GRID EDGE SUITE

# Cyber security for DEOP

DEOP (Distributed Energy Optimization) is a cloud-based software which enables transparency, optimization and monetization of Distributed Energy Resources (DER).

www.siemens.com/DEOP

SIEMENS

GRID EDGE SUITE

# Cybersecurity for DEOP

DEOP (Distributed Energy Optimization) is a cloud-based software which enables transparency, optimization and monetization of Distributed Energy Resources (DER).

**1. Cybersecurity**

Cybersecurity in critical infrastructure operations is a highly sensitive area that demands a trustworthy partner: a technology partner who understands how products, systems, and solutions integrate with the processes and people behind them and the interactions involved. Siemens' Digital Grid products, solutions and services are based on a solid foundation: expertise in and knowledge of energy automation, customer needs and processes as well as cybersecurity in compliance with international standards.

**2. Optimizing the Energy in an IoT-Infrastructure with DEOP**

With the increasing decentralization of energy resources and applications, the management and optimization of Energy utilization and production is built on IoT-infrastructures that provides the data which enables efficient business operations and value generation. The data acquisition platform Siemens DEOP - Distributed Energy Optimization -running in the cloud is the foundation to utilize the full potential of IoT and real-time analysis to optimize the value of assets connected. It supports application like performance monitoring of decentralized energy resources, optimization of micro grid infrastructures or supports decision making by providing forecast capabilities that supports KPIs like CO2 reduction. The Siemens DEOP application is running in an Amazon Web Service (AWS) cloud environment which can be operated by an energy operator or as a managed service by Siemens in order to provide services for energy monitoring, energy management and performance monitoring with an intuitive dashboard/cockpit user interface.

Siemens DEOP supports the integration of external energy systems using the MQTT protocol (http://mqtt.org/) with a MQTT Broker as information exchange platform for communication between Siemens DEOP and external energy systems like microgrids or decentralized energy resources.

### 3. Understanding Cybersecurity Regulations for Siemens DEOP

For operation of a cloud-based Siemens DEOP application to manage and optimize energy utilization and production, we are taking into consideration the regulations, standards, and guidelines applicable to digital service providers in the European Union.

This includes the EU Directive (EU) 2016/1148, also commonly known as the Network and Information Systems Directive (NIS-Directive) and EU Regulation (EU) 2018/151, which are focused on ensuring that digital service providers take appropriate security measures to protect their assets and to notify their respective national authorities about serious cybersecurity incidents. While the NIS-Directive is implemented in respective EU Member States by national law, the EU regulation is binding for all Member States. Important in the context of Siemens DEOP is the handling of personal data that is following the EU Regulation (EU) 2016/679, also commonly known as General Data Protection Regulation (GDPR).

As a technology provider in North America, Siemens understands NERC CIP standards, which are applicable to operators of bulk electrical systems in order to protect their critical infrastructure against cyber risks. However, Siemens DEOP doesn't fall under the scope of NERC CIP as Siemens DEOP doesn't count to the bulk electrical systems as defined by NERC CIP.

Nevertheless, Siemens is working according to international standards which also cover the requirements of NERC CIP-005 for Electronic Security Perimeter protection. This includes, too, requirements of ISO/IEC 27001, NISTIR 7628 Guidelines for Smart Grid Cybersecurity in order to provide a comprehensive coverage of cybersecurity controls relevant to cloud-based applications and managed service in the cloud.

Siemens, in its role as a technology partner, solutions and service provider is committed to address cybersecurity risks based on international security standards and best practices, and to help customers fulfil their regulatory requirements. Notwithstanding the above, Siemens points out that the Customer stays solely responsible for the conception, implementation, and maintenance of a holistic, state-of-the-art security concept to protect its enterprise, plants, systems, machines and network.

### 4. Security by Design in Siemens DEOP

Security by design is an essential part of the product lifecycle management process for the Siemens DEOP platform. Security and functional product features are developed are following the principles of a secure system architecture. Siemens DEOP development follows OWASP general coding practices. A fundamental building block for the secure system architecture is the quality and security automation pipeline, including dependency checks, container scanning, license scanning, and command

injection and DAST analysis for cross-site scripting. Many other supported security controls like a secure zoning concept, access control, account management, hardening and security logging following security by design principles. The principles apply to all solution components like network-devices, software applications, services, and processes. A defense in depths approach is used for the security controls that complement each other like a dedicated firewall or hardening measures.

All access to the Siemens DEOP platform undergoes a state-of-the-art, strong authentication mechanism, including certificate- and token-based authentication. The user's authorization is periodically revalidated to verify that privileges have not been altered. User permissions on the system are centrally granted and access is monitored by a dedicated logging system. A customizable password policy can be enforced centrally. All access controls are logged in detail while sensitive information is protected to meet privacy and confidentiality requirements.

Engines are managed by an engine manager (EM) component within the Siemens DEOP platform. The EM acts as abstraction layer between each engine and Siemens DEOP itself. For performance and security reasons, EM is running each engine within its own separate process. Within such processes, the EM allows engines to interact with the Siemens DEOP platform through a simplified API that does not require engine implementors to possess a-priori knowledge of the architecture, technological stack and data models of the Siemens DEOP platform.

In terms of cyber incident handling and vulnerability handling (IH/VH), the Siemens ProductCERT is an industry benchmark, which ensures a transparent and responsible process of keeping customers informed. This is valid, too, for potential security incidents affecting Siemens DEOP or its cloud infrastructure. A three-stage service support model is available and a training for CPO/EMP operators as well.

**5. Siemens DEOP in the cloud**

Customers can obtain Siemens DEOP platform as a managed service. The applications will then be operated by qualified and experienced Siemens employees. They further help customers to minimize risks and take accountability for IT security. The Siemens DEOP platform design ensures that each client environment is isolated from any other clients' data or system functions. The modular and scalable managed security services adapt to changing customer protection needs.

The service can be implemented quickly and easily by specially trained Siemens employees for use almost anywhere in the world. They constantly develop and implement a professional IT security concept that supports comprehensive protection at minimal costs without having to worry about purchasing, resources and competences, configuration, operations, and expansion.

## 6. Siemens DEOP as managed Service

Customers can obtain Siemens DEOP platform as a managed service. The applications will then be operated by qualified and experienced Siemens employees. They further help customers to minimize risks and take accountability for IT security. The Siemens DEOP platform design ensures that each client environment is isolated from any other clients' data or system functions. The modular and scalable managed security services adapt to changing customer protection needs.

The service can be implemented quickly and easily by specially trained Siemens employees for use almost anywhere in the world. They constantly develop and implement a professional IT security concept that supports comprehensive protection at minimal costs without having to worry about purchasing, resources and competences, configuration, operations and expansion.

The Siemens DEOP platform is hosted on a AWS cloud platform, whose mature security and privacy practices and protection measures are certified to be conforming to ISO 9001 (quality management), ISO/IEC 27001 (information security), ISO/IEC 27017 (cloud security), ISO/IEC 27018 (cloud privacy), SOC 1 (Audit Controls Report), SOC 2 (Security, Availability, & Confidentiality Report) and SOC 3 (General Controls Report) standards. Moreover, the AWS platform demonstrates its compliance to the security best practices published by the Cloud Security Alliance (CSA) for cloud service providers. The security and privacy controls provided by AWS for its customers include security incident management, response, and notification.

Complied standards are listed online at
https://aws.amazon.com/compliance/programs including additional nation-specific standards.

**Siemens Grid Software**

**Grid Edge suite**
**DEOP**
Cybersecurity | June 2022