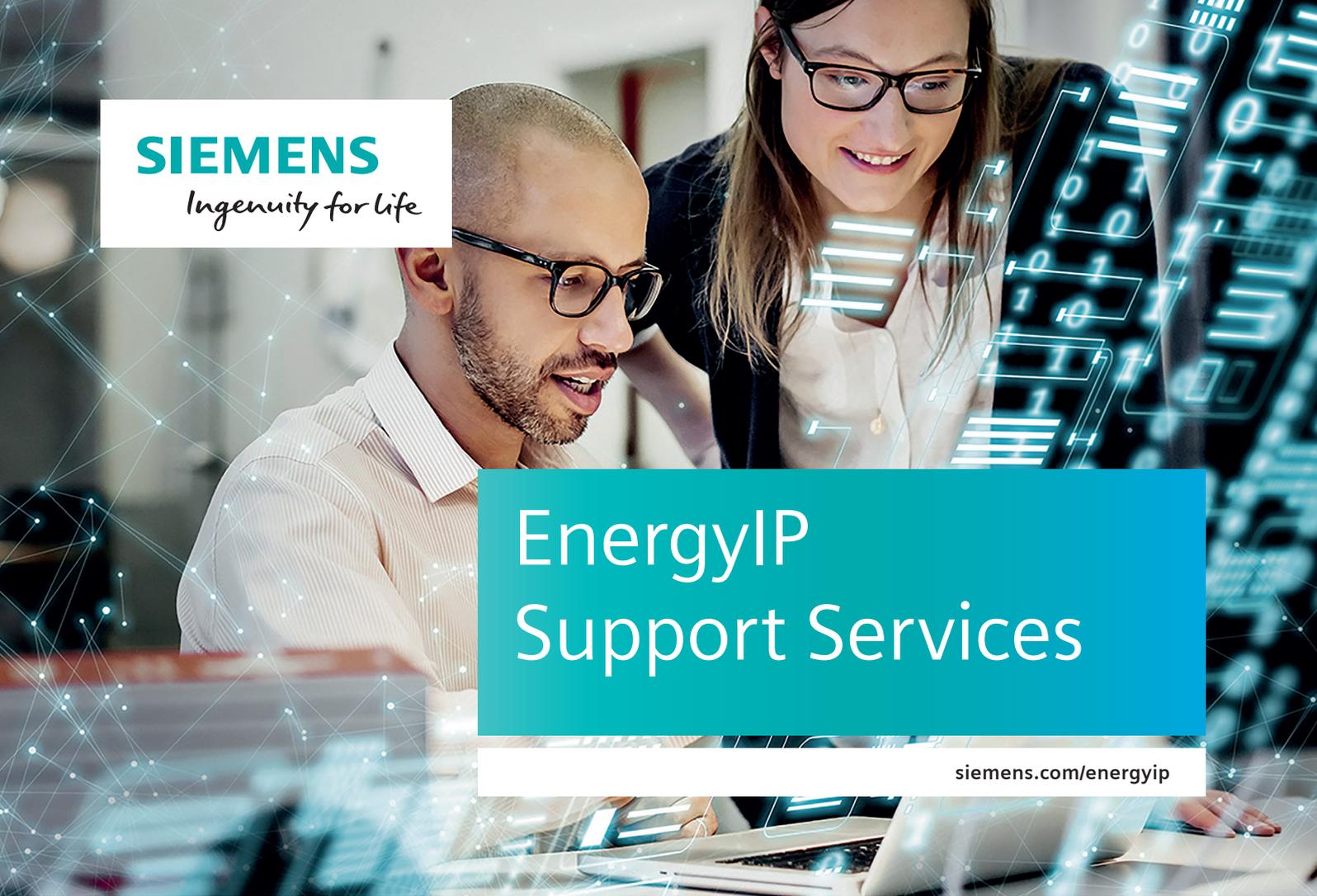




SIEMENS

Ingenuity for life



EnergyIP
Support Services

[siemens.com/energyip](https://www.siemens.com/energyip)

The information presented in this document
is current as of: September 2018

Contents

3	Standard Support
3	Overview
3	Siemens Global Support Processes
6	Additional Services
7	Analytics as a Service
7	Description
7	Methodology
7	Our services
8	Our methodology
9	Current proven use cases
10	Remote Monitoring Service (RMS)
10	Description
10	Potential Benefits
11	RMS Processes
11	RMS Benefits
11	Specific Tasks Executed as Part of RMS
12	Reporting, Continued
12	Pricing
13	QA and Performance Environment
13	Description
13	Design and Apporval
13	Build-Up and Go-Live
14	Potential Benefits
14	Pricing
15	Cyber Security Assessment
15	Description
15	Scope
15	Methodology
16	Potential Benefits

Standard Support

Overview

This is a Reference Guide for the Siemens Standard Support Services, its procedures, processes and policies, provided for your Digital Grid Application product. It details where to go and what to do when you or someone in your organization suspects that any part of the Siemens EnergyIP Platform or any of its related applications is functioning improperly or has an issue.

Siemens Global Support Team's (SGST) goal is to provide a responsive team to navigate the issues that your organization may encounter. We are confident that the investment in us will provide not only world class software but also industry-leading support and customer satisfaction.

The Maintenance and Support (M&S) contract mutually signed by the utility and Siemens provides access to the SGST and its issue resolution processes.



Siemens Global Support Processes

24/7 Urgent Care Hotline

Staffed by SGST, urgent care hotline is available for the issues severely impacting production systems. It is the first point for contact for Severity 1 and 2 issues which have a direct and significant impact on the utility's business. Response times vary depending on the severity of the issue. In the event of SEV-1 or 2 issues, putting a support ticket first with the sufficient information helps us to triage the problem and then to follow up, call the support number if you have not received adequate response via the ticketing system. When a Severity-1 or 2 ticket is created, SGST immediately receives a page notifying them of its existence and Severity level.

If you are unsure whether or not the issue is serious enough to merit a SEV – 1 or 2 level of severity, call us or create a ticket in the eSP ("EnergyIP® Support Portal") portal. We will evaluate the issue and help determine the appropriate severity level for reported issue.

EnergyIP Support Portal (eSP)

The eSP is the hub of support activities where customers can open support tickets anytime, regardless of severity.

Issues are tracked, updated, and maintained. Users will be able to look for historical and open support tickets through browsing, as well as simple and advanced searching methods. All tickets are given unique ticket numbers. Support tickets can range from questions on functionality to enhancement requests. The five levels of issue severity encompass any problem your operations might encounter and also set baseline expectations for response times. All issues, regardless of severity, must have an eSP support ticket associated with them.

Knowledge Base Center (KBC)

Ticket creation is not limited to just reporting problems. If advice or assistance is desired – for example, a question about how to work around an issue encountered due to an error – we encourage you to search KBC or product documentation and if your concerns are still unanswered, please create a ticket with appropriate severity level. SGST will respond directly in due course.

Siemens eMeter Documentation

Siemens eMeter staffs a dedicated Documentatoin Team to ensure that our customers have the correct information for their system at all the time. Documentation is provided online, and you can request greater clarification on any page that is unclear by creating a support ticket.

Issue Resolution

Every ticket upon creation in eSP are worked by SGST by different levels of support and teams formed internally. Level-1 team is responsible to acknowledge and make first response on each new ticket. It includes initial triage, request additional information if required and provide resolution. If they are unable to find a quick resolution, issue is escalated to next level.

Level-2 team has advanced knowledge of product and do deep dive analysis of the reported issues. This team verifies if reported issue is a software defect or data/configuration issue and escalate to R&D for release planning and delivery.

Sev1/Sev2 issue resolution process is well-established and repeatable. With your initiating phone call, the Support Engineer on call will quickly review all available information with you and make requests for additional information, if required, that might help to triage the issue. In some instances, SGST may request for a screen share meeting to speed up diagnosis and resolution. Once the system has regained stability, as confirmed by your organization, the next step is for Siemens to explore options for a long term solution.

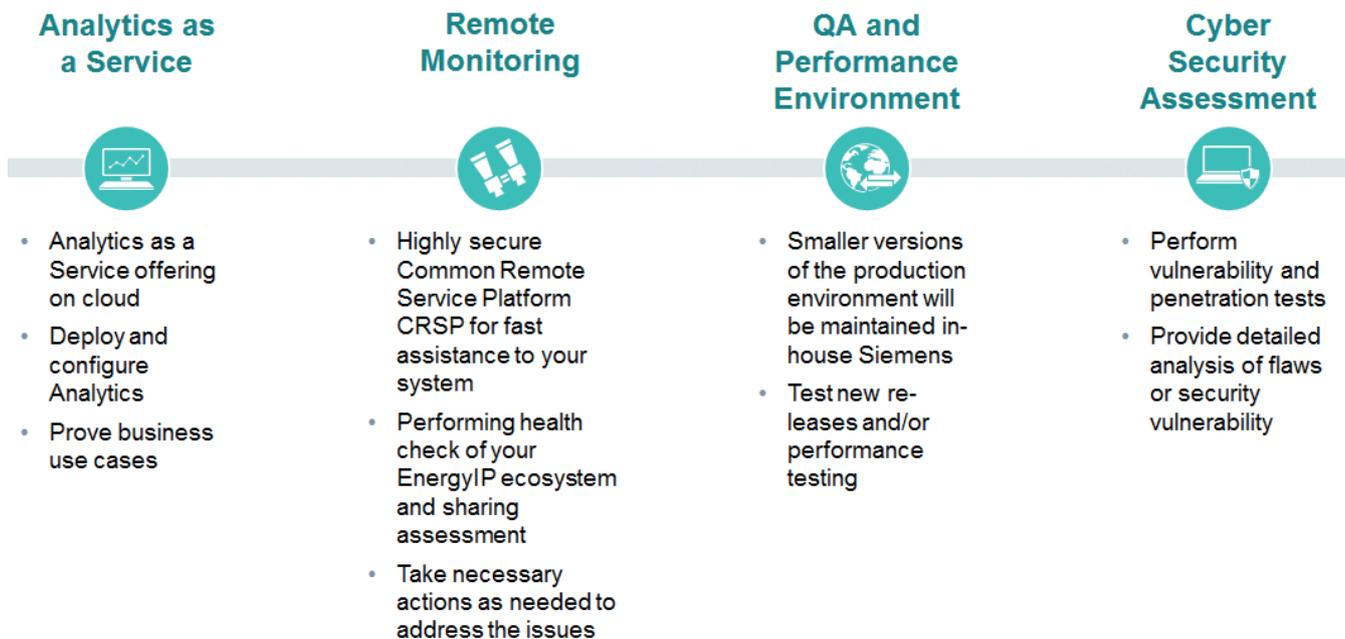
Priority-1 issues need to obtain timely responses and attention from SGST as they affect business or project timelines. We understand that these are important to our customers and therefore a dedicated team processes all the Priority-1 cases to provide faster resolution and meet your needs.

Escalation management team ascertains that concerns raised by reporter is well understood and help promoting better resolution and outcomes. Customers have the ability to trigger escalation of an issue through support portal to engage the Support Management.

SGST provides a base for the operation of the industry-leading Meter Data Management platform, Ticket and its applications. It only covers the software defect identification and resolution for core product functionality or feature and enhancement requests forwarded to Product Management. It does not cover performance tuning and environment sizing, database configuration and tuning, upgrade planning, review of custom configuration, or specific features and implementations. For such extensive service offerings, please contact your Siemens Account/Sales representative for the details and quote.

Additional Services

The next section describes additional services beyond the M&S that the SGST provides to its customers.



Interested in this Service:

- Pick one or all of the above mentioned service offering.
- Contact your Account Sales Representative for a quote
- List the areas where you need help with the EnergyIP suite of products.
- Identify the number of systems that needs to be maintained under this contract.
- Quote to include a license for the cRSP tool in case of Remote Monitoring Service.
- Approve quote and rest easy knowing that your production system is in good hands.

Analytics as a Service

Get insights and solutions for critical business problems using a combination of the EnergyIP Big Data Analytics platform and data science service provided by Siemens

Description

Siemens Analytics Applications offered by its Managed Services division, has been designed to enable our utility customers derive valuable insights into the data locked within the EnergyIP system. The aim is to transform their businesses by analyzing data from all applications and distributing targeted analytics to every stakeholder across their business network.

Our highly scalable EnergyIP platform and its corresponding analytics application, coupled with the experienced data science team, allows organizations to unlock the value of their existing data across all enterprise systems and third-party data – creating best-in-class analytic solutions that guide everyday utility users, both internal and external, to meaningful insights. These solutions allow our customers to improve their relationships with their energy consumers and C&I partners by increasing customer retention and creating new channels of revenue.

Methodology

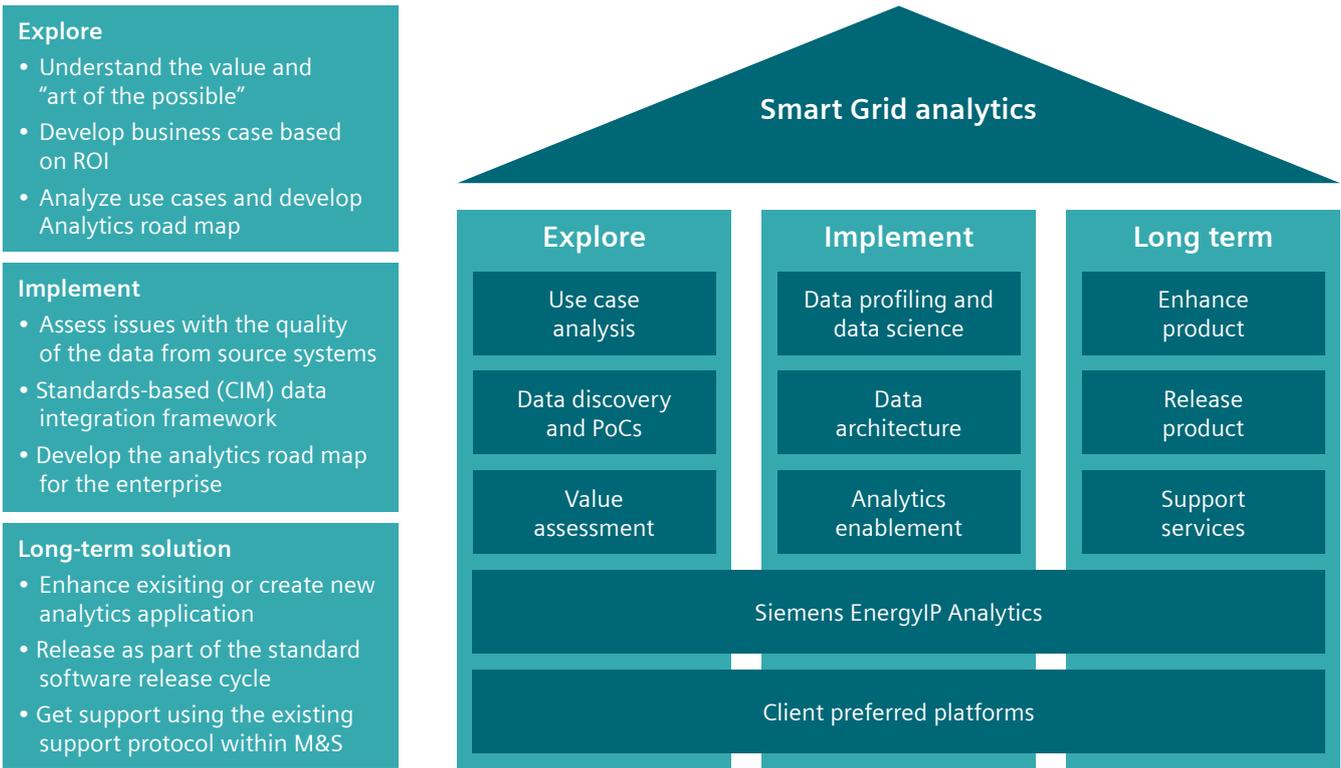
At the start, we recommend that you engage Siemens with your business users to identify requirements using workshops, conduct gap analysis to ultimately come up with a set of use cases, expected results, and a road map for your analytics needs. This will be followed by a four- to eight-week engagement to demonstrate feasibility of ad-hoc data mining results using machine learning (ML) and Artificial Intelligence (AI) algorithms to demonstrate results and value for the specific use cases in the context of client's data and operating environments. If a permanent solution is desired in a product, a custom quote will be provided so that the Siemens Analytics applications can be enhanced and/or new functionality added to cater to all the specific use cases. This will be followed by an in-person presentation to all stakeholders that would seek to establish a long-term strategy to take care of the current as well as any future analytics requirements from AMI data.

Our services

Our service offerings focus on three major areas of analytics consulting and implementation services for utilities or system integrator companies, leveraging our experience in IT, OT, and Smart Grid. We can help our customers with the following steps:

- **Explore:**
Access the data that is already in the EnergyIP platform and combine that with the problem definition and mine the data to come up with insights and priority use cases.
- **Implement:**
Deploy and configure the Siemens Analytics application in our internal cloud environment to satisfy the above use cases. This will be followed by installing the algorithms specifically designed for your use cases to finally provide the desired insights into your data.

- Long-term solution:
Once the algorithms have been proven and the results validated, Siemens will enhance its analytics solution and release a new version of its Analytics application on your EnergyIP system. Your staff will then be trained to operate this product to meet your business needs.



Siemens provides a joint product plus service offering that lets you analyze your data and receive valuable insights from your smart grid data.

Our methodology

Siemens Analytics product has been designed to be parameter-driven, and for the most common prediction issues like load forecasting and revenue protection we can use configuration parameters to cater to the specific needs of the utility. However, in certain specific use cases, Siemens recommends that utility customers first embark on a data science project. This project will help hash out the requirements, the parameters, and the prediction that is required from the analytics application. This will be followed by a short engagement by our services team consisting of EnergyIP experts, data scientists, and implementation specialists, where the data necessary for the problem analysis will be retrieved from the EnergyIP MDM system into the AWS cloud, where the analytics products can then be configured to mine this data. So at a low initial cost, the utility’s data can be used, custom data science algorithms written, and the results of such prediction algorithms presented to the stakeholders. Once the final results have been validated, if required the analytics product can be enhanced and then deployed at the utility site. Please check with your account manager and invite us to have a discussion around how Siemens can help you release the insights hidden in your data.

Current proven use cases

Siemens Analytics Foundation and its application have been deployed at many customer sites. Some of noted use cases are listed below:

1. Water leak analysis
2. Revenue protection
3. Technical balance
4. Accounting balance
5. Power quality
6. Equipment load management
7. Load forecasting

Remote Monitoring Service (RMS)

A service to proactively monitor your EnergyIP environments and minimize downtime

Description

Siemens offers Remote Monitoring Service (RMS) to its customers who have deployed EnergyIP in one or more environments and who require daily assistance to proactively look for trends and prevent system failure.

The need for RMS can vary, but in most cases, it stems from lack of administrative knowledge in the technology stack deployed for EnergyIP (Linux vs Microsoft) including Hadoop and Linux, or a lack of expertise managing the Oracle RDBMS. In most cases, it is also due to the need to monitor one additional critical system in their enterprise infrastructure, thus overburdening the already strained IT staff.

As mentioned above, some of the factors driving remote monitoring proliferation have to do with lower upfront investment costs for implementation; others are the result of leaner operations and having fewer IT staff available to monitor the systems. Not only does remote monitoring enable Siemens to monitor conditions from just about anywhere, it also facilitates more effective monitoring by fewer personnel, a real differentiator in today's tough economic climate.

Potential Benefits

The potential benefits of remote monitoring are significant: minimizing labor costs, filling the knowledge gap resulting from experienced operators retiring, preventing unplanned downtime, and more. However, there's no way to know what types of tasks can be best done by a remote monitoring service to maximize returns. While remote monitoring can greatly contribute to cost savings and improved operations, there are considerations that must be addressed to ensure the security and practicality of implementing a remote monitoring system. Also required are definitions of what data can be accessed and by whom, and most critically, what remote control options will be allowed.

In the end, it comes down to keeping the production system running smoothly with minimum downtime. Siemens personnel can monitor your production systems from our secure Network Operations Center (NOC). When an error occurs, we will notify you, and also create an eSP (Support Portal) ticket so that our certified support engineers can quickly start working on the issue to resolve it in a timely manner.

RMS Process

- Log in remotely to the production system using cRSP (common Remote Service Platform)
- Perform a mutually agreed upon list of steps and processes and tag results
- Maintain the history of the results with a daily timestamp
- For alerts, add an eSP ticket to be fixed and resolved
- For details on cRSP, please contact your Sales Account Manager

RMS Benefits

- Access to a global network of experts
- Highest security and access using cRSP for the protection of sensitive information
- Utilization of future-oriented IT-based services, provided in a partnership that is set up for longterm success
- For details on cRSP, please contact your Sales Account Manager

Specific Tasks Executed as Part of RMS

Daily System Check:

As part of the RMS service, our staff will

- Validate connectivity to the UI and other components
- Validate that meter read data is current
- Check the amount of memory being used for your systems
- Check for any CORE error dump files
- Check log files for errors

Validate Persistent Applications:

- Container status check (Apache Tomcat, ActiveMQ)
- Workflow Management System applications
- Platform applications
- Interpolation, Import Reads
- All Adapters that import / export
- Meter Data Processing – VEE

Reporting, Continued

Validate Log Files and Health of OS/Oracle:

- Look for ORA or fatal errors in all logs
- Validate other applications
- Check disk space
- Check Oracle health and its table spaces

Monthly/Quarterly/Yearly Review:

- Review and validate your daily checklist and send status reports
- Review and validate your monthly checklist and send status reports
- Review and validate all your EnergyIP environment settings and update any documentation
- Review and validate all crontab settings found in production and update any documentation
- Review and update any documentation related to your internal escalation procedures
- Review and validate the usefulness of EnergyIP reports
- Review and validate the usefulness of EnergyIP notifications
- Update Visio documents related to this site with recent changes
- Confirm with the system administrator that backups are occurring
- Verify disk space usage
- Verify that all file systems are compliant with the flat file system data retention and validation policy
- Verify that database data retention cleanup efforts have taken place
- Validate all users and document their access to the Usernames tab

Pricing

- Fixed price per month
- Number of hours based on mutual agreement and discovery of all tasks
- Tasks performed by certified Support personnel
- Full audit trail of login/logout and activities maintained for SOX compliance
- Please contact your Siemens Sales representative for further details

QA and Performance Environment

A service to create and maintain a QA / testing, system owned by you and managed by Siemens within its Data Center

Description

The QA / Testing system creation and maintenance service is a value-added service provided by Siemens to its utilities customers that would otherwise have to plan for such a system and staff it to cater to the needs of their internal business users. Typically, smaller to medium-size utilities that are hard-pressed for staff or want to focus on their core competences tend to sign up for this service.

Design and Approval

The need for a QA / Testing system is very well known, but the development and maintenance of such a system requires dedicated staff and scripts that take away time from the utilities' core mission. Siemens engineers will meet with the utility staff to ascertain the requirements of such a system – for instance, what use cases will be handled, how frequently production data will be refreshed into the system, how many users will access it, etc. – to ultimately decide the size and location of the system. A custom architecture and system will then be designed to cater to the requirements, and multiple rounds of discussion will follow to optimize the design. Once the design has been approved, it will be used to prepare a custom quote complete with hardware specifications, network size, location (customer premises or Siemens data centers), and data refresh frequencies. Our Sales team will follow up and provide clarifications, if needed, during the approval process.

Build-Up and Go-Live

Once the specifications are approved, the customer will procure the necessary hardware and software licenses and provide them to Siemens engineers. This ensures that the system belongs to our customer, but is managed by Siemens as a service. Siemens will then install all the software to exactly match the production EnergyIP system, including all the current OS, Oracle and eIP patches. This will be followed by installing scripts to collect data from production and restore a representative set of data into this system that will be refreshed periodically.

After internal testing and validation that the system meets the requirements set forth for this system, Siemens engineers will demonstrate the features to the utility staff to make sure that the system meets their requirements. Upon approval, this new QA / Testing system will be brought online and used by both the utility staff and Siemens staff assigned to provide the required service.

Potential Benefits

Such a system has many benefits.

- First it lets the utility test new functions and study the impacts of applying a new patch to their production systems, before actually applying it.
- It provides an environment to test bug fixes and other recommendations provided by the Support teams before applying them to the production system by a Siemens personnel.
- It reduces the time of such bug fixes and patch upgrades to be applied to production.
- Most important, Utility personnel can now focus on areas that are core to their business and offload the maintenance of such a system to engineers who are trained specifically to maintain and monitor it.

Pricing

- Fixed price per month
- Hardware and software licenses purchased by the utility.
- Use cases based on mutual agreement and discovery of all tasks
- Tasks performed by certified Support personnel
- Full audit trail of login/logout and activities maintained for SOX compliance
- Please contact your Siemens Sales representative for further details

Cyber Security Assessment

A service to perform controlled security vulnerability check of one or more internal systems

Description

Siemens partners with many information security companies to bring this very critical and value-added service to its Grid Control and EnergyIP Customers. This service will ultimately lead to developing effective security architecture within the utility data centers by enhancing company-wide security programs. We do this by first identifying all the vulnerabilities and performing a full security assessment of the utility organization's information technology assets as related to the EnergyIP server. The objective of this effort is to assess and the current information security posture of the organization's enterprise assets and network environment. The phases for this assessment includes internalfacing web application testing and internal information assets testing, by using a trusted appliance and accessing the network remotely to search for vulnerabilities within the network.

Defending the enterprise against security threats with today's complex information infrastructure requires a layered security strategy. Companies should structure their strategies to mitigate risk at defined points within the environment. Siemens works with organizations to apply effective security measures and provides a working knowledge of the best-in-class products and recommendations to implement improvement for the network.

Scope

Risk reduction through vulnerability assessments and penetration tests is an example of how Siemens helps our customers improve their overall security posture. As part of Siemens' ongoing commitment to ensure the security and integrity of their network assets and data, we will perform an assessment of the current information security posture of the utility's external and internal network environments. Siemens will approach security assessments and try to locate vulnerabilities document the findings, to finally create a remediation plan to secure the system, including hardware and software.

Methodology

The methodology executed by this engagement focuses on black-box/blind penetration testing of the utility's (perimeter/external/internal/complete) environment. The assessment will provide our customer with a comprehensive discovery, analysis, and controlled exploitation of its security vulnerabilities accessible from an external source. This measures the effectiveness of the organization's security efforts and prevents the compromise of critical data assets.

Throughout the technical testing phases, Siemens consultants will use multiple commercial and open-source security tools, custom scripts, and manual validation techniques to scan for, enumerate, uncover, and exploit vulnerabilities in the systems tested. Commercial scanning and penetration framework tools are used, such as NeXpose, Nessus, and Metasploit as well as best-of-breed open source tools such as NMAP that quickly identify network, host, and application-specific vulnerabilities. Manual techniques are capable of finding issues not easily uncovered by automated tools.

Potential Benefits

Siemens performs proper due diligence by engaging a trusted third parties to independently evaluate their systems and applications from an information security standpoint. Based on the findings, which will be provided to the utility as a written report, utility staff can then implement or take preventive measures including many practical steps and best practices to ultimately exceed industry standards for information security.

In the end, it comes down to keeping the production system humming smoothly with minimum downtime. Siemens personnel can perform these security audits using trusted third-party vendors, and together ensuring the smooth running of your production systems and related assets. When a security breach occurs, Siemens will also provide consultation or set up a process to properly identify such a breach, communicate it effectively, and then get the required parties to approve the fix. Once the fix has been identified and approved, Siemens staff can help our utility customer in the application and implementation of the fix to finally make sure that the breach has been corrected.

**Published by
Siemens AG 2018**

Energy Management Division
Freyeslebenstrasse 1
91058 Erlangen, Germany

For more information, please contact our Customer Support Center.

Phone: +49 180 524 70 00

Fax: +49 180 524 24 71

(Charges depending on provider)

E-mail: support.energy@siemens.com

Subject to change without prior notice.

The information in this document contains general descriptions of the technical options available, which may not apply in all cases. The required technical options should therefore be specified in the contract.