โซลูชั่นความปลอดภัยไซเบอร์สำหรับองค์กร

ช่วยให้คุณมั่นใจได้ว่าไฟฟ้าจะจ่ายอย่างต่อเนื่องและธุรกิจของคุณสามารถดำเนินงานได้โดยไม่หยุดชะงัก

ระบบพลังงานแสงอาทิตย์ที่ไม่ปลอดภัย: ภัยคุกคามไซเบอร์เงียบๆ ต่อธุรกิจของคุณ

ระบบพลังงานแสงอาทิตย์มีวิวัฒนาการอย่างรวดเร็ว ในอดีต ระบบเหล่านี้มีหน้าที่ผลิตและตรวจสอบพลังงานแสงอาทิตย์เท่านั้น แต่ปัจจุบันระบบเหล่านี้กำลังพัฒนาไปสู่ระบบดิจิทัลที่ซับซ้อนบนคลาวด์ ซึ่งสามารถจัดการระบบแบตเตอรี่ เครื่องชาร์จรถยนต์ไฟฟ้า และอุปกรณ์เพิ่มประสิทธิภาพพลังงานได้

เพื่อบริหารจัดการพลังงานอย่างมีประสิทธิภาพยิ่งขึ้น จำเป็นอย่างยิ่งที่จะต้องรวมระบบโซล่าร์เซลล์เข้ากับเครือข่ายระบบการจัดการข้อมูล (IT) ขององค์กรอย่างใกล้ชิด อย่างไรก็ตาม ความกังวลอยู่ที่ระบบเครือข่ายไอทีนั้นดูแลทรัพย์สินที่สำคัญขององค์กร ซึ่งรวมถึงฐานข้อมูลที่สำคัญ ข้อมูลส่วนบุคคล และระบบควบคุมอุตสาหกรรม แนวโน้มนี้ทำให้ความเสี่ยงขององค์กรต่อการโจมตีทางไซเบอร์เพิ่มขึ้น แฮ็กเกอร์ที่เจาะระบบอินเวอร์เตอร์ที่ไม่ได้รับการรักษาความปลอดภัยหรืออุปกรณ์อื่นๆ หรือระบบตรวจสอบโซล่าร์เซลล์หรือระบบบริหารจัดการพลังงาน สามารถแทรกซึมเข้าสู่ระบบขององค์กรได้ หากไม่มีการป้องกันที่เหมาะสม การเจาะระบบจะแพร่กระจายไปยังส่วนอื่นๆ ของธุรกิจได้อย่างง่ายดาย การโจมตีเหล่านี้ทำให้เกิดความเสียหายอย่างมากต่อทรัพย์สินที่เชื่อมต่ออื่นๆ และทำให้ธุรกิจหยุดชะงัก การโจมตีเหล่านี้อาจส่งผลให้เกิดการรั่วไหลของข้อมูลที่สำคัญ, การฉ้อโกงทางการเงิน, การโจมตีด้วยค่าไถ่, หรือการทำลายฮาร์ดแวร์ทางกายภาพ นอกเหนือจากความเสียหายโดยตรงแล้ว การโจมตีเหล่านี้อาจนำไปสู่การละเมิดข้อกำหนดและส่งผลกระทบต่อท่าทีด้านความปลอดภัยไซเบอร์ขององค์กร

42,000

จำนวนระบบโซล่าร์เซลล์ที่ติดตั้งในบ้านและธุรกิจของเนเธอร์แลนด์ถูกรัฐบาลเนเธอร์แลนด์มองว่ามีความเสี่ยงต่อการควบคุมระยะไกล (กรกฎาคม 2022)

130,000

จำนวนระบบโซล่าร์เซลล์ของผู้ผลิตอินเวอร์เตอร์หลายรายที่ถูกรายงานว่ามีความเสี่ยงต่อการถูกโจมตีทางไซเบอร์ (สหรัฐอเมริกา, กรกฎาคม 2023)

$200 M

เป็นค่าเสียหายโดยประมาณที่ Target Corporation ได้รับหลังจากที่เครือข่ายผู้ให้บริการ HVAC ของบริษัทถูกแฮ็กในสหรัฐอเมริกาในปี ค.ศ. 2015

การลงทุนพลังงานแสงอาทิตย์ของคุณมีความเสี่ยงต่อการละเมิดกฎหมายด้านความปลอดภัยไซเบอร์หรือไม่?

ด้วยการเพิ่มขึ้นของระบบโซล่าร์เซลล์ที่เชื่อมต่อกับระบบไฟฟ้า (กริด) ทำให้มีความกังวลที่เพิ่มขึ้นในรัฐบาลและหน่วยงานกำกับดูแลเกี่ยวกับความเสี่ยงด้านความปลอดภัยไซเบอร์ที่อาจเกิดขึ้นกับระบบพลังงานกระจายตัว พลังงานที่ส่งออกไปยังระบบไฟฟ้า (กริด) จากหลายระบบโซล่าร์เซลล์ขณะนี้ถูกมองว่าเป็น “พลังงานที่เชื่อมต่อ” และหน่วยงานกำกับดูแลคาดหวังว่าระบบโซล่าร์เซลล์ที่เชื่อมต่อจะแบ่งปันความรับผิดชอบในการลดความเสี่ยงไซเบอร์ต่อระบบไฟฟ้า เพื่อแก้ไขความเสี่ยงที่เพิ่มขึ้นเหล่านี้และรับประกันความน่าเชื่อถือของระบบไฟฟ้าและความมั่นคงทางไซเบอร์ กำลังมีนโยบายการกำกับดูแล กฎหมาย PSTI ของสหราชอาณาจักรได้ถูกนำมาใช้ในสหราชอาณาจักรเมื่อวันที่ 29 เมษายน 2567 กฎหมายความยืดหยุ่นทางไซเบอร์ได้ผ่านในช่วงต้นปี 2567 และจะบังคับใช้ทางการในอีก 2-3 ปีข้างหน้าทั่วสหภาพยุโรป ในขณะที่กฎระเบียบเกี่ยวกับอุปกรณ์วิทยุ (Redio Equipment Directive หรือ RED) จะกลายเป็นข้อบังคับในสหภาพยุโรปในเดือนสิงหาคม 2568 คาดว่าภายในสองถึงสามปี บริษัทที่มีระบบโซล่าร์เซลล์จะต้องปฏิบัติตามมาตรฐานที่เข้มงวดอย่างเคร่งครัด ในบางกรณี ระบบที่ไม่สอดคล้องอาจต้องถูกเรียกคืนและเปลี่ยนใหม่ ภูมิทัศน์ที่เปลี่ยนแปลงนี้กำลังกดดันหน่วยงาน CISO, CIO, ไซเบอร์, IT และโครงสร้างพื้นฐาน สำหรับธุรกิจใดๆ ที่ลงทุนในระบบพลังงานแสงอาทิตย์ที่มีระยะเวลาคืนทุนหลายปี การพิสูจน์อนาคตของการปฏิบัติตามข้อกำหนดด้านกฎระเบียบของการลงทุนเป็นปัจจัยสำคัญที่ต้องพิจารณา

ระบบพลังงานแสงอาทิตย์ของคุณ - เป็นโครงสร้างพื้นฐานสำคัญที่เชื่อมต่อกับระบบไฟฟ้า จำเป็นต้องได้รับการป้องกันจากภัยคุกคามทางไซเบอร์

แนวทางแบบขั้นบันไดของ SolarEdge ในการรักษาความสมบูรณ์ของข้อมูล, การสื่อสาร, และการดำเนินงานทางธุรกิจ

การร่วมมือกับ SolarEdge หมายถึงคุณจะได้รับการปกป้องเพิ่มเติม วิธีการแบบแบ่งชั้นด้านความปลอดภัยไซเบอร์ของ SolarEdge มุ่งเน้นการปกป้องความสมบูรณ์ของข้อมูล การสื่อสาร และการดำเนินธุรกิจ ตั้งแต่ขั้นตอนการเปิดไซต์งานจนถึงการผลิต เพื่อรักษาการเชื่อมต่อของระบบ ฟังก์ชั่นการทำงาน และข้อมูลลูกค้า SolarEdge ปฏิบัติตามหลักการ Cyber Informed Engineering (CIE) โดยฝังกลไกความปลอดภัยข้อมูลเข้าไปในผลิตภัณฑ์ตั้งแต่ขั้นตอนการออกแบบเริ่มต้น เราปรับปรุงโซลูชั่นของเราอย่างต่อเนื่องเพื่อให้สอดคล้องกับความต้องการที่เปลี่ยนแปลงและมาตรฐานด้านกฎระเบียบ

แนวทางการรักษาความปลอดภัยทางไซเบอร์ของเราตั้งอยู่บนหลักสี่เสา:

ความปลอดภัยของอุปกรณ์

การรักษาความปลอดภัยของอุปกรณ์จากการเข้าถึงโดยไม่ได้รับอนุญาตมีความสำคัญอย่างยิ่งต่อการรับประกันการทำงานที่ราบรื่นและการดำเนินงานอย่างต่อเนื่องของระบบโซล่าร์เซลล์ของคุณ สิ่งนี้ทำได้โดยการรวมมาตรการความปลอดภัยหลายอย่างที่ปรับให้เหมาะกับความต้องการด้านความปลอดภัยของแต่ละระบบโซล่าร์เซลล์และส่วนประกอบของระบบ SolarEdge ใช้รหัสผ่านอุปกรณ์ที่ไม่ซ้ำกันและจำกัดการเข้าถึงระยะไกลเฉพาะผู้ใช้ที่ได้รับอนุญาตไว้ล่วงหน้า การเข้าถึงระยะไกลนั้นขึ้นอยู่กับบทบาทและได้รับอนุญาตให้แก่ผู้ใช้เฉพาะรายเป็นระยะเวลาจำกัดหลังจากเสร็จสิ้นการตรวจสอบสิทธิ์แบบหลายปัจจัย (Malti-factor Authentication หรือ MFA) มาตรการความปลอดภัยของอุปกรณ์เพิ่มเติมรวมถึงการตรวจจับและป้องกันความผิดปกติในขณะทำงานโดยตัวแทนความปลอดภัยที่ฝังอยู่, การป้องกันการสแกน Wi-Fi แบบสุ่ม, การวิเคราะห์โค้ดแบบคงที่, และการทดสอบการเจาะระบบโดยบุคคลที่สาม อินเวอร์เตอร์ SolarEdge ทั้งหมดจะได้รับการอัปเดตความปลอดภัยแบบไร้สายเมื่อมีการร้องขอเพื่อให้ลูกค้าสามารถเข้าถึงซอฟต์แวร์และเฟิร์มแวร์ที่ลงนามอย่างปลอดภัย ลูกค้ายังสามารถรับไฟล์โดยตรงและอัปเกรดผ่าน USB ได้

ความปลอดภัยของข้อมูล

เพื่อปกป้องข้อมูลที่สร้างขึ้นโดยระบบโซล่าร์เซลล์ของคุณ เราดำเนินการมากกว่าการรักษาความปลอดภัยของอุปกรณ์ทางกายภาพ อินเวอร์เตอร์ SolarEdge ที่เชื่อมต่อจะไม่เก็บข้อมูลที่ละเอียดอ่อนใดๆ ในตัว และสามารถรีเซ็ตกลับไปเป็นการตั้งค่าจากโรงงานได้อย่างสมบูรณ์ ลบข้อมูลการกำหนดค่าทั้งหมด SolarEdge เก็บข้อมูลที่สร้างขึ้นโดยระบบในสถานที่ที่ศูนย์ข้อมูลของ SolarEdge ดำเนินการในประเทศเยอรมนี เราใช้การสำรองข้อมูลที่ครอบคลุมเพื่อปกป้องข้อมูลของลูกค้าและเก็บข้อมูลด้วยความซ้ำซ้อนหลายระดับ การเข้ารหัสและการตรวจสอบสิทธิ์ที่ดีที่สุดมีอยู่สำหรับระบบที่จะเข้าถึงเซิร์ฟเวอร์ SolarEdge ปฏิบัติตามข้อกำหนดของ GDPR อย่างครบถ้วน

ความปลอดภัยของเครือข่าย

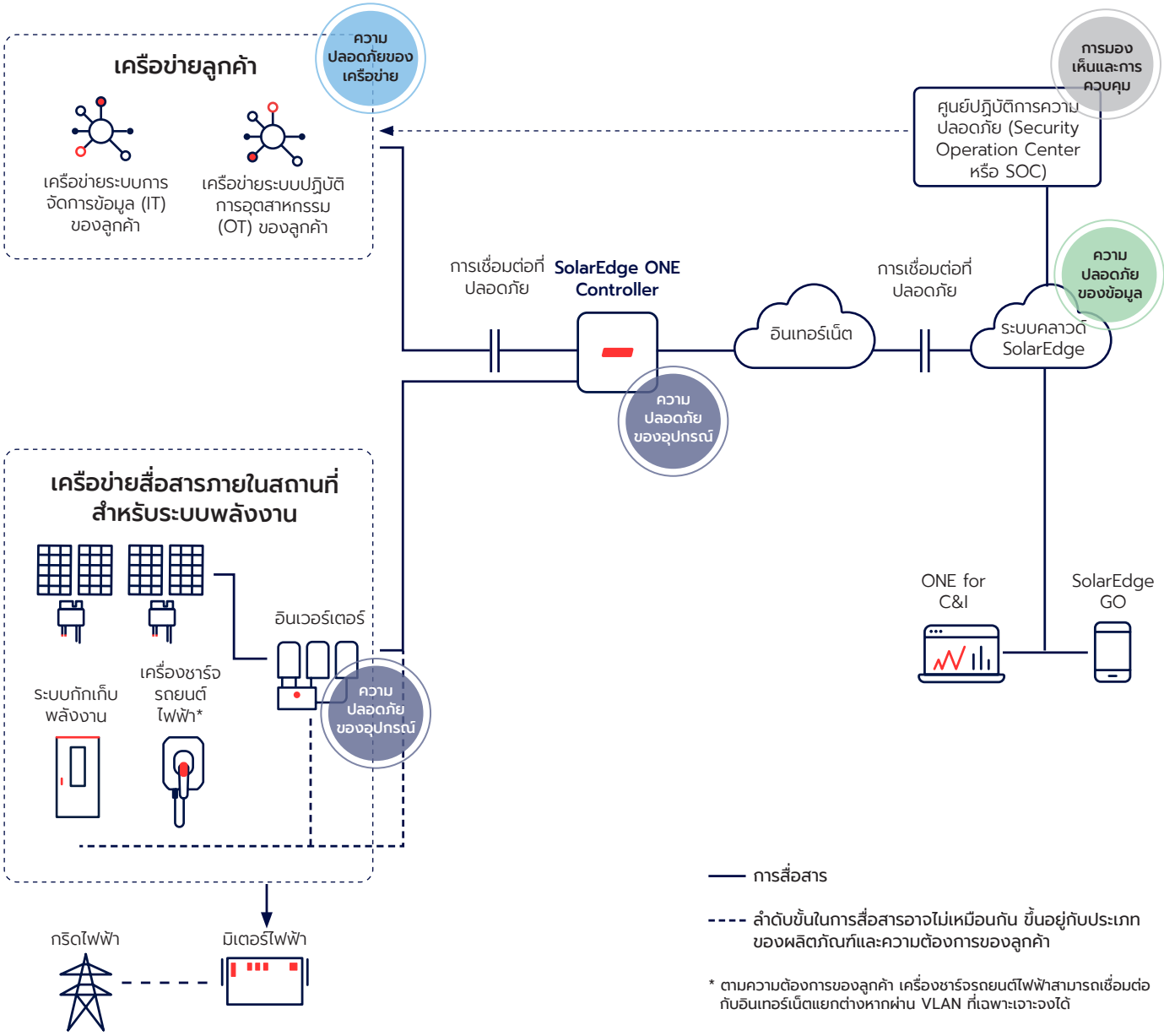
ระบบโซล่าร์เซลล์ขั้นพื้นฐานใดๆ ต้องการการเชื่อมต่ออินเทอร์เน็ตเพื่อให้การตรวจสอบประสิทธิภาพ ความเสี่ยงด้านความปลอดภัยทางไซเบอร์นี้จะเพิ่มขึ้นอย่างรุนแรงเมื่อระบบเพิ่มประสิทธิภาพพลังงานขั้นสูงถูกรวมเข้ากับเครือข่ายระบบการจัดการข้อมูล (IT) ขององค์กร ผู้โจมตีที่เข้าถึงระบบโซล่าร์เซลล์อาจสามารถแทรกซึมเข้าสู่เครือข่ายระบบการจัดการข้อมูล (IT) ขององค์กรได้ เพื่อปกป้องทั้งระบบโซล่าร์เซลล์และเครือข่ายระบบการจัดการข้อมูล (IT) ขององค์กร SolarEdge จำกัดการเข้าถึงระบบโซล่าร์เซลล์ผ่านจุดเข้าเพียงจุดเดียวผ่านทาง SolarEdge Local Controller หรือผ่านทางอินเวอร์เตอร์ SolarEdge ในการติดตั้งขนาดเล็ก การสื่อสารทั้งหมดที่ผ่านทางเกตเวย์จะถูกตรวจสอบและวิเคราะห์ และคุณสมบัติการปิดบังช่วยเพิ่มการป้องกันโดยทำให้ไม่สามารถเข้าถึงได้ แม้ว่าจะมีการพยายามแทรกซึมภายใน LAN เดียวกัน เพื่อบรรเทาความเสี่ยงเพิ่มเติม การสื่อสารของเกตเวย์กับเซิร์ฟเวอร์ของเราสามารถตั้งค่าได้ผ่านการเชื่อมต่อแบบเซลลูลาร์แยกต่างหากหรือ VLAN ที่ทุ่มเท อุปกรณ์ป้องกันการถ่ายโอนสามารถเพิ่มเพื่อให้การป้องกันวงจรทางกายภาพ

การมองเห็นและการควบคุม

นอกเหนือจากการตรวจสอบเชิงรุกอย่างต่อเนื่อง วิธีการรักษาความปลอดภัยของ SolarEdge ยังช่วยให้ทีมไอทีและความปลอดภัยของลูกค้าสามารถตรวจสอบทรัพย์สินพลังงานของตนได้แบบเรียลไทม์ การสื่อสารทั้งหมดระหว่างเกตเวย์และเซิร์ฟเวอร์ของ SolarEdge จะถูกเข้ารหัสและส่งผ่านทางพอร์ตเดียว (443) ซึ่งสามารถเพิ่มรายการที่อนุญาตโดยแผนกไอทีได้ หากต้องการการตรวจสอบและความสามารถในการปิดสวิตช์ของไอที ระบบสามารถตั้งค่าได้ภายใต้ VLAN ที่ทุ่มเท อุปกรณ์ SolarEdge ประกอบด้วยคุณสมบัติความปลอดภัยเพิ่มเติม ออกแบบมาเพื่อบล็อกการดำเนินการระยะไกลใดๆ บนอินเวอร์เตอร์ เว้นแต่จะได้รับการอนุญาตจากบุคลากรที่ได้รับอนุญาตซึ่งปรากฏตัวทางกายภาพที่อุปกรณ์ อุปกรณ์ SolarEdge ยังรวบรวมข้อมูลการบันทึกความปลอดภัยที่ครอบคลุมเกี่ยวกับความพยายามในการเข้าสู่ระบบที่ล้มเหลว การล่มของระบบ และประสิทธิภาพโดยทั่วไปของระบบ ข้อมูลที่วิเคราะห์ที่ Security Operation Center หรือ SOC (ศูนย์ปฏิบัติการความปลอดภัย) ของ SolarEdge สามารถทำให้ทีมไอทีของลูกค้าเข้าถึงได้

*เร็วๆ นี้

ความปลอดภัยทางไซเบอร์ของ SolarEdge ในการปฏิบัติจริง



ความปลอดภัยเป็นหัวใจสำคัญของธุรกิจของเรา

การควบคุมห่วงโซ่อุปทาน

- กระบวนการตรวจสอบผู้ขายสำหรับส่วนประกอบฮาร์ดแวร์ (Hardware Components หรือ HBOM)
- การพัฒนาซอฟต์แวร์แบบครบวงจรในสหภาพยุโรปและอิสราเอลทั้งสำหรับอินเวอร์เตอร์และ SolarEdge ONE Controller
- การวิเคราะห์ความปลอดภัยของโค้ดของบุคคลที่สาม
- การควบคุมไซต์การผลิตที่ปลอดภัย

ความสำคัญอันดับต้นๆ ขององค์กร

- การฝึกอบรมความตระหนักรู้ทางไซเบอร์
- การฝึกอบรมการเขียนโค้ดอย่างปลอดภัย
- โปรแกรมเปิดเผยช่องโหว่ (โบนัสสำหรับรายงานข้อบกพร่อง)

ความเชี่ยวชาญทางเทคนิค

- ผู้อำนวยการด้านเทคนิคสำหรับความปลอดภัยทางไซเบอร์ของผลิตภัณฑ์
- ทีมพัฒนาซอฟต์แวร์ (Secure Development Lifecycle หรือ SDL) ที่มุ่งเน้นความปลอดภัยแบบเฉพาะเจาะจง
- นักวิจัยด้านช่องโหว่และทีม "Red Team" ภายในองค์กร
- ทีมตอบสนองเหตุการณ์ (Incidence Response Team หรือ IRT)

ผู้นำด้านการปฏิบัติตามข้อกำหนดด้านความปลอดภัยทางไซเบอร์

SolarEdge เป็นผู้มีส่วนร่วมอย่างแข็งขันในคณะกรรมการเทคนิคต่างๆ ที่กำหนดมาตรฐานไซเบอร์ระหว่างประเทศ เราออกแบบโซลูชั่นของเราให้สอดคล้องกับกฎระเบียบเหล่านี้ในอนาคต อุปกรณ์ของเราเป็นไปตามมาตรฐานของคู่มืออ้างอิงและมาตรฐานล่าสุดเกี่ยวกับความปลอดภัยทางไซเบอร์ของ DER

มาตรฐานสำหรับการจัดการระบบความปลอดภัยข้อมูลขององค์กร		มาตรฐานและกฎระเบียบความปลอดภัยไซเบอร์สำหรับอุปกรณ์ IoT	
ISO 27001	ผ่านมาตรฐาน	ETSI 303-645	ผ่านมาตรฐาน
		กฎระเบียบเกี่ยวกับอุปกรณ์วิทยุ (Redio Equipment Directive หรือ RED)	ผ่านมาตรฐาน
		UK PSTI Act	เป็นไปตามมาตรฐาน

มาตรฐานและระเบียบข้อบังคับที่เกี่ยวข้องในอนาคต

UL 2941: มาตรฐานสากลสำหรับความปลอดภัยทางไซเบอร์ของอินเวอร์เตอร์อัจฉริยะและทรัพยากรพลังงานกระจาย (คาดการณ์การเผยแพร่อย่างเป็นทางการในปี ค.ศ. 2025)	Cyber Resilience Act หรือ กฎหมายความมั่นคงทางไซเบอร์: กฎหมายสหภาพยุโรปเกี่ยวกับความปลอดภัยทางไซเบอร์ของอุปกรณ์ IoT และอุปกรณ์ที่เชื่อมต่อ (มีผลบังคับใช้ตั้งแต่ปี ค.ศ. 2026-2027)
"U.S. Cyber Trust Mark" หรือ เครื่องหมายความน่าเชื่อถือทางไซเบอร์ของสหรัฐอเมริกา: โครงการรับรองและติดฉลากด้านความปลอดภัยทางไซเบอร์ (คาดว่าจะเปิดตัวอย่างเป็นทางการในปี ค.ศ. 2025)	NIS 2 (กฎหมายความปลอดภัยเครือข่ายและข้อมูล 2): กฎหมายระดับสหภาพยุโรปเพื่อยกระดับความปลอดภัยทางไซเบอร์ทั่วสหภาพยุโรป (มีผลบังคับใช้ตั้งแต่เดือนตุลาคม ค.ศ. 2024)

ต้องการเรียนรู้เพิ่มเติมเกี่ยวกับการรักษาความปลอดภัยทรัพย์สินด้านพลังงานของคุณ โปรดติดต่อเราที่ mailto:Security@SolarEdge.com

ติดตามเราได้ทาง LinkedIn และอย่าพลาดข่าวสารอัปเดต

พบปัญหา? เข้าสู่ หน้าความปลอดภัยไซเบอร์ของ SolarEdge

เกี่ยวกับ SolarEdge

SolarEdge Technologies เป็นผู้นำระดับโลกด้านเทคโนโลยีพลังงานหมุนเวียน นำวิศวกรรมชั้นนำและนวัตกรรมมาประยุกต์ใช้เพื่อมอบโซลูชั่นพลังงานแสงอาทิตย์แบบ PV สำหรับภาคที่อยู่อาศัย, เชิงพาณิชย์, และสาธารณูปโภค SolarEdge นำเสนอแนวทางที่เหมาะสมที่สุดในการผลิต กักเก็บ จัดการ และใช้พลังงาน บริษัทพัฒนาและผลิตอินเวอร์เตอร์พลังงานแสงอาทิตย์ (PV) และ Power Optimizer โซลูชั่นการจัดการและเพิ่มประสิทธิภาพพลังงาน ระบบกักเก็บพลังงาน และบริการด้านระบบจำหน่ายไฟฟ้า เทคโนโลยี DC-optimized ของ SolarEdge ถูกติดตั้งในบ้านเรือนหลายล้านหลังคาเรือนในกว่า 140 ประเทศ และบริษัทในกลุ่ม Fortune 100 มากกว่า 50% มีเทคโนโลยี SolarEdge อยู่บนหลังคา SolarEdge กำลังเร่งการเปลี่ยนผ่านไปสู่เครือข่ายพลังงานแบบกระจายที่ยั่งยืน ซึ่งจะช่วยเพิ่มประสิทธิภาพการใช้พลังงานทุกที่.

ข้อจำกัดความรับผิดชอบ

ข้อความข้างต้นอาจประกอบด้วยข้อความที่มีลักษณะคาดการณ์ล่วงหน้า ซึ่งอาจมีความไม่แน่นอน และไม่สามารถรับประกันผลลัพธ์ในอนาคตได้ ข้อความดังกล่าวอาจขึ้นอยู่กับสมมติฐาน การประมาณการ และการตัดสินใจที่ทำขึ้นโดยพิจารณาจากข้อมูลที่มีอยู่ SolarEdge ไม่รับประกันความถูกต้อง, ความครบถ้วน, หรือสถานะที่ได้รับการอัปเดตของข้อความดังกล่าว