The REC evolution – Embracing the cyber dimension

Whitepaper

siemens-energy.com/omnivise-t3000

The REC Principle

Every kind of power plant needs instrumentation and control systems to operate normally. This is just as true for new generation energy plants, using wind, solar power or hybrid systems, as it is for traditional generation coal, oil and gas-fired plants. They all need controls, and they are all vulnerable to different kinds of threat.

The Remote Expert Center (REC) concept was established by Siemens Energy over 20 years ago to provide comprehensive, rapid support to all operators of Siemens Energy Instrumentation and Control Solutions. Right from the start, the REC extended far beyond acting simply as a hotline and helpdesk for Siemens Energy controls related products.

Comprehensive, integrated capability

The REC brings together experts in Siemens Energy control technology, with capabilities in market operations, production technologies, sensors, data management and advanced IT. At the REC we integrate these disciplines as part of a single, customer and market-focused resource. It is available for support across a wide range of requirements: from advice on system and process optimization to rapid response regarding time-critical concerns.

Safeguarding availability

The key priority for power generation businesses today, as it was the day the service was launched, is to safeguard availability.

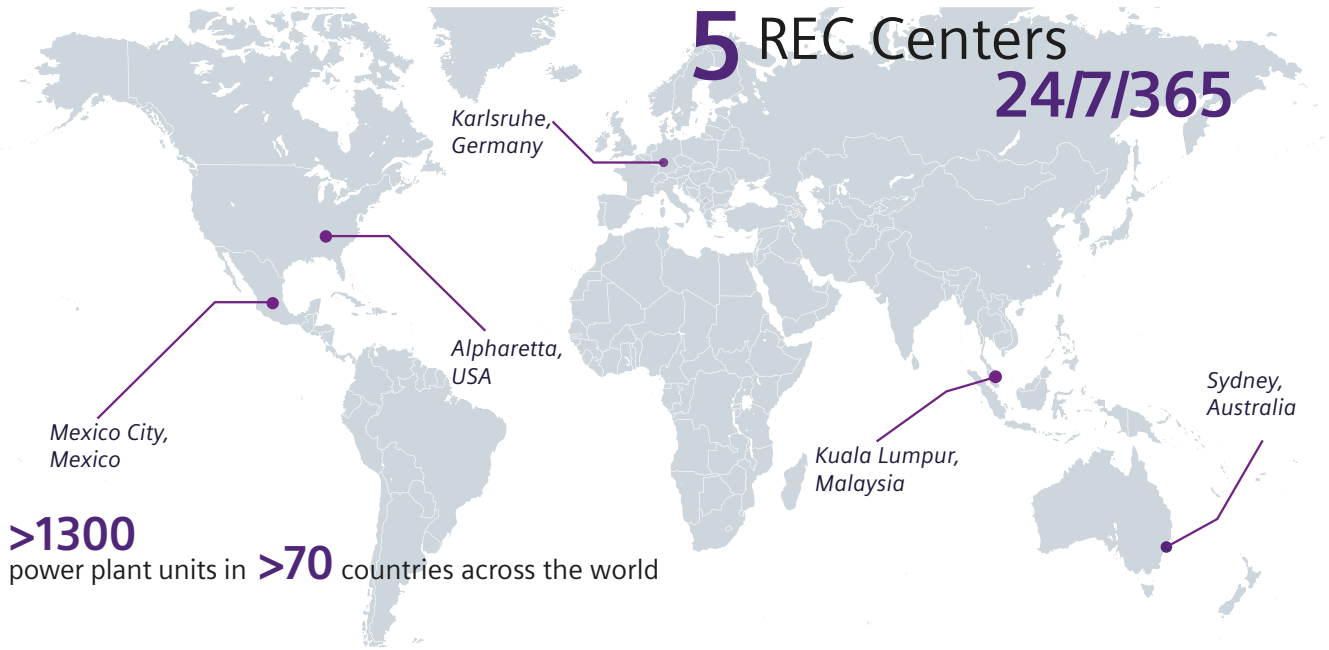
The aim of the REC is to be that single touch point that enables operators to access all the help they need to meet availability challenges for their power plants.

Wherever they operate, power generation companies are committed to provide defined power output to their grid as and when required, often with serious penalties for failure. Availability, therefore, is the key to keeping a business viable and profitable, and it has increasing significance for a range of different regulatory reasons, as well. National and, in some cases, international regulators have established tougher regimes to manage all key indicators, from time to come online to security protocols to emissions and other sustainability measurements.

Siemens Energy REC plays an important role in helping operators to meet all their varied commitments, maximizing their investment in capital equipment, and continuously keeping and even improving operational efficiency.

The REC in operation

The global network of RECs includes central and regional centers to ensure that technical and appropriate language skills, cultural awareness and local knowledge are always available. Together, the RECs provide comprehensive 24/7 online support for all managed functions related to Instrumentation and Controls.



Key Priorities

The REC proposition goes far beyond routine monitoring and reports, backed by a hotline for accessing emergency support. Used effectively, the REC provides an extension to the customer's own team, enabling them to access capabilities that may no longer be affordable in house (especially given the continued shortage of appropriate expert resources in the market).

The service provided by the REC network covers a very wide scope of activities, monitoring data flows from production equipment, providing reports and expert insight to optimize predictive maintenance, helping maximize production output and take rational steps to extend the life of their components and core assets.

Responsive and preventive

REC support falls under two key headings:

Responsive

A *responsive,* 24/7/365 service designed to provide fast support to operational problems as they emerge. Here the global structure of the REC network means that customers will be in contact with experts who can be online as and when needed, and with a certain level of regional expertise to supplement their engineering know-how.

Preventive

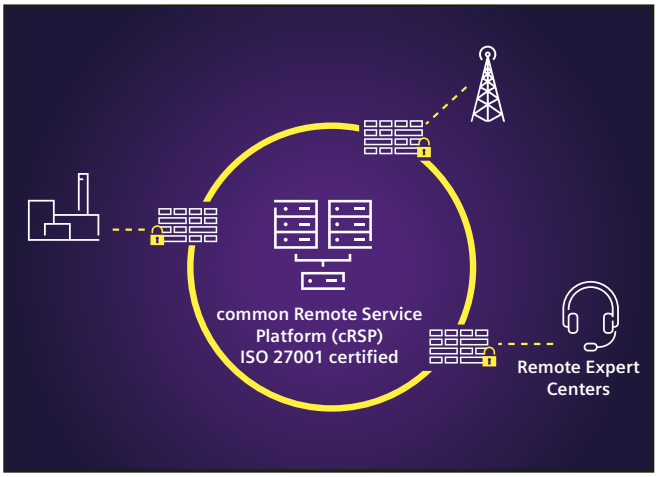
A *preventive* service designed to investigate current systems, scan for and identify potential weak spots, and plan a program of remedial work to fix problems and strengthen the resilience of customer systems.

These two services are mutually supportive and will be explored in more depth later.

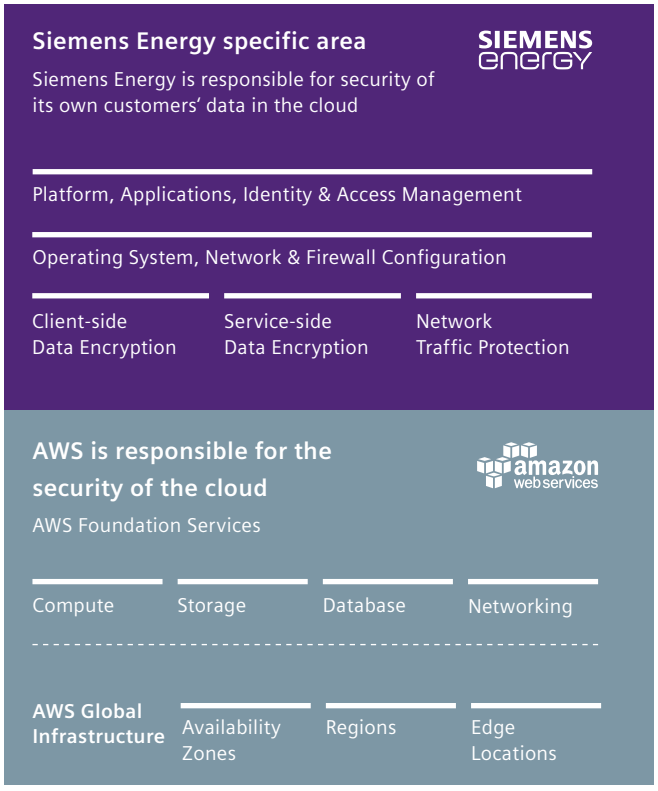
Integrated global reach

To ensure secure, uninterrupted communication between RECs and customer sites, Siemens Energy uses its common Remote Service Platform (cRSP). This establishes a secure (ISO27001 certified) connection from individual Siemens Energy service experts and systems to each customer site, wherever and whenever needed.

Remote Service Distance is not an obstacle



The REC network currently serves a large, globally distributed installed base of Siemens Energy T3000 and legacy I&C solutions. It provides an environment that combines the ease of use and cost efficiency of cloud, offering access through a customer portal, and the security of an environment that meets the most demanding security standards. To deliver the right combination of convenience, cost and security, Siemens Energy builds on its strategic relationships with AWS, the world's largest cloud services provider, through our Shared Responsibility Security Model, as shown in the figure below.



In this approach, the AWS hyperscale cloud platform concept provides the basic infrastructure for all cloud services, corresponding to the building, utilities and hardware that are used in a standalone datacenter. AWS is also responsible for securing this core infrastructure: *so AWS is responsible for the security OF the cloud*.

Siemens Energy, however, is fully responsible for building the platform required for service delivery, just as in a physical datacenter. In this model, Siemens Energy defines the physical location of data, which makes it a private cloud instance, and so helps to ensure full compliance with prevailing regulations in any appropriate jurisdiction where services are offered.

Siemens Energy also manages identity and access, provides the operating systems and applications, while handling all aspects of configuration, service and application update, and end-to-end security. *Siemens Energy is therefore responsible for security IN the cloud*.

In this way, customers gain the benefits of high performance matched by affordable cost, always updated / at best practice level cloud infrastructure, with no need for upfront capital investment, backed by the same or maybe better security assurances that fully on-premise systems can deliver.

Growing capability

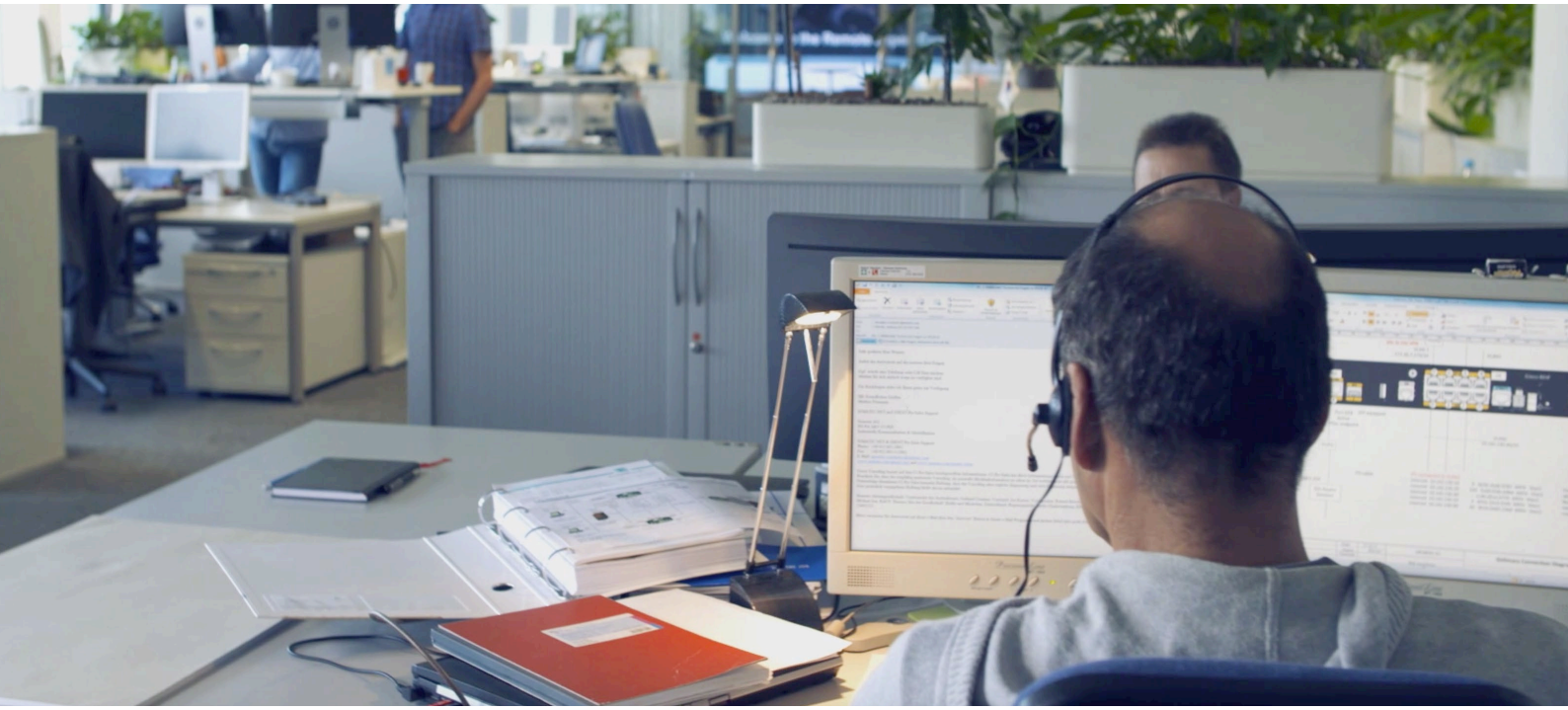
Initial customer questions are routed to appropriate personnel in the full-time REC team of engineering experts. RECs are fully-equipped and self-contained, physically separate from other operational centers, and possess their own systems, locations and dedicated teams.

The image below shows the REC in Karlsruhe in Germany, which provides dedicated expertise, able to manage the majority of DCS-related issues. It can also make available the full range of Siemens Energy engineering expertise for support to problems that present unusual challenges.

The REC concept in its earliest stages enabled expert Siemens Energy staff working remotely to collect and analyze data from customer sites, identifying potential issues and providing advice on request, giving input to customers for trouble-shooting, updates and production optimization. Further capability has been added, year by year, to the point where the REC can act as a normal, and essential, extension to customers' own in-house systems and personnel.

As a preventive service, Remote Inspection permits Siemens Energy REC engineers to review general operational performance and the status of individual components in depth, helping to identify current or potential weak points, and providing detailed advice to the customer. This makes it possible to carry out planned maintenance on components that are likely to fail, thereby avoiding unplanned shutdowns, while safeguarding availability.

The REC now integrates digital solutions, the Instrumentation & Controls Monitors and Advisors service (ICMA), a full digitized strategic service that enables customers to define exactly the right level of support for their needs, and use Siemens Energy resources to provide this.



Supporting Industry 4.0

As the entire industry digitizes and moves towards an Industry 4.0 model, so the ability to mobilize specialized resources and capabilities in support of current operational priorities becomes more important. This enables faster scaling, greater operational agility and rapid access to best practice, without having to maintain costly expert resources in-house.

The REC forms the key access point to these enhanced Siemens Energy services for power generation businesses worldwide, whether they require immediate action to address an ongoing problem, or long-term preventive support for continuous optimization to maximize availability. Services available via the REC are constantly evolving:

ICMA Tailored Patch Information (TPI)

The ICMA Tailored Patch Information (TPI) service ensures that systems are kept secure, with every security update provided on time, while rapidly addressing urgent security patch issues

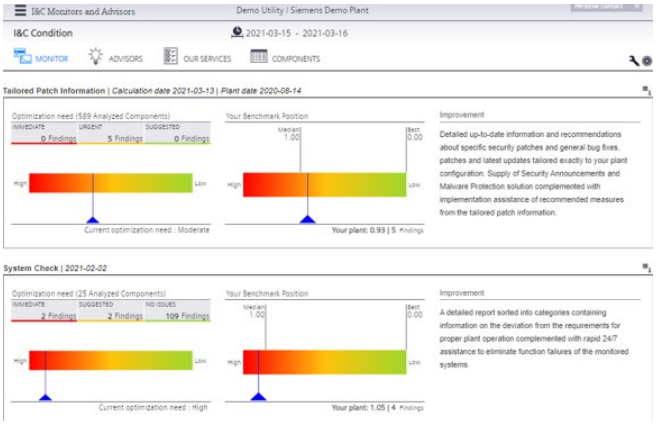
ICMA System Check (SysCheck)

ICMA System Check (SysCheck) is a key preventive service, monitoring the health of every component and system within an operational environment, providing detailed analysis of current condition, down to component level, with recommendations for actions to optimize performance

Customer-focused and tailored services

These are examples of how the REC's unique blend of technology and human expertise provides customers with deep insights into systems and components, helping them to dig into specific issues, while also providing answers to the more complex technology questions. The REC connects customers directly to the outstanding expertise, quite apart from automated response systems and algorithmically generated data analytics.

The REC offer is also tailored to exact customer needs. The level of access to expertise and the associated costs of the services they require is defined by the customer and fits in with their own capabilities and technology platforms. The concept is also at the heart of other, targeted Siemens Energy solutions, such as I&C Monitors and Advisors, and can be customized to meet exact needs due to its broad scope and three stage engagement model. Customers can access alarm views and generated reports; online or onsite expert trouble-shooting advice; or full consultancy support for complex requirements.



Monitor view for TPI and SysCheck showing information in a dashboard

Advisor view for TPI and SysCheck showing recommendations for related elements

The Cyber Security Challenge

When the REC concept was originally developed, cyber security was not a well-developed or understood concept. For most power generation businesses, security was largely about the physical integrity of their plant and its equipment, while the most urgent issues they faced were largely related to system and production technology. They were concerned about component failure, the condition of their production assets, faulty electrical connections, wear and tear: classic mechanical and electrical issues.

A growing problem

In the last two decades, evolutionary changes to corporate systems have led to unexpected consequences, some of which are directly responsible for major security challenges. The key factor here is the growing convergence between Operational Technology (OT) and corporate business systems (IT).

OT systems are based around customized IT components, designed to drive rapid improvements in operational efficiency, deliver more agility and enable centralized management of multiple assets. To strengthen management control, improve planning and align key activities, such as maintenance with financial systems (ensuring that a company's supply contracts are in step with planned downtime, for example), OT integration with IT has become not just more normal but increasingly important.

IT systems are normally accessible via the internet, and integration of IT and OT means that production systems are also more easily accessible to external actors. This process of integration, therefore, has led to increased vulnerability to cyber-attacks. The number of small-scale attacks and failures is too large to be easily counted, and many of them are caused by disaffected ex-employees, or by opportunists carrying out ransom-based attacks. Yet there has also been a frightening range of large-scale attacks by state actors, as well.

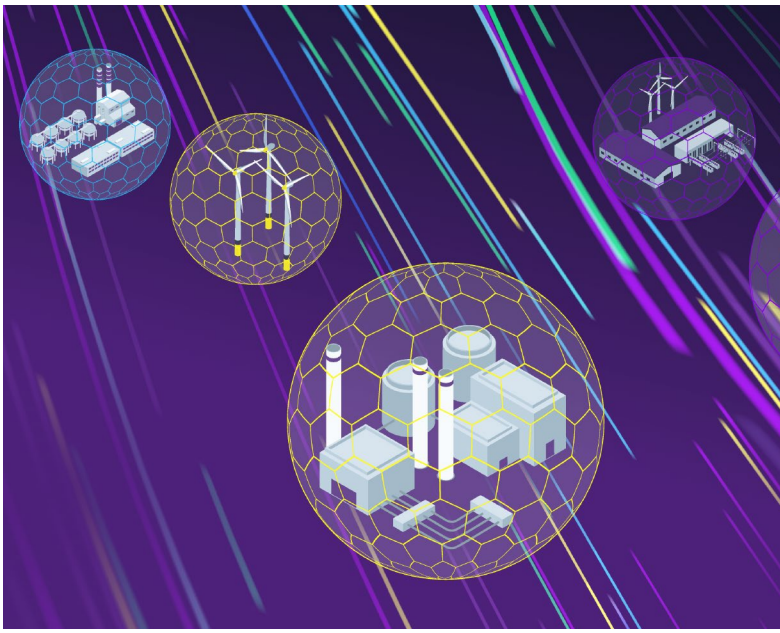
Targeting Critical National Infrastructure (CNI)

The first major known attack happened as early as 2001 (NIMDA), which was spread through infected email attachments. This approach seems almost simplistic in nature, compared with what has followed since. Major attacks against critical national infrastructure have taken place more often since then. One example is an attack that managed to take the Ukraine power grid almost completely offline for a time (2015 – Ukraine Blackout).

Other attacks, such as WannaCry, seem to have been criminal in nature, aimed at securing ransom payments. Petya, again of Russian origin, mimicked the ransomware approach but was clearly aimed at causing political damage to a state (Ukraine – again). Yet perhaps the worst such threat did not emerge until 2019, with Xenotime, which is specifically targeted at power generation, national grids and other Critical National Infrastructures through its Triton malware.

These extremely well-funded and organized, professional adversaries represent the single greatest threat to power generation businesses, as they have the potential to take them offline altogether, thus removing their ability to supply power and therefore to trade. Of course, if there is a truly successful attack, the failure of an individual company to meet its profit targets will not be top of anyone's priorities. The blacking out of an entire national economy will be rather more pressing.

Regulators and governments have responded to these growing threats by urgently requiring Critical National Infrastructure businesses to meet far more stringent requirements than ever before. They also expect proof of compliance, not just at one point in time but continuously, always taking account of new threat profiles as they evolve. To ensure availability in the future, power generation businesses need to look beyond technical concerns and also ensure they are cyber-secure. The risk of a cyber-attack increases day by day, therefore relevant stakeholders should position themselves in a protected state.



Beyond production technology – from REC to REC Cyber Security

The REC concept is designed to offer power generation businesses the first line support they need to deal with their most urgent technical issues, profit from expert support and, by doing so, meet their availability commitments.

It has always brought together experts from a range of disciplines, supported by the technology capability required to deliver the services most appropriate to customers today and into the future. That means capability has evolved to meet changing needs as a matter of course.

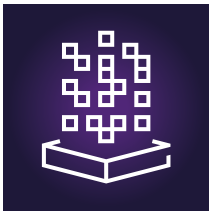
Cyber security services

Siemens Energy uses its own well-established security principles for all customer-facing services, as well as for our own internal systems and processes. Full details of our security strategy can be found in our "Cloud Security White Paper", with relevant headlines that include:

360 degree governance

The strategic approach taken by Siemens Energy to build cyber security into new services and products from the ground up. Based on 5 interconnected processes, this covers the entire value chain at organizational and design levels, then at implementation, constant assessment for new threats and fast response when new threats emerge.

Basic security principles



Introduce a "defense in depth" approach to all aspects of Siemens Energy products and services, ensuring that potential issues are identified early and engineered out through proactive rather than reactive intervention.

Digital security

Using secure data transfer, Shared Responsibility (described earlier) and digitalization of platforms to enable remote intervention without compromising customer data.

These actions form the foundations for Siemens Energy remote support services and enable the REC concept to support customer interests in a completely secure manner. Cyber is now also a core component of the REC service

Building cyber into the REC concept

Cyber security is now becoming a higher priority factor in staying operational, so the REC has expanded its scope to include OT cyber security as part of its normal scope of services and capability. The REC for Cyber Security Service combines our OT expertise and know-how with cyber security leadership to offer a complete and integrated service that addresses all potential threats to availability – from technical failures through malicious attacks.

Cyber security expertise is embedded within the REC to offer customers a comprehensive, Cyber Security Operations Center (cSOC). This is a shared service that brings together expertise on a higher and deeper level than can feasibly be provided by any individual power generation business.

It is a center of excellence in cyber that delivers services tailored to exact customer needs and specifications, with service options defined within three broad areas of activity, as illustrated in the figure on the following pages.

cSOC – the REC for Cyber Security Service

Stage 1
Cyber Inspection

Analysis based on plant data. Preventive detection of cyber vulnerabilities.

Omnivise Cyber Inspection is an End Point Detect and Response (EDR) service that fulfills the preventive part of REC Cyber Security Service. Its capabilities are extended to the point where it can operate as a true Remote Forensics tool.

To support compliance with regulations, **Cyber Inspection** offers Cyber Security Status (Profile) and Event Report, meeting ISO 27001 standards. This gives customers access to a detailed inventory of their systems configurations and settings. Daily data analysis is used to create alarms on abnormal situations. These alarms are extracted and presented including recommendation via the Siemens Energy Portal. More important, red alarms are daily managed by the REC cSOC Cyber Hotline team.

Stage 2
Cyber Hotline

Detection and triage classification of incidents.
Remote Support Cyber Omnivise T3000 Ecosystem.

Whenever a Cyber Hotline ticket is raised by a red **Cyber Inspection** alarm or a reported issue from the customer is identified as a Cyber issue, REC's cSOC team reactively takes action. Before solving and/or support rectifying possible problems, the first level of support is Triage – which is a comprehensive standard algorithm. Triage aims to identify and separate cyber events from cyber events that need to be handled in greater depth and will be handed over to the specific Incident Response service.

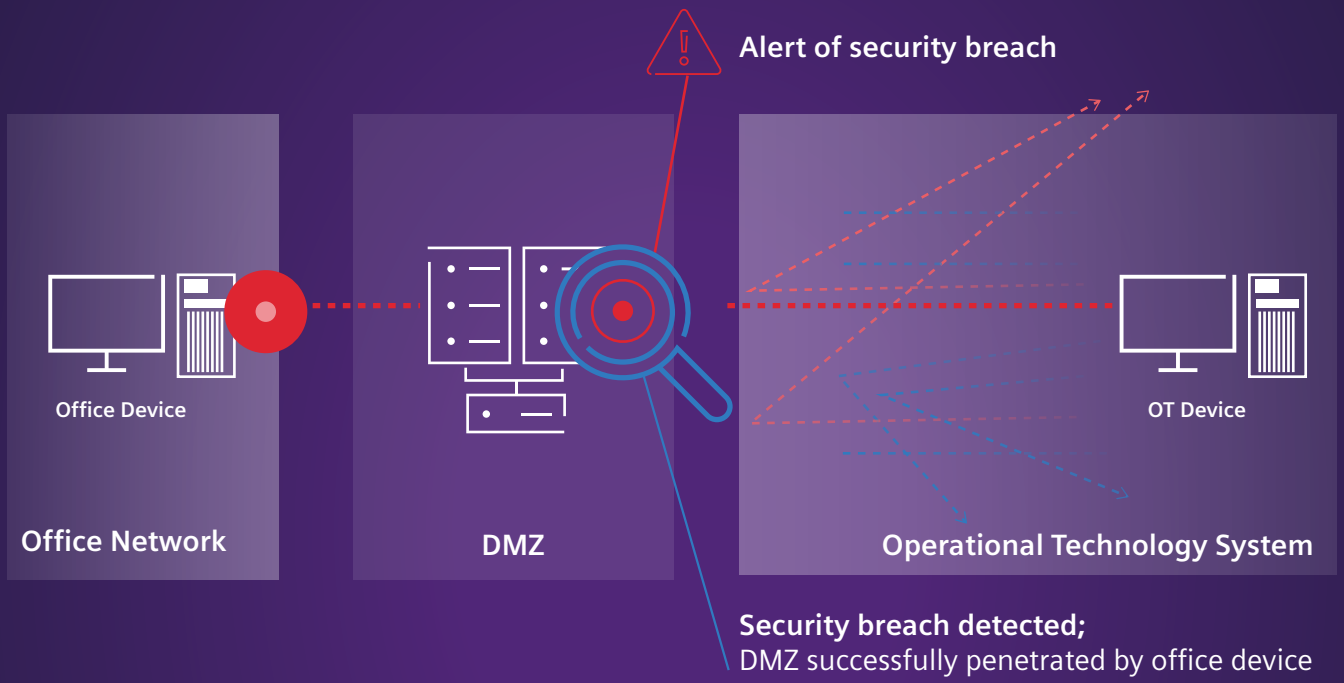
Stage 3
Incident Response

Analysis, containment, eradication, recover and lessons learned from security incidents.

If a real incident is identified in Triage, the **Incident Response** team is activated. Here a full forensic analysis of the system will be performed, and all levels of support are provided to the customer up to the point where a report submission is made to the appropriate authorities, if applicable. The **Incident Response** service will carry out a forensic investigation to identify the nature and origin of the threat in question, to clarify potential points of weakness, and confirm elimination of the threat, together with recommendations and lessons learned.

Addressing a real customer security incident

Siemens Energy REC cSOC identified a potential threat at a large power generation company with operations on several sites and a fleet of assets managed from a central control room, with DMZ between production and office systems. The cSOC noted successful penetration of the DMZ from an office device, following ~5000 log-on attempts.



Actions

Stage 1 Cyber Inspection flagged the incident, a ticket was raised by **Stage 2 Cyber Hotline** and the customer was notified. Rapid triage revealed a significant security incident and, following a customer request, access to the machine.

Forensic action and follow-up.

Stage 3 Incident Response forensic analysis identified a change made to existing DMZ status, designed to open a permanent back door for further access. The DMZ was returned to its required status, with the back door closed. Further analysis showed the source of the breach, a Windows machine inside the company. Charges were made against the person responsible, while the incident response team recommended tightening of protocols and heightened awareness in company personnel.

The combination of new cSOC and existing REC capabilities ensures that all power generation companies with Siemens Energy I&C equipment will now have support against both normal technical issues and the new emerging cyber threats. This combined approach is essential for safeguarding their operational efficiency, availability and regulatory compliance, now and into the future.

Implementation and management

The REC concept has proven its value to power generation companies around the world, staying relevant through constant updating and expansion, developing additional capabilities as new requirements and threats have emerged.

The greatest development in the energy market over the past ten years is the rise of increasingly dangerous cyber-security threats, and that is why Siemens Energy has developed its cSOC for integrated threat management and has built cyber services into the fabric of the REC, itself.

Cyber is now an integral part of the REC concept and will be provided to all new customers from this point on as a matter of course. Existing REC customers will be offered an immediate upgrade to ensure that cyber is added to and integrated with their existing service levels. Siemens Energy believes that DCS remote support must from now on include cyber security services to deliver the comprehensive support that the market needs.

The landscape in which we operate changes constantly, and the support services we provide will evolve continuously to remain completely relevant, to reflect market priorities, and to safeguard customers against a growing number of emerging threats. We have moved from a world in which high fences were an effective security response to a very different reality today. The REC is continuously evolving to remain the only DCS support service any T3000 operator ever needs.

Published by and copyright © 2021
Siemens Energy Global GmbH & Co. KG
Otto-Hahn-Ring 6
81739 Munich, Germany

Article Nr. SVXX-T10023-00-7600

For more information, please visit our website:
siemens-energy.com/omnivise-t3000