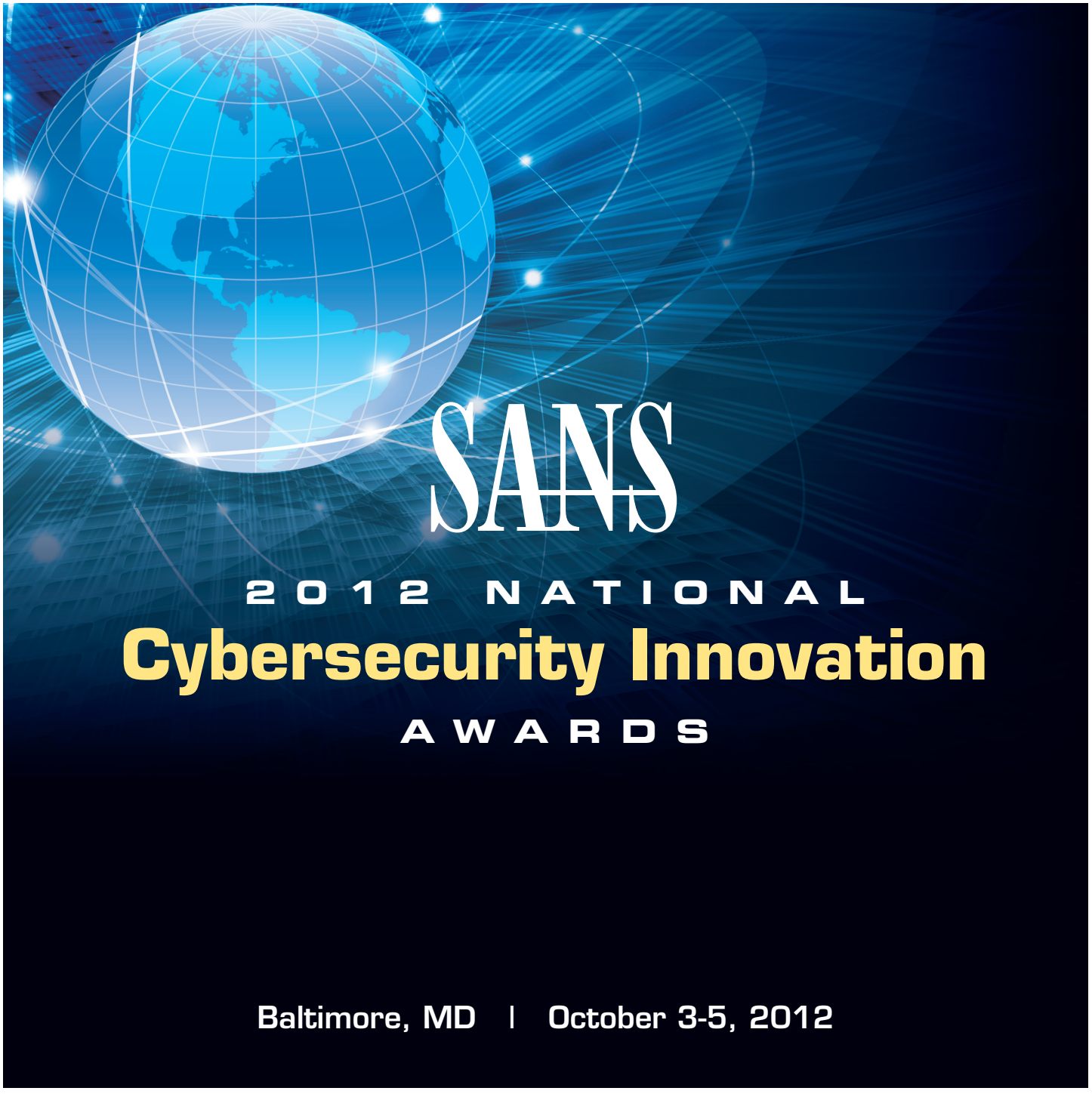

SANS
2012 NATIONAL
Cybersecurity Innovation
AWARDS
Baltimore, MD | October 3-5, 2012

SANS

2012 NATIONAL

Cybersecurity Innovation

AWARDS

TABLE OF CONTENTS

Innovation:

Exploiting the kill chain to block both intrusion vectors exploited in nearly all targeted intrusions nicknamed APT

Department of Industry, Innovation, Science, Research, and Tertiary Education – Australian Government

A year ago, SANS presented a National Cybersecurity Innovation Award to the Australian Defence Signals Directorate (DSD) for its identification of four key cybersecurity policies that, when implemented, can reduce an organization's threat exposure by up to 85%. This was a major discovery and well deserving of recognition. However, two core issues remained: 1) achieving that remaining bit of vulnerability reduction (the so-called 15 percent gap) required an additional 31 security policies, and 2) an Australia-sized chasm separated the delineation of security "policies" and their practical, operational implementation.

Over the past couple years, Australia's Department of Industry, Innovation, Science, Research, and Tertiary Education (DIISRTE) set out to finish the job – discovering and documenting, the first-ever practical operationalization of DSD's Top 35 Mitigation Strategies. The crux of DIISRTE's innovation is a method for the leveraging and retraining of existing security resources and technologies. Typically, organizations expect their software to perform immediately out of the box. Instead, professionals should configure their software to seal-off vulnerabilities by limiting unnecessary capabilities, minimizing unnecessary user privileges, creating white lists, and finding clever ways to ensure users keep their software updated. In particular, DIISRTE discovered new ways to customize Symantec's Endpoint Protection (SEP) software in the service of DSD's Top 35. Through proper configuration of SEP alone, DIISRTE was able to complete 7 of the 35 controls.

Leveraging their current software to meet requirements was only a piece of the solution. DIISRTE was also key in cultivating change within their IT organization by providing training as well as ensuring administrators were granted only the permissions needed and disabling rights that were not required. Perhaps most significantly, DIISRTE has written a Practical User's Guide for partner organizations – which goes far beyond mere technical documentation, and outlines the practical steps for replicating DIISRTE's successes. Not only has DIISRTE's approach to the Top 35 been a road map for other Australian organizations including the Defence Signals Directorate, but organizations across the globe can learn from this and soon be able to drastically reduce their vulnerabilities – without any significant investment.

Innovation:

Rapid risk reduction through automated continuous monitoring at ultra low cost

NASA Ames Research Center

NASA Ames Research Center proved that the power of continuous monitoring and mitigation, first seen at the State Department, could be easily and inexpensively replicated even in a smaller agency. NASA Ames altered their vulnerability detection program to bring responsibility directly to the sysadmins and technical staff - those who can actually fix problems. By normalizing and tabulating CVSS vulnerability scores for each host and cross-referencing hosts to our asset inventory, they produced a "scoreboard" showing which hosts, (and which system administrators), are security heroes - and which are security zeroes. The scores are further modified by scanning the agency constantly from a truly external server, and adjusting scores upward when vulnerable hosts have services exposed beyond agency firewalls. The sysadmins responded immediately and positively, The system has now spread to most NASA Centers and the entire cost was two programmers and some management oversight.

The database of external scan results is retained and updated monthly for quick searching when questions arise as to which emerging vulnerabilities are exposed to potential attackers in the 1st defensive layer. The scoreboards are updated weekly and available to ALL syadmins to view their own score in relation to those of their peers.

From the very first week, vulnerable systems either were turned off (they had apparently not been needed) or fixed. The agency security staff (via ability to lookup exposures) and the system administrators (via ability to quickly gauge where to spend their limited time on security hardening) have both benefited from the tool. Additionally there is now strong incentive for sysadmins to correct deficiencies in the asset database, to normalize their scores and they are responding.

Innovation:

Using continuous automated monitoring to radically reduce the risk of cyber attacks against confidential citizen health data

The Centers for Medicare & Medicaid Services
Dept. of Health & Human Services

The Centers for Medicare & Medicaid Services (CMS) comprise information systems in nearly 200 data centers, processing claims and payments with a value of over $800 billion each year, for medical services rendered to over 100 million program beneficiaries and recipients. The vast majority of CMS confidential citizen data is stored and administered by a complicated network of 38 contractors, across nearly 200 sites, obliging CMS to educate, train, and guide each of these contractors to produce, and make effective use of, compliant Cyber Scope feeds.

CMS designed a process to leverage the data collected internally, creating an agency-wide, proactive risk reduction program designed to continuously improve security across their network of contractors and data centers. CMS developed and implemented a system that ingests data collected from sites, prioritizes the findings, and then creates easily interpreted reports to help system owners take the highest value mitigation steps required for rapid and efficient remediation of the most serious cyber security weaknesses.

To effectively monitor and reduce risk across the widely disbursed network of CMS and contractor sites, CMS first developed a process to assess the relative security of each datacenter and normalized these security scores across the variety of security tools providing the feeds. The product is a single, cohesive, apples-to-apples scoring solution that pinpoints critical risks, provides remediation information, and creates visibility in a manner that drives rapid remediation responses. CMS demonstrated initial success with this system in 2010 by developing a vulnerability risk scorecard and letter grading system to foster healthy competition and engage business owners. Through this program, CMS reduced the average host risk scores at two high data centers by over 68% between July 2010 and January 2011.

By creating a positive competitive spirit, CMS motivated contractors to succeed in reducing risk across CMS entire nationwide system footprint. The lessons learned by each contractor during this process immediately resulted in the reward of helping sister programs achieve similar results at a minimal incremental cost, and CMS has since applied this repeatable and proven CMRS framework to their most visible system, the newly created Affordable Care Act Health Insurance Exchanges.

Innovation:
A big step forward toward a global minimum standard of due care in cybersecurity: guidance for implementing the 20 Critical Controls

The Centre for the Protection of National Infrastructure (CPNI)
National Technical Authority for Information Assurance (CESG)

Organizations that are implementing the 20 Critical Controls can look to guidance and education developed by the National Technical Authority for Information Assurance (CESG) and the Centre for the Protection of National Infrastructure (CPNI). CESG pulled from CPNI's work on the 20 Critical Controls to develop "10 Steps to Cyber Security," a launching pad for CISOs and their teams.

This initiative marks the first time multiple national governments (the UK and US) have come together to agree on answers to the three questions most often aksed by industry and government leaders about cybersecurity:

1. What is needed to secure our systems?
2. How much is enough?
3. And whom can we trust to answer the first two questions?

CPNI didn't create its own answer, but joined the US (DHS and NSA) in backing and improving a single global benchmark. Their cooperation led to the formation of an International Consortium on Critical Security Controls of governments and the largest multinational user organizations, led by Tony Sager who recently left a top job at NSA, to ensure the Critical Controls continue to be the authoritative answer too those three questions, leading to rapid adoption and much greater security at lower costs for all participating user organizations.

Innovation:
Raising the bar in collegiate cybersecurity education

Associate Directorate for Education and Training, National Security Agency

and

Dakota State University

Northeastern University

Naval Postgraduate School

University of Tulsa

Although very few colleges have been graduating technically proficient and highly skilled students to fill the need for cyber operations missions, in the past year, the National Security Agency created a higher standard for colleges in cyber security operations and an innovative new incentive system that schools are competing to meet.

For institutionalizing the process that enabled this program, and for rising to the very high new standard, the NSA ADET organization and the first four schools to be designated CAE-Cyber Operations schools – Dakota State University, Northeastern University, Naval Postgraduate School and University of Tulsa - are jointly awarded the 2012 National Cybersecurity Innovation Award. Other federal agencies with substantial cybersecurity responsibilities involved in hiring from the CAE schools have seen what is possible and are encouraging schools from which they recruit to raise their standards to a level nearly as high as the one deployed at the four model schools.

Innovation:

Educating senators and other policymakers on the actual cyber threat through demonstration

US Department of Homeland Security

In an effort to make the complex technical issues surrounding cyber security policy debates accessible and concrete to senior level executives who may not have technical cyber backgrounds, the Department of Homeland Security developed a 20 minute live action demonstration of a real cyber attack.

The demo shows how hackers can use free, "open source," tools that are widely available on the Internet to launch a spear phishing attack that can steal or manipulate files, take over control of a computer, crack confidential passwords, and even covertly spy on a victim through their webcam and microphone. The demo then illustrates how intrusion detection and prevention software work to protect the boundaries of Federal networks and can stop malicious actions in real time.

By having the roles of victim and attacker "played" by different individuals using separate computers whose screens are displayed on large televisions, the audience can easily see the attack occur in a more realistic way than conducting the entire display using virtual machines on the same computer.

By utilizing free software that is available on the web, the demo also conveys that attackers do not necessarily need the sophistication to develop unique malware in order to successfully infiltrate and exploit a system where known vulnerabilities remain unpatched. The demo not only shows the importance of good cyber hygiene, but also provides an opportunity for a larger discussion of DHS's work to protect Federal networks, analyze malware, and distribute effective security guidance to private sector partners.

The demo is built to be unclassified and repeatable within minutes. It has been shown to many audiences, including senior Administration officials, congressional members and staff, and the press. It will continue to play an important role in the Department's efforts to educate Congress and the public about the seriousness of cyber security threats and the need for smart policy.

Innovation:
NSA shows how to combat APT with convenient, transparent non-persistent desktop browsing

National Security Agency
Information Assurance Division

The promise of non-persistent desktop browsing (NPDB) has long been just that – a promise, but NSA has now made it real. It is an emerging technology that effectively addresses the rapidly increasing security threat stemming from malicious software (malware) used by nation states, cyber crime, and rogue actors, to socially engineer people browsing the Internet, in order to attack and penetrate systems and networks, and ultimately exfiltrate valuable information for profit. Recently, the Department of Defense conducted a successful Joint Capabilities Technical Demonstration (JCTD) as part of a pre-acquisition activity for the Joint Chiefs of Staff to prove the viability of this technology and to speed the discovery, development, and delivery of non-persistent browsing technology to the Department of Defense Information Enterprise.

The NPDB technology was proven during an Operational Demonstration (OD) at the Special Operations Command (U.S. SOCOM) on a production network, and simultaneously on an isolated laboratory network at the Cryptologic Systems Division. The OD was structured to present NPDB as a virtualized instance of an Internet browser that would co-exist on an enterprise desktop alongside the native browser. When the user opened the native browser to engage the Internet, the NPDB version would trigger and provide a seamless non-persistent browsing experience on the Internet while isolating the operating system of the host from any threats that may be encountered. If the virtual browser is compromised, non-persistence is realized and all artifacts affected by the compromise are immediately eradicated.

Innovation:

Proving that defenders can work together to improve security; combating APT through real time sharing & development of the Master Block List (MBL) tool, which allows multiple labs and plants to share block information in real time.

Focused Advanced Persistent Threat Group
Lawrence Livermore National Laboratory
Department of Energy

The Master Block List (MBL) is a tool developed by the Department of Energy's Focused Advanced Persistent Threat (FAPT) group led by Lawrence Livermore National Laboratory (LLNL). MBL allows any application to be easily hooked, to automatically share up to the minute data on malicious websites, hashes and spear phishers, with all those that participate in the MBL, and allows multiple labs and plants to share block information in real time. Through the use of tools like MBL, DOE is increasing its ability to leverage the intelligence of the collective as opposed to the fragmented, individual pieces.

The work for MBL largely took place in Livermore, CA at Lawrence Livermore National Laboratory (LLNL) and partially in Albuquerque, NM at Sandia National Laboratories (SNL). MBL is in use by 10 other organizations (within the DOE) and is rapidly growing. The innovative idea, with MBL, was that sharing didn't have to be complicated and that we could adopt methods used by our adversaries to create a protocol that would function in any environment. This innovation helped us overcome the segregated nature of cyber security across DOE organizations. In an effort to improve our network defenses, LLNL blocks an average of 50 domain and/or IP addresses daily from other MBL participants.

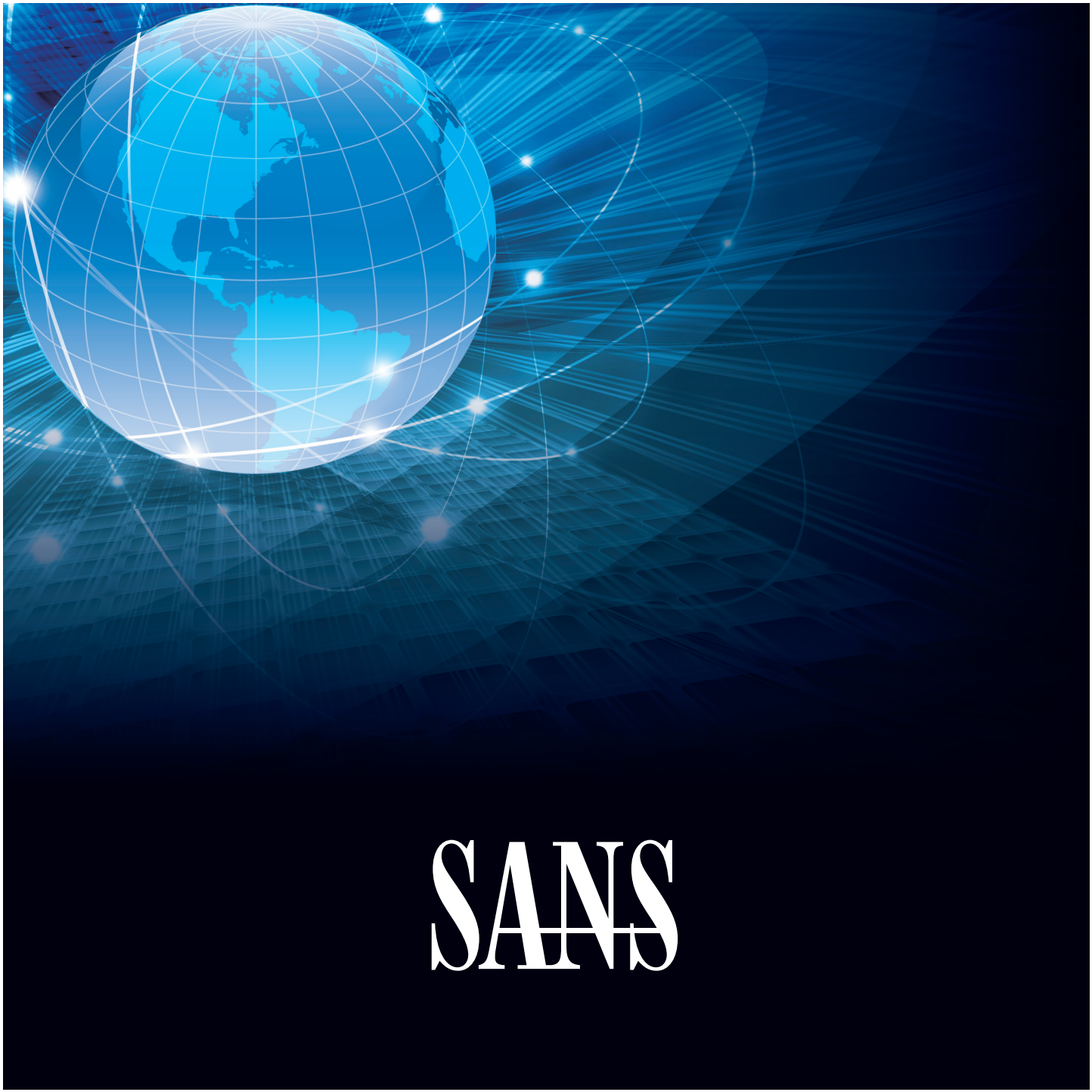
Innovation:

Creation of a statewide information security office team and accompanying certification program

Department of Technology & Information
State of Delaware

The State of Delaware Security Program centers upon a statewide Information Security Officer (ISO) team. Every State organization in Delaware is required to designate one to three ISOs who are responsible for all security matters within their organization. This includes information security, physical security, confidentiality, and privacy. The importance and visibility of this role has grown dramatically and requires that ISOs stay current in their field.

A Delaware Certified Information Security Officer, also known as a DCISO, achieves full certification by completing four core requirements over a 24-month period, which includes ISO meeting attendance, security training for their organizations employees, surprise inspections for data leakage, elective credits for continuing education, vulnerability scanning, and risk assessments. ISOs track their certification credits using a DCISO portal modeled after other professional certification sites, such as PMP and CISSP. The certification program was created by ISOs, and the full ISO membership was asked for input and feedback along the way. The program enables Delaware ISOs to demonstrate their knowledge of information security, enhances their career with increased credibility, and confirms their security commitment to their leadership team. The DCISO innovation was designed to scale to statewide implementation, including all three branches of government and the K12 Education community.


SANS