



Independent Electricity Systems Operator (IESO) Protects Ontario's Power Grid with TippingPoint IPS

The Challenge: The Independent Electricity System Operator (IESO) works at the heart of Ontario's power system, connecting more than 300 participants, including generators that produce electricity; transmitters that send it across the province; retailers that buy and sell it; industries and businesses that use it in large quantities and local distribution companies that deliver it to people's homes. The IESO manages electricity between these participants, balancing supply and demand to ensure reliable operation of the provincial electricity grid. Every five minutes, the IESO forecasts consumption throughout the province and collects the best offers from generators to provide the required amount of electricity.

"We have a high level of confidence in our TippingPoint implementation and the Digital Vaccines. The product was easily integrated into our existing environment and is instrumental in helping us meet both our regulatory commitments and strict ongoing operational requirements."

Ben Blakely
Information Security Officer
Independent Electricity
Systems Operator (IESO)

Given the complexity of the IESO's networks – as well as the criticality of the services they provide – it is important for the IESO to secure its networks from all external and internal security threats. In 2007, the IESO's primary defense against security threats was firewalling, anti-virus, manual patching, and investigating events from an aging, legacy IDS system. As security threats increased and became more sophisticated, it was becoming more time consuming for the IESO's IT staff to deal with infected systems and to chase down false positives kicked back by the IDS. Additionally, with the number of vendor vulnerabilities and exploits increasing, it was becoming too challenging to manually patch every system.

"We were spending too much time running around trying to deal with common, everyday security occurrences. If a critical incident occurred, we'd be stretched too thin to be able to remediate it before system performance was impacted," said Ben Blakely, Information Security Officer for the IESO."

In addition to the challenges outlined above, the IESO needed a security solution that helped the organization meet compliance requirements of the North America Electric Reliability Corporation (NERC) and Critical Infrastructure Protection (CIP) standards.

In order to better its security infrastructure and comply with these standards, the IESO began a major project to reposition its approach to operational security management. "We basically started from scratch – we needed to reconsider where the critical cyber assets existed and how we could protect them in an effective and efficient manner," said Blakely.

While a patch management system and updated anti-virus were nice additions to the security infrastructure, the IESO was still looking for a security solution to protect its diverse operating environment with a high level of reliability. It was critical for the security technology to gather data and monitor what was happening on the wire. But even more important, the solution needed to

evaluate that data with pinpoint accuracy to avoid blocking appropriate messages.

The_Solution

In June 2008, the IESO implemented the TippingPoint® Intrusion Prevention System to help identify traffic coming into the network and ensure that malware and viruses weren't getting in. The deployment included a dozen TippingPoint 1200E devices throughout its multi-layered DMZ perimeter, stretching across redundant data centers. While the organization initially ran its TippingPoint IPS appliances in alert-only mode, they quickly moved into full IPS mode. "We haven't had a false positive yet," said Blakely.

The IESO also needed a way to keep its systems safe from vulnerabilities when they couldn't be patched appropriately either because a patch is not available or because the process of patching would disrupt other systems. The TippingPoint solution helps the IESO close the window of threat exposure, protecting its most critical systems from being exploited by viruses, malware and other security events.

"We're responsible for providing reliable power to the entire province. We can't always take critical systems offline to patch them," said Blakely.

"TippingPoint's Digital Vaccine® service allows us to implement filters that provide a 'virtual software patch' at unprecedented speed across our entire security infrastructure. These implementations were executed with absolutely no impact to our critical systems."

NERC compliance also requires organizations to define critical cyber assets and a clearly established Electronic Cyber Security Perimeter

that is designed to detect and prevent infection from malicious software, malware, unauthorized access, etc. TippingPoint is the cornerstone for this cyber perimeter ensuring that nothing comes in or goes out of the infrastructure without being inspected by the IPS.

"We have a high level of confidence in our TippingPoint implementation and the Digital Vaccines. The product was easily integrated into our existing environment and is instrumental in helping us meet both our regulatory commitments and strict ongoing operational requirements," said Blakely.

The_Results

For Blakely, the benefits of the TippingPoint IPS were significant and immediate. Within weeks of the deployment, a virus was released that exploited a vulnerability in Microsoft's Web browser. At the time, there wasn't a patch available. However, the IESO was able to use one of the Digital Vaccine filters to keep the exploit from reaching the IESO's networks.

Today, TippingPoint is one the first lines of defense for protecting the IESO infrastructure from the ever-evolving threats to the organization's operating environment. "TippingPoint is a key component of our Enterprise Threat Prevention program. We are able to leverage the IPS solution to build a robust, highly available system that is configured in such a way that it is almost self-maintaining. The system provides us unprecedented visibility into our infrastructure without substantial human interaction," said Blakely.

Corporate_Headquarters: 7501B North Capital of Texas Hwy. > Austin, Texas 78731 USA > +1 512 681 8000 > +1 888 TRUE IPS

European_Headquarters: Herengracht 466, 2nd Floor > 1017 CA Amsterdam, The Netherlands > +31 20 521 0450

Asia_Pacific_Headquarters: 47 Scotts Road #11-03 Goldbell Towers > Singapore 228233 > +65 6213 5999