Information Security Management - Partner Information Pack

Version History

- Version 1.0 – first issue

Contents

Executive Summary

In recent years, the world has witnessed an onslaught of cyber-attacks against IoT devices.

The current cybersecurity landscape requires manufacturers of smart IoT systems to enhance the effectiveness of their products' built-in protection mechanisms.

SolarEdge is committed to promoting cybersecurity across its entire line of smart inverters, its worldwide data & communication infrastructure, and data centers.

Our holistic security architecture protects the photovoltaic (PV) infrastructure's in-transit data and avoids the need for additional traffic protection schemes, such as a VPN.

SolarEdge regularly performs third-party cyber risk assessments and penetration testing to identify potential security breaches and improve cybersecurity readiness.

We diligently follow cybersecurity best practices across all our digital assets and aim to comply with all relevant industry regulations, such as ISO27001 and GDPR.

Disclaimer

Introduction

General

The purpose of this document is to introduce SolarEdge's current and potential customers and partners to the information security framework, mechanisms, and controls employed in SolarEdge software and hardware products.

SolarEdge's PV control and monitoring solution includes communications and information systems that provide customers with remote site-level, inverter-level and module-level monitoring. These systems are subject to threats that jeopardize the confidentiality, integrity and availability of the information stored, processed, or transmitted by the systems and its various components. SolarEdge has adopted an ongoing methodology to protect against these threats, which include intentional attacks, disruptions, environmental events, human/machine errors, and structural failures.

SolarEdge's system components and associated security measures are outlined in the diagram below.

Device Inverter	Uplink Telemetry Link	Downlink Inverter Control	SolarEdge Data Center	DC to DC Link (API)
• Software integrity check and FW manipulation protection • Zero day attack protection	• Traffic encrypted with AES128 (TLS1.2) • Each inverter has a unique encryption key • All communication initiated only by the inverter • Inverter communication settings are preconfigured to reach only SolarEdge domain	• All communication initiated only by the inverter • Inverter communication settings are preconfigured to reach only SolarEdge domain	• ISO 27001 certified • Best practices implementation • GDPR compliant	• SSL VPN • Layered API key (site/account keys, user authentication/capabilities) • Pull only by customer

Holistic, Multi-layer Security

SolarEdge has implemented a multi-layer solution that provides holistic protection against unauthorized attempts to access the SolarEdge system. The solution provides remote protection against scalable attacks and unauthorized access to a single unit. It is designed to protect each of the solution's components, connectivity, system functionality, and stored data.

Scope of Solution

The following security measures are reviewed:

- Endpoint security
- Communication between endpoints (inverters) and data centers
- Server security (hardware and software)
- Secure hosting facility
- Backup and business continuity plan (BCP)
- Organizational procedures and processes

Methodology

As part of its regular security reviews, SolarEdge engages with 3rd party cyber-security risk assessment and penetration testing companies to review SolarEdge's security mechanisms. Periodic assessments of SolarEdge's information security systems and communication systems that are based on the methodologies specified in the NIST 800-171 and OWASP international standards for information security are perfomed.

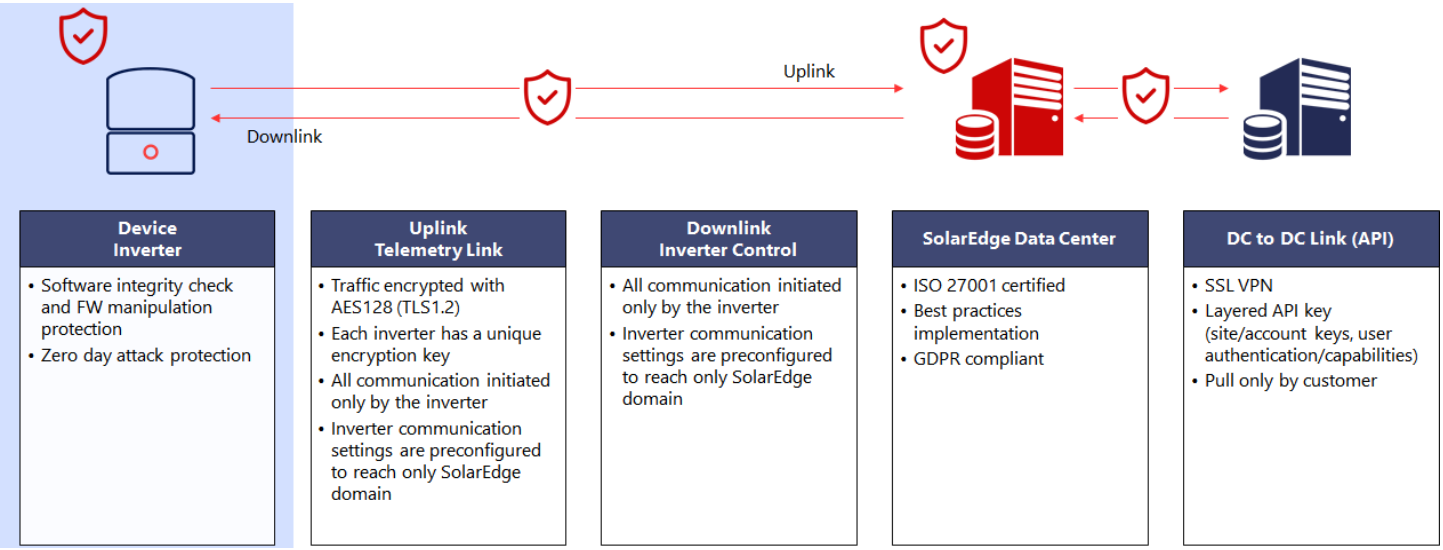
Summary

The following document is an abridgment of 3rd party reviews. This unbiased and thorough analysis reveals that no critical or major issues were found. SolarEdge was found to have established a comprehensive process for continuous security improvement. SolarEdge considers information security and customer privacy a vital part of its solution offering.

Security Policy

SolarEdge reserves the right to change its security policies at any time.

Endpoint (Smart Inverter) Security



SolarEdge inverters have multiple security layers – including both built-in and third-party mechanisms – that are designed to limit exposure to opportunistic and targeted cyber-attacks.

Device Access Control

- Access hardening - All unused interfaces (services/ports) of the inverter are disabled. Only specified, protected ports are open to communication, allowing access to pre-determined, secured services.
- Only approved user/service accounts exist. By default, we remove unnecessary accounts to limit the attack surface of unused and unsecured user/service accounts.
- Endpoints do not support the automatic discovery and connect capabilities provided by UPnP, thus preventing the establishment of unauthorized and unknown connections – they must be manually paired.
- Short-range wireless communication for a variety of devices is based on the ZigBee protocol and its security requirements (IEEE 802.15.4) – enforcing close proximity to an inverter to initiate access and establish a connection.
- The inverter acts as a Wi-Fi router to SolarEdge's peripheral devices. The inverter's Wi-Fi access point does not publish its SSID (source) and can only be turned on for a very short time by physically accessing the inverter. Casual Wi-Fi scanning will not reveal the inverter's access point.

Device Authentication Security

Authentication is the mechanism for verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

SolarEdge creates a unique encryption key for each inverter during production. As a result:

- Each inverter is designed to be uniquely authenticated by the control and monitoring server.
- The key exchange process limits exposure to encryption attack vectors.

Protection Against Malicious Code Exploitation

Malicious code is software or firmware code intended to perform unauthorized actions that will have an adverse impact on the safety, confidentiality, integrity, and availability of an information or operational system. Malicious code can appear in the form of a virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.

SolarEdge firmware is designed to protect against local and remote malicious code exploits, using the following mechanisms:

- Inverter firmware code is encrypted with a secret key intended to ensure that firmware updates are authentic and do not include backdoors or unapproved code.
- Security design is embedded in various stages of the secure development life cycle (SDLC) in order to protect against different kinds of code vulnerability.
- When performing remote, over the air (OTA) software upgrades, SolarEdge secures the transmission channel and provides firmware validation. The process is managed by our control and monitoring platform (management server) in order to ensure swift and uniform upgrades.
- In Q1 2020, SolarEdge partnered with Karamba Security to integrate advanced IoT anti-malware agents on its smart inverters, providing the following security enhancements:
  - The Karamba Security mechanism provides IoT protection against zero-day attacks (that target unknown security flaws in code) and real-time prevention capabilities.
  - An additional verification layer to check and permit legitimate code updates.
  - An advanced security layer called Control Flow Integrity (CFI). The inverter code is protected against hostile manipulation attempts in the production line and in the field.
  - The solution continuously monitors security events and alerts the SolarEdge security team (alert notifications are transmitted in near real-time to our security operation center).

Device Data Protection (Privacy)

- Our hardware is not capable of audio and video recording by design, nor does it store any personal information, such as names or addresses.

Inverter Baseline Configuration (Security by Design)

The baseline configurations used on our inverters and power optimizers are the basis for future builds, releases, or changes to device firmware and settings. Baseline configurations include the endpoint hardware build, factory-installed software, local or remote software upgrades, and parameters that control functionality. Endpoint configuration reflects the current field configuration.

SolarEdge inverters and power optimizers have a defined baseline configuration that is documented in each of the product engineering management systems. Changes are formally reviewed and updated as part of our design and manufacturing process.

Distributing and Applying Patches

A patch is a software update comprised of code inserted (or patched) into the code of an executable program. Typically, a patch is deployed into an existing software program. Patches may do any of the following:

- Fix a software bug / Address software stability issues
- Address new security vulnerabilities
- Upgrade the firmware

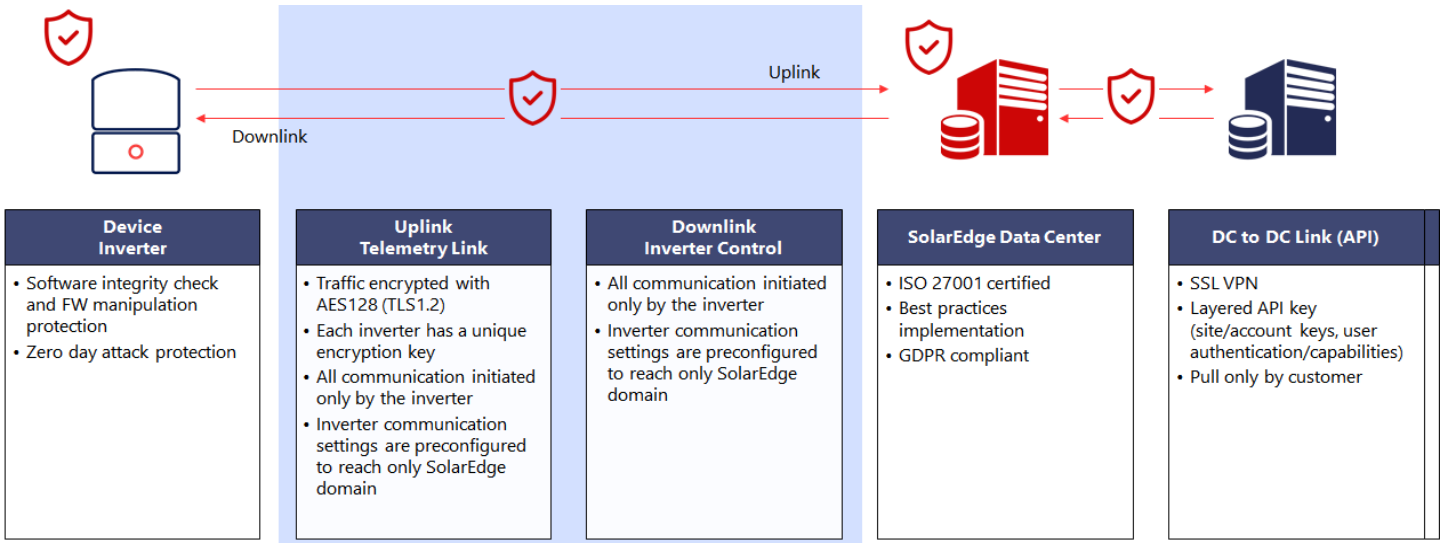
SolarEdge continuously monitors the cyber threats to its products and delivers security patches accordingly. The patches are controlled and regularly monitored.

Inverter Remote Support Activities

Technical support is required to address a variety of product failures, service disruptions or other issues. The technical support group is staffed with certified support engineers as well as accredited support partners.

Due to the operational and security sensitivity of support activities, each activity is logged, while access to cardinal support activities is limited and fully monitored.

Communication Security (Between Inverter and SolarEdge Servers)



Communication Encryption

Organizations employ encrypted communication links to enhance confidentiality and integrity. The use of encrypted communication links, however, affects an organization's ability to monitor communications traffic adequately for malicious code.

The SolarEdge control and monitoring solution enforces encryption of communications between the inverter and the server -- when using Ethernet, Wi-Fi or Cellular modem -- by employing the Advanced Encryption Standard 128-bit AES bits cipher.

SolarEdge's security approach assumes that the user of the equipment provides protection from an unauthorized person who may attempt to physically access the hardware or penetrate the LAN.

- Wi-Fi LAN and WAN communication are implemented with security-related best practices for strong authentication (802.1x) and encryption algorithms (WPA2-PSK with 128-bit AES keys).
- SolarEdge inverters communicate only in encrypted TCP mode (SSL over TCP).

Asymmetrical Communication

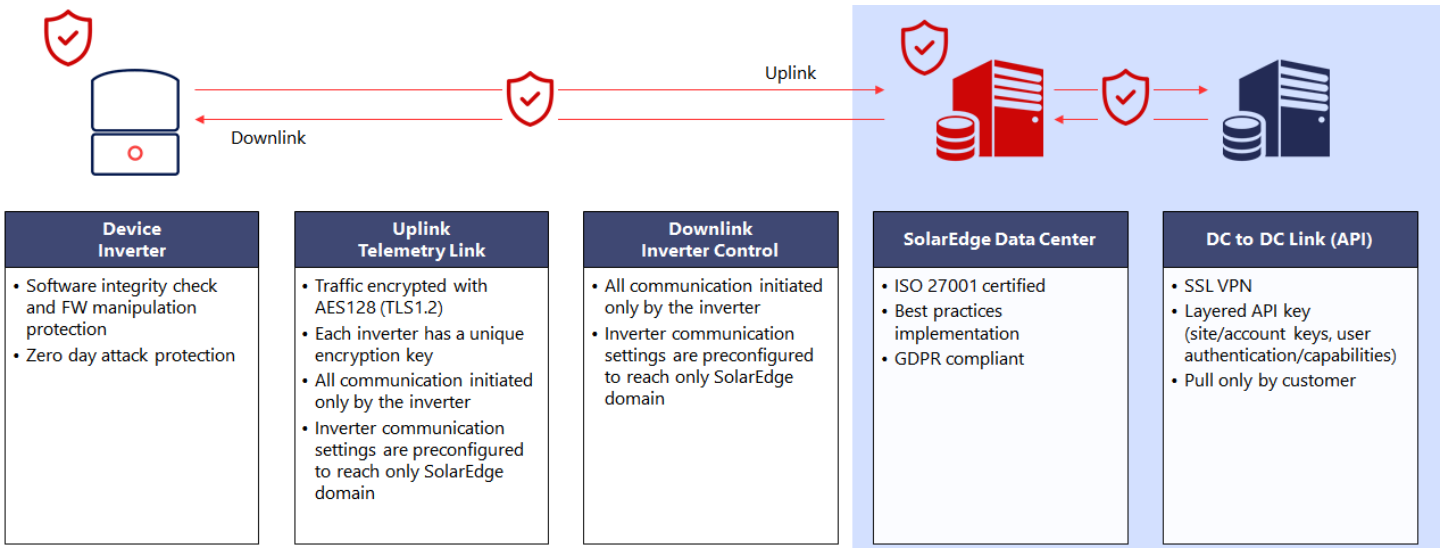
Enabling network or internet communication from inverters to datacenter servers can compromise the system.

Open receiving channels can be exploited by cyber threat actors that query the device to look for open ports and search for service vulnerabilities.

To mitigate this risk, SolarEdge inverters were designed with a one-way communication mechanism, in which inverters receive messages from the servers *only* when the inverter initiates contact with the servers, polling for new commands and transmitting new data.

The designed solution masks the inverters from potential hackers and effectively renders them invisible to scanning attacks.

SolarEdge Datacenter Security



The SolarEdge datacenter is the focal point for smart inverter data.

The web-based SolarEdge monitoring portal provides enhanced PV performance monitoring and yield assurance through immediate fault detection and propagation of alerts at the module, string, and system levels.

SolarEdge's control and monitoring platform does not process any credit card payments.

The measures used to secure SolarEdge datacenters are described in the following sections:

Server Hardening

Hardening is the process of implementing standard secure configurations to provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for specific information technology platforms/products, and instructions for configuring those information system components to meet operational requirements.

SolarEdge implements a thorough hardening process, based on vendor guidelines and best industry practices to improve the servers' security posture and operational performance.

Access to the servers for management purposes is enabled using a dedicated SSL VPN, which utilizes 3DES/SHA256 encryption algorithms and requires the use of 2-factor authentication.

Infrastructure Architecture

The SolarEdge datacenter employs a cluster of load balancers, firewalls, and servers. To ensure business continuity, we use cluster topologies that employ duplicate, redundant servers in order to meet capacity and enforce information security standards. Our firewalls and servers are deployed with leading anti-virus and malware applications. The center has a dedicated Internet access link with backup provided by multiple tier-1 providers.

Database Security

SolarEdge databases are maintained according to industry best practices. SolarEdge performs periodic database hardening according to international standards, such as NIST 800-123.

- Our databases are hosted in secure facilities that are managed according to ISO 27001 guidelines.
- From a network point of view, the databases are located in a separate network and protected by a firewall. Database traffic is open to specific applications only (segmentation).

- We impose periodic data backup and perform rollback tests in the event that a previous state must be restored.
- We implement logical separation of customer data by enforcing strict access control (each customer is exposed only to their data).

Traffic Flows

SolarEdge incorporates the following methods to secure traffic flow:

- Web browsing to the PV monitoring platform is encrypted using SSL with up-to-date encryption best practices (we deprecate vulnerable TLS versions).
- User and installer applications use SSL for all traffic to and from the server.
- A dedicated VPN supports secure communication between the different data centers. All traffic is encrypted.

Patching and Updating Servers

As mentioned, SolarEdge manages a comprehensive patching process. Due to their high operational sensitivity, SolarEdge updates its servers through a controlled process that includes:

- Deploying updates only after testing them in a controlled IT environment to identify any operational gaps or technical issues.

Server Monitoring

Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions.

SolarEdge has implemented and continuously adjusts its server monitoring strategy, using a variety of technological solutions and best practices:

- Establishment of organization-defined metrics to be monitored
- Based on the above, implementation of continuous performance monitoring using technological tools
- Ongoing security control assessments in accordance with the organization's monitoring strategy

Advanced Hosting Facility

SolarEdge stores its data and information in multiple dedicated hosting facilities in Europe, operated by a global hosting provider that operates more than 140 data centers across five continents.

The sites comply with the following standards:

- ISO 9001:2008 Quality Management Systems Standard - the world's leading quality management standard that provides a clearly structured and systematic approach to maintaining and improving customer experience.
- ISO / IEC 27001:2005 and 27001:2013 Information Security Management System Standard - the most widely accepted certification available for supporting information and physical security and business continuity. ISO 27001 ensures that:
  - Risks and threats to the business are assessed and managed.
  - Physical security processes such as restricted/named access are enforced consistently.
  - Audits are conducted regularly at each site, including tests of security and CCTV planning and monitoring.
- NIST 800-53/FISMA is published by the National Institute of Standards and Technology (NIST), which creates and promotes the standards used by federal agencies to implement the Federal Information Security Management Act (FISMA) and manage other programs designed to protect information and promote information security. Agencies are expected to meet NIST guidelines and standards within one year of publication. Homeland security issues are not included in these standards.

Backup and Business Continuity Plan (BCP)

Backup Cycle

Information backup is a mechanism employed by organizations to protect against loss of data, and it is a critical enabler of any business continuity plan (BCP).
SolarEdge implements a comprehensive backup cycle of the configuration and data of its systems. Backups can be used to enable a quick and full recovery in case of limited data loss or data center failures. The backup copies are located at multiple sites with multiple copies at each site.
A copy of the backup data is stored on AWS and in Israel, in addition to the copy in the European data center.
Every quarter, a backup test is executed to ensure full recovery in case of disaster.

Restoration Tests

To verify the full functionality of the backup process and to identify existing gaps and failures, periodic documented restoration tests are performed.

SolarEdge conducts these tests based on a predefined plan to fully verify the functionality of the backup process. In these tests, SolarEdge uses a sample of backed-up information in the restoration of selected information system functions.

Backup Protection (Onsite and Offsite)

SolarEdge enforces strict physical and environmental control over its onsite and offsite backup hosting sites to provide full assurance of its backups.

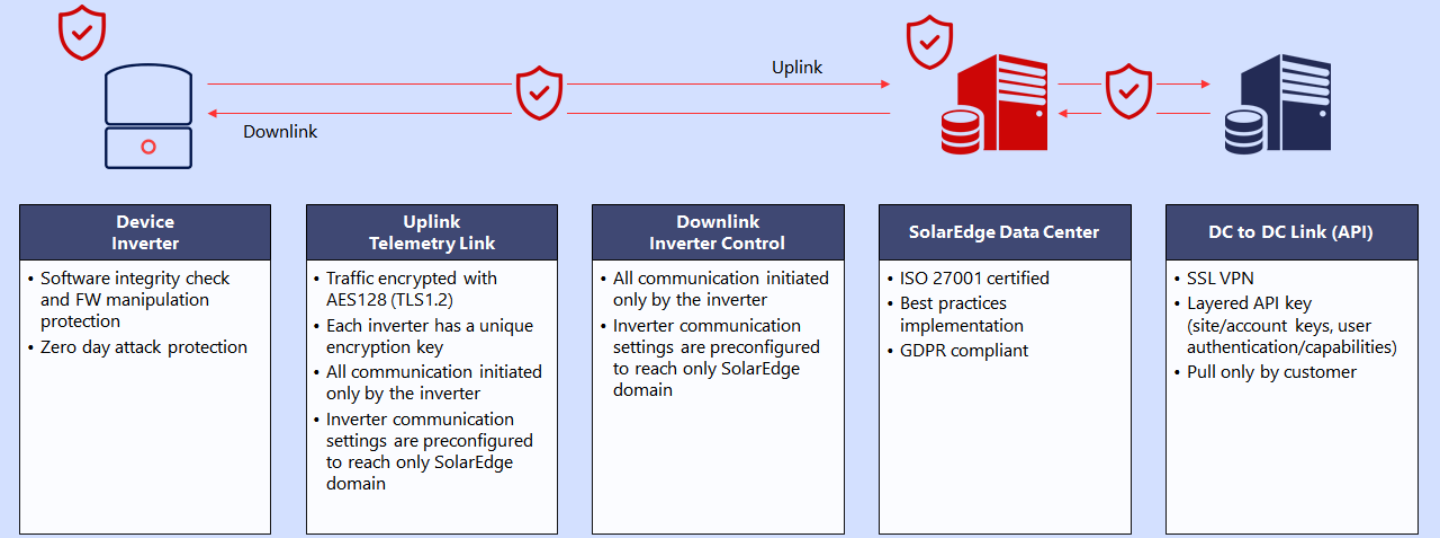
Alternate Site (Disaster Recovery Planning)

Business Continuity Planning (BCP) refers to the process of developing advance arrangements and procedures that enable an organization to respond to an interruption in such a manner that critical business functions continue within planned levels of interruption or essential change. In simpler terms, BCP is the act of proactively strategizing a method to prevent, if possible, and manage the consequences of a disaster, limiting the effects to the extent that a business can absorb the impact.

Disaster Recovery Planning (DRP), a key component of BCP, refers to the technological aspect of BCP – the advance planning and preparations necessary to minimize loss and ensure continuity of critical business functions in the event of a disaster.

Based on its commitment to customers, SolarEdge has a dedicated operational disaster recovery solution located in Europe.

Organizational Procedures and Processes



SolarEdge's internal security procedures and processes are aimed at ensuring that each component meets the same high standards, and that the entire end-to-end flow does not have a weak link.

User Account Management

Information system account types include individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service. Organizational information systems can implement some of the account management requirements listed above. Identification of authorized users of the information system and the specification of access privileges should reflect the requirements detailed in other organizational security procedures.

SolarEdge employs an automated business intelligence platform to support information system accounts management, including systems to monitor account usage to ensure acceptable use and prevent malicious activity.

User rights are reviewed regularly and adapted to each new functionality.

SDLC (Secure Development Lifecycle)

SolarEdge uses an array development methodologies for its hardware and software development processes. We practice secure software development procedures, including periodic vulnerability testing. Full automation tests on all permission-related code are performed as part of any minor or major release.

Privilege Allocation

Organizations employ "minimum privilege" to ensure that information system users and processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions, thus enhancing systems' security and information privacy.

Separation of Duties

Separation of duties addresses the potential for abuse of authorized privileges and reduces the risk of malicious activity without collusion.

SolarEdge implements separation of duties between mission and information system support functions, and among different individuals and/or roles.

Users and Privileges Validation

Solaredge implements periodic access reviews of user accounts and privileges that help ensure that authorized personnel have access to essential systems and that unauthorized employees (or miscreants) do not.

Managed SLAs with third parties

A service-level agreement (SLA) is a document describing the level of service expected by a customer from a supplier, laying out the metrics by which that service is measured, and the remedies or penalties, if any, should the agreed-upon levels not be achieved.

SolarEdge has signed contracts and defined SLAs with IT suppliers to ensure 24x7 response to equipment or infrastructure-related issues.

Bug Bounty

As a common practice, SolarEdge offers compensation to cyber experts who report cybersecurity vulnerabilities. The compensation offered is at the company's discretion, and is based upon risk, impact, ease of exploitation, quality of the report, and additional considerations.

Further details can be found at https://www.solaredge.com/cyber-security-policy

Logging

A log is a record of the events occurring within an organization's systems and networks.

SolarEdge incorporates a best-of-breed, time-based database system that indexes all monitoring platform infrastructure and networking logs into time-based indices, integrating a time-based dashboard that allows SolarEdge to search past and present logs, as well as to investigate past and present incidents.

Penetration Tests

Periodically, SolarEdge hires a third-party company to perform penetration tests for its monitoring platform, APIs, and mobile applications. The penetration tests are implemented using both manual and automatic tools, focusing on business logic to expose vulnerabilities that may cause the most severe business impact. Any findings are managed according to their criticality.

In addition, SolarEdge utilize an automatic web application scanning tool to detect vulnerabilities in its applications.

Incident Response

The SolarEdge security team employs advanced IR (incident response) tools to detect any suspected breach into its servers and generate alerts for immediate handling. Any potential breach is investigated and mitigated with those tools, in accordance with the best practices.

Supplier Relationships – Supply Chain Security

All SolarEdge suppliers undergo a legal review process before gaining access to the SolarEdge ERP system as approved vendors. The review applies risk parameters to potential vendors by establishing a minimum-security baseline before they are approved as a legitimate supplier.

GDPR – General Data Protection Regulation

SolarEdge provides global services, and maintains a significant presence in Europe.

SolarEdge does not store highly sensitive details, but still treats all data with the utmost care and complies with privacy regulations such as GDPR.

SolarEdge fully complies with GDPR requirements, including:

- Lawful, fair, and transparent processing
- Limitation of purpose, data, and storage
- Data subject rights
- Consent
- Personal data breaches
- Privacy by design - technical controls
- Data Protection Impact Assessment
- Data Protection Officer
- Awareness and training

Appendix A
Qualys SSLabs Report

To generate and view the report, visit the site:
https://www.ssllabs.com/ssltest/analyze.html?d=monitoring.solaredge.com