Millennium Challenge Corporation uses nCircle Suite360 to Implement Consensus Audit Guidelines: Critical Security Controls for Effective Cyber Defense

Established in January 2002, the Millennium Challenge Corporation (MCC) is a Federal agency designed to work with some of the poorest countries in the world. MCC's mission is to reduce global poverty through the promotion of sustainable economic growth.

MCC's rapid growth caused important network services to become unreliable and many systems to be out of compliance with security best-practices. Dennis Lauer joined MCC as the CIO in late 2007 and was immediately faced with these service, security, and compliance challenges. In Mr. Lauer's view, a controlled, stable environment reduces operational costs, and network service instability and insecurity was completely unacceptable. He faced the challenge of securely rebuilding his domestic and international information systems without interrupting the important business of partnering with developing countries to help provide aid in the form of clean water, new roads, and access to medical care (to name just a few program areas).

MCC spent much of 2008 re-architecting systems to deliver current-generation information technology services to its worldwide constituents while also securing MCC data and computing resources. This transformation included creating a new Security & Oversight Team to develop and implement a risk management program for MCC. MCC also contracted with Iron Vine Security to lead the new team and tasked them with implementing a compliant and risk-based information systems security program, thereby separating the oversight role from the operation and administration role of MCC's IT systems. Iron Vine began with a complete overhaul of the organization's policies and procedures. At the same time, they introduced technologies to support the measurement and reporting of risk metrics so decisions could be made based on risk to the business and operations.

MCC's Security & Oversight Team also went to work improving processes and needed an independent and consistent way to measure risk, ongoing progress, and success. They selected nCircle's Suite360, including nCircle IP360TM vulnerability and risk management system, IP360 MobileTM and nCircle Configuration Compliance ManagerTM (CCM), to support this risk management approach. In mid-2009, the Team began to use the Consensus Audit Guidelines (CAG) to assess the progress of securing MCC systems and installing or improving critical controls. The Team soon realized that the nCircle Suite360 automated the continual assessment of several of the key areas of the CAG, which simplified monitoring and identification of changes in risk. MCC currently uses nCircle solutions to cover the following 6 areas of the Consensus Audit Guidelines:

CONSENSUS AUDIT GUIDELINE		
1.	Inventory of Authorized and Unauthorized Hardware	✔
2.	Inventory of Authorized and Unauthorized Software	✔
3.	Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers	✔
4.	Secure Configurations of Network Devices such as Firewalls, Routers, and Switches	✔
8.	Controlled Use of Administrative Priviledges	✔
10.	Continuous Vulnerability Testing and Remediation	✔

"Because we measured risk and provided metrics we were able to focus attention where it was most effective and that helped drive down our overall risk."

-William Geimer, President, Iron Vine Security , Program Manager for Millennium Challenge Corporation

"Millennium Challenge Corporation achieved some immediate benefits with nCircle. For the first time, we had an accurate and continuous view of our risk and the level of compliance we were achieving with our key regulations—letting us focus our efforts where it matters the most."

-Dennis Lauer, Chief Information Officer, Millennium Challenge Corporation

CONTINUED ON NEXT PAGE

Inventory of Authorized and Unauthorized Hardware

MCC uses nCircle to produce an automated, complete inventory of systems on the network as both nCircle IP360 and CCM can agentlessly scan any IP-enabled device, including servers, desktops, laptops, routers, switches, printers, voice over IP telephones and firewalls.

MCC leverages nCircle's capabilities of using multiple ways of correlating hosts across scans, including IP address, MAC address, host name, stack fingerprinting, open port fingerprinting, and NetBIOS name to ensure the discovery process are accurate. This optimizes the ability to track a host over time and identify new hardware on the network.

Inventory of Authorized and Unauthorized Software

MCC uses CCM to catalog all installed software, including operating system (and patch level), applications (with versions) for all workstations, servers, and laptops. The software also has the ability to detect the presence of anti-virus software, what signature version is in use, and how many are out of date.

CCM supports a flexible centralized credentials management system to make authenticated scanning usable in a large, complex environment, and MCC has taken advantage by using nCircle CCM to augment their asset inventory information. For example, they are now able to create queries such as "how many Dell systems with less than 3GB of memory do we have" and "how many copies of Adobe Acrobat are in use?"

Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers

Secure Configurations of Network Devices such as Routers and Switches

MCC went through a refresh of all desktops and laptops to include a standard image compliant with the Federal Desktop Core Configuration (FDCC). FDCC compliance requires the ongoing auditing and verification of over 500 technical controls. As part of the rollout, the Security & Oversight Team used the FDCC policy that ships with nCircle CCM and now performs ongoing, iterative testing to make sure the devices stay FDCC-compliant.

In addition to testing against the FDCC standard, MCC has also used CCM to evaluate their routers and switches against the Cisco standard. MCC used the nCircle Policy Engine to create group policies for the ongoing monitoring of other devices and relies on CCM for configuration variance reports to highlight any deviations from their standards or approved build for each system on the network.

Controlled Use of Administrative Privileges

MCC uses nCircle Suite360's auditing capabilities of user rights and privileges across all major devices in the enterprise and uses nCircle's granular role-based access control to assign rights in a "least privileged" framework, restricting configuration, scan, reporting and remediation access to those hosts and networks as dictated by internal policies.

Continuous Vulnerability Testing and Remediation

MCC is scanning with nCircle IP360 daily to assess all systems on the network. nCircle updates signatures at least weekly, and MCC downloads new software and signatures as they are released. MCC relies on the nCircle method of discovery, only testing the system for vulnerabilities that are relevant to the particular version of the application and OS, for accuracy in discovery. They also utilize the bandwidth shaping capability to have minimal impact on the distributed global network.

MCC takes advantage of granular vulnerability scoring, including CVSS scores for prioritization purposes. MCC also uses IP360 to measure the performance of the Operations and Maintenance Team's patch management process and utilizes remediation verification scanning to verify patches are applied and the vulnerability is actually eliminated.

MCC utilizes regular and objective nCircle reporting to keep all teams and management informed about ongoing compliance and risk metrics. MCC runs reports that summarize vulnerability scores by department and location, and they go a step further by mapping the average host score to a letter grade to create a report card for executives. Differential reporting, or "back-to-back tests", provides insight into specific changes. Executive reporting supports departmental comparisons and timeliness of responses.

85% Reduction in Risk Score in the First Year

When MCC began using nCircle Configuration Compliance Manager to measure FDCC compliance, most desktops and laptops were 30% compliant; today they are 100% compliant. Additionally, with consistent measurement and focus the Security & Oversight Team was able to improve vulnerability risk scores by 85%, driving down the average host score (a measurement of cumulative vulnerabilities) from an average of 27,000 to less than 1,700. MCC has been able to close over 95% of open FISMA audit items and has deployed new secure FDCC controls to 100% of its systems worldwide. nCircle solutions provided the tools the team needed to continuously identify non-compliant systems and prioritize remediation.

Real, Measurable Security

MCC has embraced the core tenet of the CAG by implementing technology that can automate assessing IT systems and configurations against secure baselines. As a result, its reward is not shelves of binders and paper but real, measurable security that protects agency assets and data. With nCircle's suite of technology, MCC identifies weaknesses, manages compliance, and reports regularly to ensure the clear communication of risk to the agency.

nCircle

SANS

About nCircle

nCircle is the leading provider of automated security and compliance auditing solutions. More than 4,000 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.