธุรกิจมักจะไม่รู้ด้วยซ้ำว่าเรากำลังตอบสนองต่อภัยคุกคาม** และนั่นคือตัวชี้วัดความสำเร็จที่สำคัญของเรา”
>
> **Rick Gehringer**
> Chief Information Officer, Wedgewood

เกือบ
68,000
Microsoft SIEM และ XDR ปรับปรุงประสิทธิภาพการทำงานของพนักงานคนอื่นๆ เกือบ 68,000 ชั่วโมงต่อปี

วิธีการ SIEM และ XDR แบบผสานรวมช่วยให้คุณมอบประสบการณ์การใช้งานที่ราบรื่น ซึ่งช่วยให้พนักงานของคุณมีประสิทธิการทำงานและมีความปลอดภัยในทุกแง่มุมของประสบการณ์ประจำวัน สามารถลดผลกเสียต่อประสิทธิภาพการทำงาน เช่น ต้องปิดบริการหรือแยกเครื่องแล้วสร้างอิมเมจใหม่ แถม SIEM และ XDR แบบผสานรวมเข้ายังสามารถสร้างโอกาสใหม่สำหรับการเพิ่มประสิทธิการทำงานของผู้ใช้ปลายทาง เช่น การสนับสนุนความปลอดภัยแบบบริการตนเองมากขึ้น แดชบอร์ดและการรายงานที่ดีขึ้น และการตอบสนองที่มากขึ้นและเวลาบูตที่เร็วขึ้นจากการเรียกใช้เอเจนต์ความปลอดภัยที่น้อยลง

ในการศึกษา Forrester Total Economic Impact™ (TEI) ที่มอบหมายโดย Microsoft องค์กรสมมติที่มีพนักงานทั้งหมด 8,000 คน แสดงให้เห็นถึงประสิทธิภาพการทำงานของพนักงานที่เพิ่มขึ้นโดยการปรับใช้ Microsoft SIEM และ XDR:

- **การรับปรุงประสิทธิภาพการทำงานของพนักงานคนอื่นๆ เกือบ 68,000 ชั่วโมงต่อปี** Microsoft SIEM และ XDR ป้องกันผลเสียต่อพนักงานคนอื่นๆ จากกระบวนการรักษาความปลอดภัยที่ไม่มีประสิทธิภาพ ตัวอย่างเช่น การผสมผสานนี้ช่วยประหยัดเวลาได้ 4,000 ชั่วโมงต่อปี เนื่องจากความสามารถใหม่ของผู้เชี่ยวชาญด้านไอทีในการให้บริการด้วยตนเองเกี่ยวกับการอัปเดตและคำแนะนำด้านความปลอดภัย อีกทั้งยังช่วยให้สามารถแก้ไขปัญหาด้านความปลอดภัยจากระยะไกลบนเครื่องของพนักงาน และลดจำนวนเอเจนต์ความปลอดภัยที่ทำงานบนเครื่อง ซึ่งช่วยประหยัดเวลาได้เกือบ 64,000 ชั่วโมงต่อปีในด้านประสิทธิภาพการทำงานของผู้ใช้ปลายทาง

การรักษาความปลอดภัยได้กลายเป็นปัจจัยสำคัญสำหรับความสำเร็จทางเทคโนโลยี นั่นเป็นเหตุผลที่องค์กรต้องการมาตรการรักษาความปลอดภัยที่สร้างความยืดหยุ่นมากที่สุดเท่าที่จะเป็นไปได้จากการโจมตีที่ทันสมัย เพื่อปกป้องและสร้างประสิทธิภาพการทำงานและนวัตกรรมที่ขับเคลื่อนการเติบโต

รับการป้องกันภัยคุกคามทางไซเบอร์แบบผสานรวมด้วย SIEM และ XDR

การผสานรวมผลิตภัณฑ์ชั้นนำของอุตสาหกรรมนี้ให้การป้องกัน การตรวจจับ และการตอบสนองภัยคุกคามทางไซเบอร์ในโซลูชันเดียวที่ครอบคลุม

Microsoft นำเสนอโซลูชัน SIEM และ XDR แบบผสานรวมเป็นรายแรกและรายเดียว ซึ่งให้การมองเห็นแบบครบวงจรทั่วทั้งระบบคลาวด์และแพลตฟอร์มทั้งหมด การผสานรวมผลิตภัณฑ์ชั้นนำของอุตสาหกรรมนี้ให้การป้องกัน การตรวจจับ และการตอบสนองภัยคุกคามทางไซเบอร์ในโซลูชันเดียวที่ครอบคลุม

Microsoft SIEM และ XDR ใช้ประโยชน์จากพลังของ AI และระบบอัตโนมัติ รวมถึงการลงทุนเชิงลึกอย่างต่อเนื่องในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ ด้วยข้อมูลเชิงลึกจากผู้เชี่ยวชาญและการมองเห็นสัญญาณ 43 ล้านล้านรายการทุกวัน ด้วยการผสานรวมระหว่างผลิตภัณฑ์เหล่านี้ ทีม SOC จึงมีบริบทมากขึ้นกว่าที่เคยในการตามหาและแก้ไขภัยคุกคามทางไซเบอร์ที่สำคัญได้รวดเร็วขึ้น:

Microsoft Sentinel

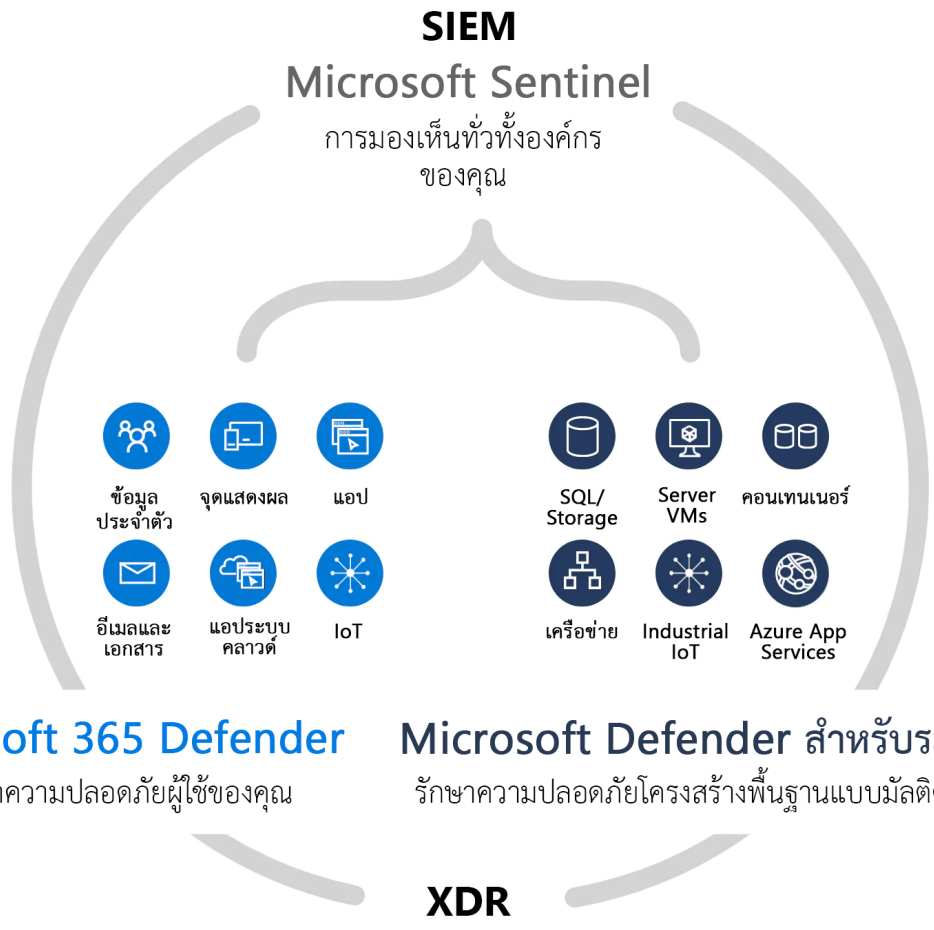
รับมุมมองจากมุมสูงทั่วทั้งองค์กรด้วย SIEM แบบคลาวด์เนทีฟของ Microsoft รวบรวมข้อมูลความปลอดภัยจากแหล่งที่มาทั้งหมดและใช้ AI เพื่อแยกสัญญาณรบกวนจากเหตุการณ์ที่เป็นจริง เชื่อมโยงการแจ้งเตือนข้ามห่วงโซ่การโจมตีทางไซเบอร์ที่ซับซ้อน และเพิ่มความเร็วในการตอบสนองต่อภัยคุกคามทางไซเบอร์ด้วยระบบการจัดการและระบบอัตโนมัติในตัว

Microsoft Defender XDR

ป้องกันและตรวจจับการโจมตีทางไซเบอร์ทั่วทั้งข้อมูลประจำตัว อุปกรณ์ปลายทาง แอป อีเมล ข้อมูล และแอปบนระบบคลาวด์ด้วยความสามารถของ XDR ตรวจสอบและตอบสนองต่อการโจมตีทางไซเบอร์ด้วยการป้องกันที่พร้อมใช้งานที่ดีที่สุดในรุ่น ค้นหาภัยคุกคามและประสานงานการตอบสนองได้อย่างง่ายดายจากแดชบอร์ดเดียว

Microsoft Defender สำหรับระบบคลาวด์

ปกป้องเวิร์กโหลดมัลติคลาวด์และไฮบริดคลาวด์ของคุณด้วยความสามารถของ XDR ในตัว รักษาความปลอดภัยเซิร์ฟเวอร์ ที่เก็บข้อมูล ฐานข้อมูล คอนเทนเนอร์ และอื่นๆ มุ่งเน้นไปที่สิ่งที่สำคัญที่สุดด้วยการแจ้งเตือนที่จัดลำดับความสำคัญ



อย่าเพิ่มการรักษาความปลอดภัยแต่จงสร้างขึ้นภายใน

นำเครื่องมือที่เหมาะสมและข้อมูลข่าวกรองไว้ในมือของคนที่เหมาะสม ป้องกันการโจมตีที่ทันสมัยด้วยโซลูชันคลาวด์เนทีฟแบบบูรณาการที่ครบวงจรแบบ

เรียนรู้เพิ่มเติมเกี่ยวกับการป้องกันภัยคุกคามทางไซเบอร์แบบผสานรวมด้วยโซลูชัน SIEM และ XDR ของ Microsoft >

Microsoft Security

© 2024 Microsoft Corporation สงวนสิทธิ์ทุกประการ เอกสารนี้มีให้ “ตามสภาพที่เป็น” ข้อมูลและมุมมองที่แสดงในเอกสารนี้ รวมถึง URL และการอ้างอิงเว็บไซต์ทางอินเทอร์เน็ตอื่น ๆ อาจเปลี่ยนแปลงได้โดยไม่ต้องแจ้งให้ทราบล่วงหน้า คุณคือผู้รับผิดชอบความเสี่ยงในการใช้เอกสารนี้ เอกสารนี้ไม่ได้ให้สิทธิทางกฎหมายใดๆ แก่คุณเกี่ยวกับทรัพย์สินทางปัญญาสำหรับผลิตภัณฑ์ของ Microsoft คุณสามารถทำสำเนาและใช้เอกสารนี้เพื่อการอ้างอิงภายในองค์กรของคุณเท่านั้น