A rich track record of innovation and client service for power and utilities companies

Deloitte….

- provides financial audit and advisory services to over half the utilities in the U.S.
- has provided security and compliance services for more than 25 public and privately held power and utility companies in North America since 2010
- maintains a technical configuration library of dozens of pre-built monitoring use cases for NERC/FERC ICS environments
- maintains pre-built SIEM data collection integrations for dozens of models of proprietary control devices
- provides custom threat awareness services to energy industry leaders, helping to maintain ongoing, proactive visibility on emerging threats across the sector.

Advisors, solution architects and project teams with rich experience in the power and utilities industry

Steve Livingston, CISSP, CISM
Principal
Cyber Risk Services
slivingston@deloitte.com

Steve brings 20 years of information security consulting and auditing experience, focused on advanced security monitoring solutions. He currently leads Deloitte's cyber risk services in the Power & Utilities sector. Steve has over 15 years of experience leading client teams on large, global implementations of SAP, Oracle and Siebel. He also led the development of Deloitte's ArcSight for SAP solution, and co-developed Deloitte's smart grid security offerings. Steve received his MBA in Management and Information Systems from New York University's Stern School of Business.

Ray Soriano, CISSP, CISM, CSSLP, CISA
Director
Cyber Risk Services
rsoriano@deloitte.com

Ray is a senior leader of Deloitte's Cyber Threat & Vulnerability Management service offering within Deloitte's Power and Utilities sector practice. He has over 24 years of professional experience in the areas of cyber security, network systems design and implementation. On a national basis, Ray is responsible for providing integration services for distributed systems infrastructure solutions and information protection consulting services.

Sharon Chand, CISSP
Director
Cyber Risk Services
shchand@deloitte.com

Since 1996, Sharon has been assisting clients with design, implementation, and management of security solutions for global clients. Through this work, she has gained broad experience across many security domains, including identity & access management, regulatory compliance, threat & vulnerability management, security strategy & planning, security policy & standards, risk assessments, and data protection. She is focused on the Power & Utilities industry, and has led cyber risk and NERC CIP compliance efforts for one of the largest U.S. utilities since 2008. Sharon received her BS in Electrical Engineering from Purdue University.

David Nowak, CISSP, CIPP
Senior Manager
Cyber Risk Services
danowak@deloitte.com

David has over 15 years of experience in information security focusing on the Power and Utilities sector. David has designed and implemented enterprise security solutions in a wide range of areas including security event management, identity management, network access control, and privacy. David has experience in developing business cases articulating the business needs, requirements, costs / benefits for security strategies. He has developed regulatory compliance programs including NERC CIP and Payment Card Industry Data Security Standard (PCI DSS).

*All individuals represent Deloitte & Touche LLP

This document contains general information only and Deloitte is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this document.

About Deloitte

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Deloitte.

Keeping the lights on
Defending rate payers against the impact of targeted cyber attacks

In November of 2014, Admiral Michael Rogers, commander of the U.S. Cyber Command and director of the National Security Agency, warned of the need to prepare for cyber attacks aimed at critical infrastructure, identifying the electric grid as potential target.[1]

The possibility of such attacks was first made clear in June of 2010, when a sophisticated worm called Stuxnet was discovered in Iranian nuclear facilities with the specific intent to cripple SCADA systems. The incident demonstrated that cyber threats can target the sensitive industrial control systems at the heart of many critical utilities and other public services. SHODAN, Havex, and other malware have been propagating throughout the commercial energy industry. Although utilities have been subject to NERC CIP and other security-related regulations, many remain unprepared to address this new and evolving generation of threats.

Deloitte offers specialized cyber risk services designed to help protect your critical generation, transmission and distribution systems.

[1] "U.S, Power Grid and Infrastructure Vulnerable to Foreign Cyber Attacks, NSA Director Warns," *Newswire.net,* November 21, 2014

Deloitte.

Cyber risk is a business issue

Cyber attacks against utilities are becoming more targeted, but defenses lag.

• • •

The *Verizon 2014 Data Breach Investigations Report – Energy and Utilities* notes that in 2013 the energy sector was hit by significantly greater numbers of web application attacks, crimeware, Denial-of-Service attacks, and cyber espionage than the all-industry averages. 38% of energy and utilities incidents were web application attacks, almost two-thirds of which were enacted by groups with an ideological motivation to disrupt, rather than to commit a financial crime.

• • •

The *ICS-CERT Monitor, May-August 2014* reported that at least four vendors of industrial software had been compromised by Havex, a malware capable of gathering information about connected control system resources.

• • •

According to *2014 Strategic Directions: U.S. Electric Industry*, a report by Black & Veatch (http://bv.com/reports/electric), 48% of electric utilities surveyed said they do not have the "proper segmentation, monitoring and redundancies" needed to protect against cyber threats.

While NERC regulations have been around for several years, and many utilities have adequately complied with them, others still lack a sufficient cyber defense capability — or at least one likely to give true confidence to boards, regulators and rate payers. So as threats to the grid have increased in number and sophistication, public confidence has begun to erode.

Power and utilities companies face unique security challenges.

The complex connections between SCADA, smart grid, advanced meters, intelligent substations and new customer systems increase cyber risk and make detection and monitoring especially challenging. As we saw with the Stuxnet incidents, cyber criminals exploit vulnerabilities in the control system software. Although product manufacturers are increasingly diligent in releasing updates to resolve these problems, companies often decline to install the new software releases for fear of destabilizing the infrastructure, leaving significantly vulnerabilities unattended. Monitoring can be a critical stop-gap measure, but skills to build these solutions are in short supply.

Point solutions don't solve the problem.

Tools that monitor single components of the infrastructure often fail to detect cyber threats. Why? Because malicious actors use strings of seemingly unrelated tactics to gain access to what they're after, often masquerading as legitimate actors and staying quiet for months. Threat detection requires enterprise visibility – the ability to identify sequences of events by correlating information from many sources, in both the SCADA and corporate IT networks.

Compliance-driven solutions have a short lifespan.

Concerns over customer privacy and grid resilience to cyber attacks lead to continuous, manual review of already burdensome regulations. Changing NERC CIP standards, FERC audit requirements, DHS guidance and Executive Orders, combined with Congressional gridlock, create an atmosphere of constant uncertainty. While demonstrating compliance will always be important, setting sites narrowly on regulatory requirements means you'll always be racing to catch up.

The board is watching, too.

Focus on compliance at the expense of a risk-focused approach may also distract thinly stretched security teams from focusing on what really matters to your bottom line. As pressures mount, boards and governing bodies are putting greater pressure on CEOs to demonstrate they can effectively monitor their infrastructure and demonstrate results. Detailed approaches focused on cyber threat detection help utilities mitigate fundamental business risks – while also streamlining audit-related functions.

AN INDUSTRY-WIDE SNAPSHOT OF CYBER RISK PRIORITIES

ACTORS	Financial Theft / Fraud	Theft of customer data	Customer service disruption	Attacks on critical infrastructure	Reputation damage	Threats to health & safety
Organized criminals	Moderate	Very high	Low	Moderate	Moderate	Moderate
Environmental hacktivists	Low	Moderate	High	Very high	Very high	High
Nation states	Low	High	High	Very high	Low	Moderate
Insiders	High	Moderate	Moderate	Very high	High	Very high
Joint Ventures	High	Low	Low	Low	Low	High

Who wants to attack my utility, and why? Leveraging broad experience across the industry, Vigilant by Deloitte works with you to align a solution to your specific set of risk priorities.

KEY

■ Very high
▩ High
▒ Moderate
□ Low

Advanced Threat Monitoring for Utilities

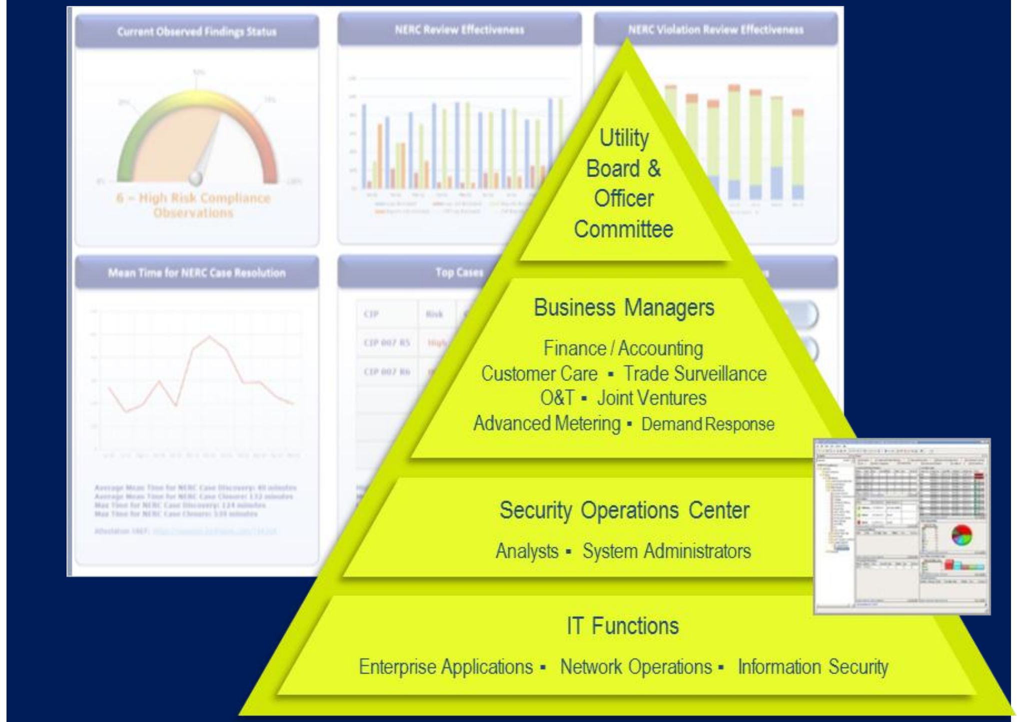
A turnkey solution to protect the grid *and* demonstrate compliance

Advanced Threat Monitoring for Utilities provides broad visibility across critical and IT infrastructures using a library of pre-built cyber monitoring use cases and executive reports designed for Utilities. Leveraging the real-time automation and analytic power of security information and event management (SIEM) technology, the solution equips teams to improve identification of cyber threats and policy violations, optimize incident response processes, streamline audit functions, and provide upstream reporting on Key Risk Indicators (KRIs).

SOLUTION BENEFITS

- *Effectively communicate your cyber security posture* to the board, shareholders, customers, and regulators.
- *Focus limited resources* on what matters most to your business.
- *Get ahead of compliance* and regulatory challenges.
- *Improve security effectiveness* while reducing the need for expensive security retrofitting of existing infrastructure.
- *Support your in-house teams* with the extra skills and specialization they need.

EFFECTIVE CYBER REPORTING – FROM THE NETWORK TO THE BOARD ROOM



Current Observed Findings Status
6 – High Risk Compliance Observations
NERC Review Effectiveness
NERC Violation Review Effectiveness
Mean Time for NERC Case Resolution
Top Cases

Utility Board & Officer Committee

Business Managers
Finance / Accounting
Customer Care • Trade Surveillance
O&T • Joint Ventures
Advanced Metering • Demand Response

Security Operations Center
Analysts • System Administrators

IT Functions
Enterprise Applications • Network Operations • Information Security

Our Power and Utilities cyber risk team knows how to work with your stakeholders: Generation, Distribution, Water, Gas, IT and others. We apply a common risk language that supports your CIP compliance, but also helps shape cyber monitoring.

- Executive reports summarize threats, risks and areas of non-compliance to support effective governance. Risks and cyber threats are illuminated for the first time using simple, system-generated dashboards aligned against the KRIs.
- Management reports support oversight of the people, process, and technology areas required to manage functional aspects of cyber risk within lines of business.
- Security operations reports contextualize alerts and detail events to support cyber monitoring, incident response, remediation and forensics, and enable effective collaboration with other IT functions.

Fusion managed services help you attain more mature security operations and monitoring capabilities – faster.

Cyber risk preparedness lags for many organizations because it can be cost-prohibitive to retain a diverse staff with the wide range of skills needed to keep pace with threats. Deloitte's Fusion team provides a tailored program of support , leveraging our specialized staff to work in tandem with your in-house teams to:

- monitor your environment for cyber threats, provide incident analysis and guide internal remediation efforts;
- tune your monitoring technologies to adapt to changes in business requirements and threat conditions;
- support the development of more efficient security operations processes;
- help you manage NERC/FERC and other compliance requirements.