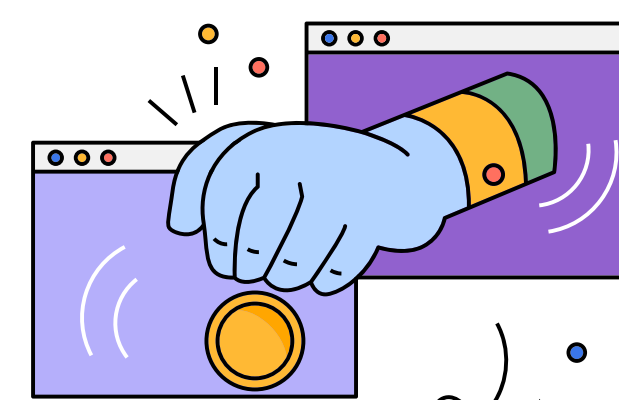


Industrial IoT

เทคโนโลยีที่มาพร้อมกับ



ภัยคุกคามทางไซเบอร์



IIoT เป็นหนึ่งในเทคโนโลยีที่เป็นรากฐานสำคัญของการปฏิวัติอุตสาหกรรมและการพัฒนาโรงงานอัจฉริยะ ช่วยเพิ่มประสิทธิภาพการผลิต ลดต้นทุนในระยะยาว และตอบสนองตลาดได้อย่างแม่นยำ แม้ว่า IIoT จะมอบประโยชน์มหาศาล แต่ทุกวินาทีที่ IIoT ทำงานก็ทำให้องค์กรเผชิญกับภัยคุกคามทางไซเบอร์ที่กระทบต่อความอยู่รอดของธุรกิจและสามารถสร้างวิกฤตการณ์ครั้งใหญ่กว่าที่เคยมีมา

ภัยคุกคาม

ทางไซเบอร์ใน IIoT



มัลแวร์

การแทรกแซง ควบคุม หยุดการทำงานของ IIoT หรือทำลายข้อมูล และนำไปเรียกค่าไถ่

การโจมตีแบบ MitM

การดักฟัง ดักจับ และแก้ไขข้อมูลที่ส่งระหว่าง IIoT เพื่อขโมยหรือปลอมแปลงข้อมูล สร้างความผิดพลาดในกระบวนการผลิต

การโจมตีแบบ DDoS

การรับส่งข้อมูลปริมาณมหาศาล เพื่อทำให้เครือข่ายล่ม ล่าช้า หรือใช้งานไม่ได้

การแสวงหาประโยชน์จากช่องโหว่ซอฟต์แวร์

การโจมตีช่องโหว่จากรหัสผ่าน ซอฟต์แวร์และเฟิร์มแวร์ ที่ไม่มีการอัปเดต

การโจมตีผ่านห่วงโซ่อุปทาน

การแทรกแซงผู้ให้บริการ หรือผู้จัดจำหน่าย IIoT ที่องค์กรไว้วางใจ

**ประเมินความเสี่ยง
และจัดลำดับความสำคัญ**
ของข้อมูลและกระบวนการ
ในการผลิต

สร้างความปลอดภัยพื้นฐาน

เปลี่ยนรหัสผ่าน สำรองข้อมูล
อัปเดตซอฟต์แวร์
และเฟิร์มแวร์เป็นประจำ

**แบ่งแยกเครือข่าย
อย่างเหมาะสม**

แบ่งระบบ OT ออกจาก IT
ปกติ และสร้างเครือข่ายแยก
สำหรับ IIoT ที่มีความสำคัญ

**เลือกพันธมิตร
ทางเทคโนโลยีที่น่าเชื่อถือ**

ตรวจสอบนโยบาย
การอัปเดตความปลอดภัย
ของผู้ให้บริการ ระยะเวลา
ที่จะสนับสนุนผลิตภัณฑ์
และวิธีการจัดการ
กับช่องโหว่ที่พบ

**ใช้บริการ Security
as-a-Service**

เพื่อเข้าถึง
ความสามารถ
ด้านความปลอดภัย
ระดับองค์กร
โดยไม่ต้องลงทุนสูง

**วางแผน
ตอบสนองต่อเหตุการณ์
และความต่อเนื่องทางธุรกิจ**

กำหนดขั้นตอนดำเนินการ ผู้ที่ต้อง
ติดต่อ วิธีจำกัดความเสียหาย
และวิธีกู้คืน รวมถึงวิธีการรักษา
ฟังก์ชันธุรกิจที่สำคัญในกรณี
IIoT ไม่สามารถใช้งานได้

**สร้างวัฒนธรรม
ความปลอดภัย
และฝึกอบรมพนักงาน**

ปลูกฝังความตระหนัก
ด้านความปลอดภัยในวิธีการทำงาน
ของทุกคนในองค์กร

**ร่วมมือกับพันธมิตร
และสร้างเครือข่าย**

แบ่งปันข้อมูลเกี่ยวกับ
ภัยคุกคาม แนวทางปฏิบัติ
และบทเรียนที่ได้รับ

