SOLUTION PAPER

SITUATOR FOR ELECTRIC UTILITIES AND NERC-CIP COMPLIANCE

SOLUTION PAPER

OVERVIEW

The North American Electric Reliability Corporation (NERC) is a non-government organization which has statutory responsibility to regulate bulk power system users, owners, and operators through the adoption and enforcement of standards for fair, ethical and efficient practices.

Along with the Regional Reliability Organizations, NERC has the legal authority to enforce compliance with NERC Reliability Standards, which it achieves through a rigorous program of monitoring, audits and investigations, and the imposition of financial penalties and other enforcement actions for non-compliance.

As part of these regulations NERC has established the Critical Infrastructure Protection (CIP) 002 –009 standards. These standards specify the implementation of a holistic security approach to protect the bulk electric systems in North America. Energy companies and utilities across the US must move quickly towards compliance to the CIP 002 – 009 standards.

Achieving NERC CIP compliance and maintaining it is a daunting task. With the consequences for non-compliance both costly and risk increasing, the electric utilities industry faces significant challenges in ensuring and sustaining effective, efficient compliance.

This white paper reviews aspects of the electric utilities industry's operating environment and how Qognify solutions comprehensively address the challenges of implementing NERC CIP standards around physical security and sustaining compliance.

BUSINESS CHALLENGES

Faced with the increased scope of new technologies and growing regulatory compliance requirements, Electric Utilities are seeking ways to address challenges such as:

- Consolidation and effective management of huge amounts of data in multi-site environments
- Enforcing consistent event response according to NERC CIP standards
- ncreased training costs and time as a result of high employee turnover rate
- Increased threats and risks while budgets are constant
- Achieving and sustaining NERC CIP compliance

Data Consolidation And Unified Management In Complex Environments

Electric utilities function in challenging environments, with multiple sites -- some unmanned and many remote. In addition, growing expectations for continuously improving, cost-effective safety, security and operations has dramatically increased the scope of new technologies and sensors that are deployed across the organization's sites, sending vast amounts of information into the security control room. The continuous trend of mergers and acquisitions among power utilities increases the number of different brands and technologies that are used in the organization and the number of siloed systems that need to be monitored. This information overload reduces control room operator efficiency and increases the risk of human error.

Inconsistent Event Response

Most electric utilities do not have the necessary policies, procedures and processes in place to adequately meet NERC CIP requirements and to handle events consistently and effectively. In addition, many utilities find it difficult to take written procedures and implement them in actual security control room day-to-day operations and then make sure that every event is handled and documented according to those procedures. With the dynamic nature of the NERC CIP standards, the challenge increases.

Qognify

High Rate of Employee Turnover and Increased Training Costs

Electric utilities must ensure that all security operators within the organization are not only familiar with NERC CIP standards and the organizational procedures that result from these standards, but will follow these procedures consistently. This becomes particularly challenging since many security operators are contracted workers with a high turnover rate. The result is a costly and time-consuming training and certification process which must cover complex procedures and a variety of security systems from multiple vendors - each with a different look and feel. And still, this does not ensure that procedures and response will be followed and acted upon.

Increased Threats and Risk

The electric utility industry faces more threats than ever in the form of terror, crime, vandalism and, increasingly, costly copper theft:

- As potential terror targets, the ramifications of damage to the bulk electric system could be severe
- Crime, sabotage and vandalism are no less of an issue. Not only costly to replace or repair, these incidents can affect the service provided by organizations to the surrounding population and impact public image
- With a direct correlation between the price of copper and the rate of theft, incidents of copper theft are on the rise as the price of copper has reached an all time high

Complex and Ever-changing Reporting Requirements

An ongoing challenge to electric utilities is creating a verified audit trail and having a proper reporting mechanism. While crucial to regulatory compliance, debriefing, investigation and prosecutorial actions, reporting is also extremely time-consuming, costly and damaging when done inaccurately.

PHYSICAL SECURIT Y AND NERC CIP

With NERC's requirement to develop and enforce mandatory reliability standards, new and increasing threats make regulatory compliance even more necessary. Additionally, the costly penalties associated with non-compliance are prohibitive, and can be up to $1 million per day. While significant attention and resources have been devoted to the compliance of the cyber security aspects of NERC CIP, given the potential consequences of the above listed threats, physical security should be considered with as much focus. In the following section, we will show you how Qognify solutions were designed to respond to the electric utility industry's challenging environment, mitigate threats NERC CIP compliance.

HOW QOGNIF Y SITUATION MANAGEME NT SOLUTIONS DELIVER NERC CIP COMPLIANCE

Situator, the leading Situation Management solution, integrates and correlates information in real time from multiple and diverse systems across the enterprise. At the same time, it coordinates the most effective and compliant responses, ensuring that everyone in the security management and operational chains know what is happening, where it's happening and how to respond.

Qognify Solution Highlights

Meeting the business challenges faced by modern electric utilities, Situator:

- Consolidates and manages the vast amount of data flowing into control rooms from all connected security systems
- Automates processes to ensure consistent event response
- Helps organizations meet and sustain regulatory compliance requirements – even dynamic requirements such as NERC-CIP

Qognify

Unified Management, Centralized Control

Situator merges all access control systems, video cameras, perimeter protection sensors, geo- location systems, communication systems, web feeds, fire and safety systems, HR systems, other data sources and operating procedures into a single unified platform. Situator then fuses, correlates and prioritizes all data from these disparate systems. At any point, only the most relevant data is displayed on a single intuitive user interface to the operator with clear guidelines, ensuring that the operator has everything needed to manage the situation according to the organization's policies, SOPs (Standard Operating Procedures) and regulations. In a multi-operator environment, Situator ensures that only the right people see the right information resulting in consistent and efficient response as well as freeing up other operators to work on other tasks without interruption. Evolving incidents can be assigned to multiple stakeholders at once, allowing operators to collaborate on managing an incident. One example is assigning tasks or sharing information between the physical and cyber security teams in while handling incidents.

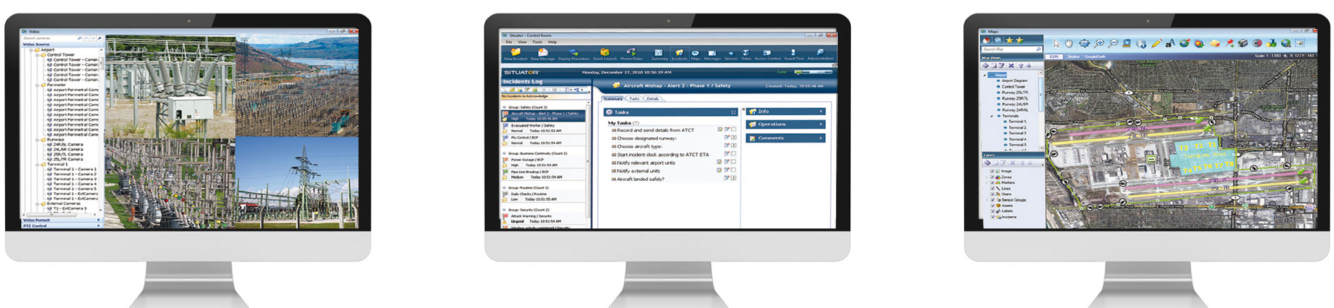

Figure 1: Identifying what happened, where it happened and what to do in Situator

Consistent Event Response and Exception Management

Situator is able to identify potential — or unfolding — situations by intelligently connecting the dots between seemingly unrelated events. Furthermore, Situator enforces processes, automates specific tasks and complex workflows, and intelligently adapts them as an event unfolds to reduce the risk of human error. This not only ensures that the right action is taken at the right time by empowering organizations and their personnel to make consistent, effective and informed decisions, it also ensures compliance with NERC CIP regulations. The exception management principles inherent in Situator make it possible to design modular response workflows that can adapt automatically or on-demand as situations develop. Featuring an industry- leading intelligent correlation engine, Situator is used to correlate security, safety, IT and operations data streams. Based on customer configurable business logic, suspected patterns are evaluated and appropriate alerts are generated, presented to the user, and trigger pre-configured workflows. Situator supports both the definition of business rules and dynamic workflows. Business rules are easily definable through a graphic wizard. Dynamic workflows are designed using a Microsoft Visio like drag-and-drop Graphical User Interface, allowing logical elements and actions to be configured by the administrator to create virtually any custom business logic required.

Anatomy of a Situator Incident

In Situator, an incident occurs:

- Automatically when triggered by sensor alarms (rule based)
- Automatically via scheduled time-based triggers
- On-demand via —Quick Launch|| buttons which enable operators to quickly and easily trigger predefined actions when responding to emergency situations or to automate routine actions.
- Typical automatic activation examples are: sending notification to responders and command post; generating reports; activating announcements; commanding external systems according to regular daily schedules; etc.

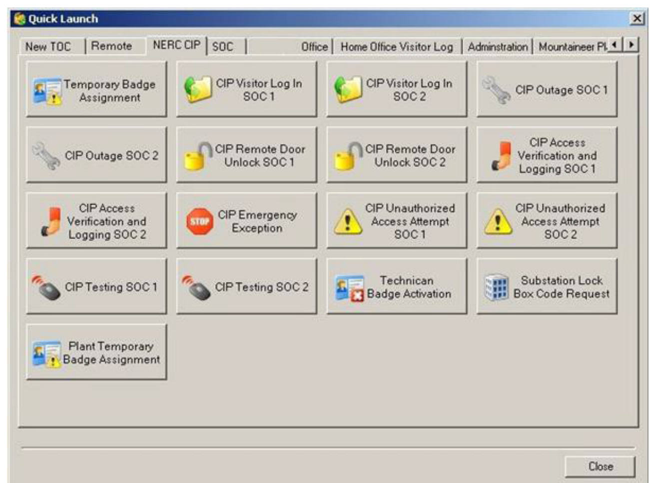

Figure 2: A sampling of NERC-CIP related Quick Launch buttons in Situator

Situator correlates all incoming data, analyzes an unfolding event for immediate situational awareness, and automatically presents all relevant information, procedures and workflows in a consistent, pre-defined response to the operator in the Incidents view. Operators are directed to handle relevant incidents when they receive situation alerts in the form of popup notifications

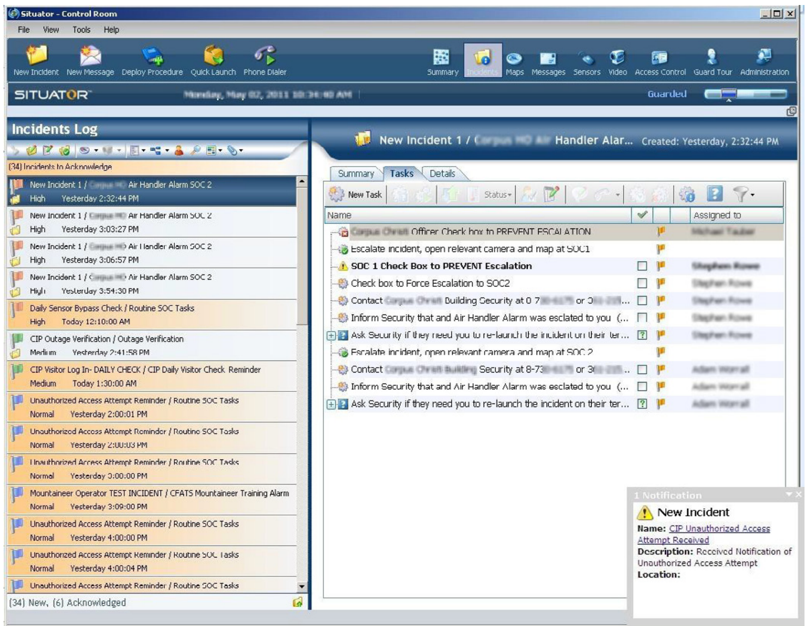

Figure 3: NERC-CIP related new incident popup notification alert

In addition, Situator provides a highly flexiblemechanism for incident escalation definition and management.

NERC CIP Requirements that Can Be Implemented in Situator

Below are some examples of various NERC CIP requirements that can be automated by Situator:

- Procedures for immediate review and handling of unauthorized access attempts such as: door forced open, multiple unauthorized card swipe and others (NERC CIP-006 R5)
- Workflow for the review of access authorization requests and revocation of access authorization (NERC CIP 006 R1.5)
- Implementation of response plan, handling procedures and communications plans (NERC CIP-008 R1) In addition, Situator provides a highly flexible mechanism for incident escalation definition and management.
- Automated classification and characterization of incidents by correlating security alerts with geographical information (GIS) and other relevant information such as time of day (NERC CIP-006 R1.1)
- Workflow for logging and maintaining visitor access logs via phone calls to SOC at remote sites that are routinely unmanned, eliminating the need to maintain paper logs on-site (NERC CIP-006 R1.6.1)
- Procedures for maintenance and testing by control room operators and on-site personnel (NERC CIP-006 R8)
- Implementation of incident reporting process (NERC CIP-008 R1.3

Examples of General Procedures Embedded in Situator

Below are some examples of general standard (security and safety) operating procedures that are embedded and automated by Situator:

- Penetration of the secured facility's perimeter
- Assault with a firearm
- Person in restricted area
- Sensor failure
- Duress button activation
- Disconnected gateway
- Door held open
- Cooper theft
- Shelter in place
- Smoke and/or fire
- Chemical spill
- Explosion of a gas pipe

Situation Management and the Electric Generation/Transmission Control Rooms

Situator's capability to connect multiple systems in order to unify different sources of information is not limited to just the security control room. Rather, it can also be used in other control rooms. One example is the electrical grid (transmission) or the electrical generation control rooms. Situator integrates different operational systems such as SCADA, Historians, Energy Managements Systems (EMS) and others and consolidates the information that needs to be presented to the operator, and identifies important alerts or situations. In the event that a response is necessary, Situator uses its advanced tasks and workflows capabilities to guide the operator on the specific tasks that need to be performed.

Situator Deployment in an Electric Utility SOC

The results achieved by one of the nation's largest electric utility providers spanning across 11 states illustrates the effectiveness of using Situator to meet and sustain NERCCIP compliance. This well known US IOU (investor-owned utility) leveraged the Qognify solution to implement its physical security plan and maintain their NERC-CIP compliance. By unifying their security platform, the IOU Security Operations Center has:

- Gone from managing 14 sites to 350 without increasing personnel
- ncreased efficiency and reduced event-handling time by 60%
- Integrated and centralized more than 5000 sensors
- Self-added more than 2000 security procedures
- Reduced new operator training time from 10 weeks to 5 weeks
- Ensures NERC CIP physical security compliance at all times

Meeting NERC CIP Personnel and Training Requirements (CIP-004)

NERC CIP also contains requirements around personnel and training, which are usually managed by HR systems and other applications. Situator can integrate with those HR systems, access control systems and other systems in order to automate certain actions and to report on the status of personnel and training compliance policies. This provides a more complete view of the NERC CIP compliance status within the organization.

Situator NERC CIP Capability Highlights

Situator implements NERC CIP physical security policies and ensures they are consistently followed by control room operators no matter what their experience or expertise. As an open solution, Situator was designed to integrate with legacy systems of all kinds and at the same time is ready for future technology, requirements and regulations to meet the evolving needs of the electric utility industry.

Situator provides many NERC CIP compliance capabilities as illustrated by this partial list:

- The Situator planning tool enables customers to create multiple incident types
- Tasks and procedures can be adjusted to specific sites
- Situator ensures that policies are consistently followed by control room operators
- For each procedure, a time-stamped report is automatically generated detailing tasks/actions performed by the control room operator
- Reports can be generated in PDF format, and serve as evidence of compliance during audits
- The Situator Task Scheduler automatically reminds responsible personnel of deadlines for review/exercise/testing to ensure they are not overlooked
- Situator automatically informs managers, relevant personnel and cyber security teams of incidents and their status by using email, SMS and mass notification systems
- Incident documentation is easily managed with reporting capabilities that consolidate all the relevant information into a single incident report

The process of using Situator to meet NERC-CIP compliance is illustrated in Figure 4.

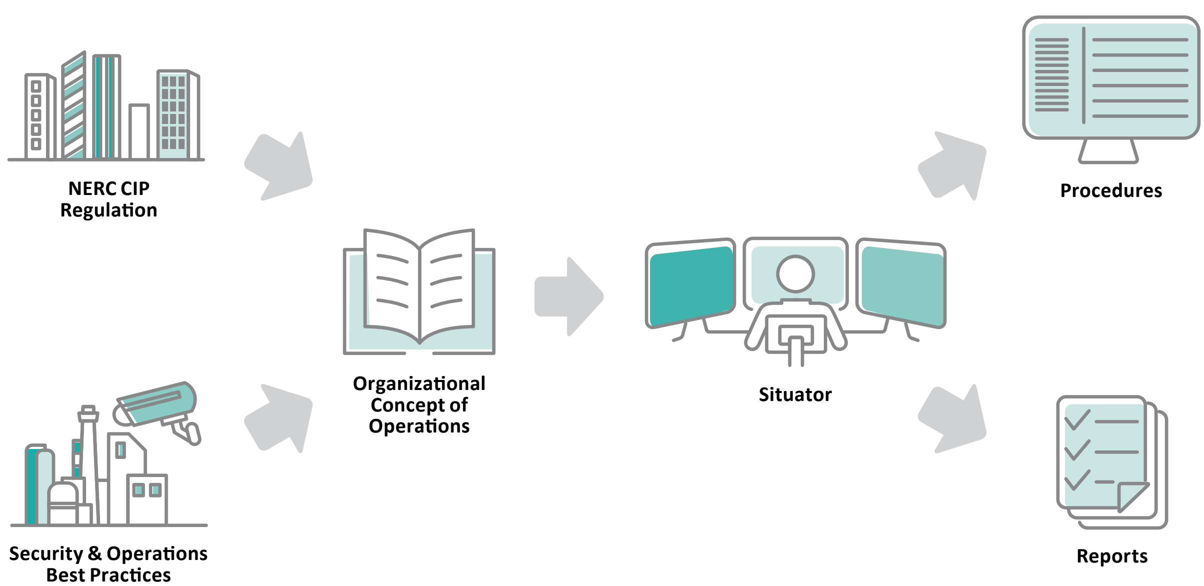

Figure 4: Complying with NERC-CIP using Situator

SOLUTION PAPER

Situator — Physical Security Compliance Automation

Situator's comprehensive and multi-layered approach to addressing the needs of the electric utility industry is based on decades of experience providing solutions for some of the world's most security conscious environments and locations. Its proven technology and capabilities are in continual use, ensuring the security and compliance of organizations throughout North America and across the world. With a completely integrated and unified platform where tasks, procedures, and responses are pre-planned, often automated and always recorded, compliance and reporting can become a seamless event for the electric utilities industry with Situator.

SP-67-02 07/2016

CONTACTS

info@Qognify.com
info.americas@Qognify.com
info.emea@Qognify.com
info.apac@Qognify.com

Qognify