nCircle™

The State of Minnesota's Office of Enterprise Technology

Overview

The State of Minnesota's Office of Enterprise Technology (OET) was established under the guidance of the Governor and the State Chief Information Officer, with a charter to deliver effective, efficient and economical government solutions. Chris Buse was named the first Chief Information Security Officer for the State of Minnesota in July 2007. Since his appointment, he has worked to develop a comprehensive enterprise security program that protects the privacy, integrity, availability, and security of citizens' information. OET has led the way in setting new standards and policies for risk management and delivering security solutions that improve the state's security posture, while taking advantage of its combined purchasing power.

New Standards Call for a Centrally Managed Vulnerability and Threat Management Solution

OET created new enterprise policies and standards that require use of a comprehensive vulnerability management program with continuous scanning. An automated vulnerability management and compliance solution was needed to centrally manage IT security, produce metrics enterprise wide and comply with federal and state requirements. "By adopting a common technology with a centrally managed solution, every agency now gets a consistent view of their security level and continuous assessment, without having to manage the back end. This yields tremendous savings for the state, when compared to every agency trying to implement a solution on its own," said Mr. Buse.

Nearly Every Agency in the State's Executive Branch has Now Deployed

OET recognized the need to exert a more centralized control over their IT infrastructure, and establish security as an enterprise-class process within the state; thereby reducing redundancies among the over 70 different executive level state agencies. OET expressed the need for a risk and vulnerability management system that would streamline the exchange of IT information among agencies and produce comparative reports.

One of the first initiatives that was executed against that mandate was to acquire an enterprise-class vulnerability management solution and after an extended evaluation, nCircle's IP360™ was selected. The deployment is now scanning approximately 150,000 networked devices.

According to Mr. Buse, "Nearly all executive branch state agencies are up and being continuously monitored by nCircle's IP360, generating metrics that are enterprise-wide." Mr. Buse has also partnered with the State's higher education system, using nCircle solutions to assess over 50 college campuses. This partnership further leverages a single security infrastructure to save scarce taxpayer resources.

Continuous Scans Help Meet State and Federal Standards

nCircle's solutions allow continuous scanning, helping state agencies achieve compliance with both state and federal security standards, such as NIST 800-53, the Recommended Security Controls for Federal Information Systems. "We are big advocates of continuous vulnerability management. Since our program is based on NIST by default, when the Consensus Audit Guidelines came out, we were already going down that path," stated Mr. Buse. nCircle solutions can be used to help automate many of the Critical Security Controls, outlined in the Consensus Audit Guidelines.

Key Benefits

- Reduced redundancies among the state agencies security programs with the use of an enterprise-class process that could be applied across the state

- Improved insight into security risk with enterprise-wide metrics that delivered comparative results among state agencies

- Met NIST 800-53 requirements

- Supports FISMA compliance while continuously monitoring the state's network

- Savings for the state with the use of a common technology statewide, without each agency having to manage the back end

"By adopting a common technology with a centrally managed solution, every agency gets a consistent view of their security level and continuous assessment, without having to manage the back end; which is where there are significant savings for the state."

— Chris Buse
Chief Information Security Officer
State of Minnesota

Producing Accountability and Reducing Risk with Facts

Publishing state-wide metrics from vast amounts of scan data now helps agencies measure their security posture with real facts. Agencies also can see how their security posture compares to their peers, using metrics such as their Average Host Score. The Average Host Score is the total score of all vulnerabilities averaged across all network devices. Agencies also can drill down to determine which devices are introducing the most risk to the network. Metric reports are now used by multiple levels, from system administrators to IT leaders. "In the past, many IT leaders assumed that everyone had the same risk posture. But with enterprise-wide metrics, it's easy to compare all agencies and hone in on those that need the most help," says Mr. Buse.

Building an Innovative Model for Other States to Follow

The appliance architecture of nCircle solutions is very scalable, yet allows for central management. "A lot of governments only focus on external scanning to meet PCI requirements. What we do is different because we do ongoing assessments of all devices, both inside secure agency networks and externally facing," says Mr. Buse.

"We also created a Small Agency Infrastructure Model that gives us the flexibility to provide vulnerability management and other security services in a shared services environment. "

"The model created by OET's implementation of nCircle solutions has formed a template now used in all internal and external continuous scans to promote and ensure IT security, risk management, and automated compliance." said Mr. Buse. "This is a proven model that other states can easily adopt."

> *The model created by OET's implementation of nCircle solutions has formed a template now used in all internal and external continuous scans to promote and ensure IT security, risk management, and automated compliance. This is a proven model that other states can easily adopt.*

— Chris Buse
Chief Information Security Officer
State of Minnesota

State of Minnesota OET at a Glance

- Approximately 300 employees
- Provides state enterprise services in three critical areas: technical services, oversight services and planning services
- Principal customers include the citizens of Minnesota, state agencies and constitutional officers, public school systems and higher education institutions, and local political subdivisions of the state

About nCircle

nCircle is the leading provider of automated security and compliance auditing solutions. More than 4,500 enterprises, government agencies and service providers around the world rely on nCircle's proactive solutions to manage and reduce security risk and achieve compliance on their networks. nCircle has won numerous awards for growth, innovation, customer satisfaction and technology leadership. nCircle is headquartered in San Francisco, CA, with regional offices throughout the United States and in London and Toronto. Additional information about nCircle is available at www.ncircle.com.

nCircle
info@ncircle.com
www.ncircle.com