

# SCADA\_AND\_SMART\_GRID \_SECURITY\_SERVICES

## IOActive's SCADA and Smart Grid Security Services

Security of critical power infrastructure is a top concern to both public and private organizations alike. IOActive has extensive experience in assessing the electrical power control systems found within the grid. From the management, generation, transmission, and distribution of bulk electrical power to manufacturing floors and offshore platforms, we maintain a deep bench of field-assessment experience our clients have come to count on and trust.

IOActive combines its collective expertise in software, firmware, and hardware security assessment to provide a breadth and depth of skill that few other services firms can offer. IOActive employs purpose built, state of the art tools and techniques that are developed specifically for use on sensitive control system networks. Since these tools and techniques have been developed by internal R&D teams and are exhaustively field tested, our clients can be confident in the accuracy and stability of our assessments.

### ■ Smart Grid Security Assessments/Research

The Smart Grid promises a range of benefits, but it is critical to ensure the infrastructure's security, so IOActive is pioneering the industry's efforts at securing the Smart Grid and associated infrastructure. IOActive researchers identified multiple programming errors on a series of Smart Meter platforms ranging from the inappropriate use of banned functions to protocol implementation issues. The research team was able to weaponize these attack vectors and create an in-flash rootkit, which allowed them to assume full system control of all exposed Smart Meter capabilities including remote power on, power off, usage reporting and communication configurations. The initial attack vector could have been leveraged to deploy a worm, much like the Blaster worm that attacked computer systems in 2003.

IOActive briefed the White House on their Smart Grid findings and unveiled this research at Black Hat USA 2009. As pioneers in Smart Grid systems security, IOActive is at the leading edge in providing thought leadership, expert techniques and accurate results in our security assessments. Only IOActive can stand behind proven results that utilities and vendors require.

*"We hope that by informing people that these serious vulnerabilities exist throughout the Smart Grid infrastructure it will prompt vendors to mitigate existing vulnerabilities and increase security in future products."*

**—Mike Davis, Senior Security Consultant**

*"The Smart Grid infrastructure promises to deliver significant benefits for many generations, but first we need to address its inherent security flaws. Based on our research, IOActive believes that the relative security immaturity of the Smart Grid and AMI markets warrants the adoption of proven industry best practices including the requirement of independent third-party security assessments of all Smart Grid technologies that are being proposed for deployment in the Nation's critical infrastructure. We are also recommending that the Smart Grid industry follow a proven formal Security Development Lifecycle, as exemplified by Microsoft's Trustworthy Computing initiative of 2001, to guide and govern the future development of Smart Grid technologies."*

**—Josh Pennell, Founder and President**

### ■ SCADA/PCS Security Assessments

Under the guidance of leading SCADA security experts, IOActive's technical deliverables offer unparalleled insight as we facilitate a deep-trust relationship with power and utility companies throughout the world. IOActive's SCADA assessment is built on information gained from direct penetration testing, architectural code review of utility and power control system, as well as related third-party technologies. Our innovative methodologies and toolsets—built from expert reverse engineering, advanced control logic threat modeling and in-depth protocol analysis—enable us to quickly detect weaknesses and anticipate exploits.

### ■ Assessing CIPS Compliance

Drawing on expertise from regional entity auditors, IOActive offers elite CIPS compliance gap assessments, as well as cyber security and energy management network architecture evaluations. With deep experience in the SCADA security marketplace, IOActive can provide CIPS-compliant vulnerability assessments in even the most sensitive electrical power facilities.



## About IOActive

Passion and pride through quality work is rare these days, which is why IOActive has spent the last decade searching for the required blend of technical expertise and work ethic that comprise a world-class, international security team. We are committed to staying on the cutting edge of technologies and offering unrelenting value—something our customers have come to rely on over the years and can depend on in the future.

Established in 1998, IOActive is an industry leader that offers comprehensive computer security services with specializations in smart grid technologies, software assurance and compliance. Boasting a well-rounded and diverse clientele, we not only provide unparalleled technical services, we also strive to become a trusted advisor to our clients, enabling us to fully understand and help them achieve their business and security goals.

As a home for highly skilled computer security professionals, IOActive attracts the likes of Dan Kaminsky, Richard van Eeden, Ilja van Sprundel, Mike Davis, Tiller Beauchamp, Walter Pearce and Wes Brown. We also boast key advisors like Steve Wozniak and Jason Larsen, luminaries who affect how security and technology shape our world. IOActive's vast industry experience consistently helps our clients stay ahead of tomorrow's threats.



### Contact Information:

[info@ioactive.com](mailto:info@ioactive.com)

206.784.4313

SCADA\_AND\_SMART\_GRID\_SECURITY\_SERVICES

[www.ioactive.com](http://www.ioactive.com)