Continuous Diagnostics and Mitigation : Making it Work

Security professionals in federal, state and local agencies face many unique challenges in protecting critical systems and information. The CDM program has tremendous potential for both increasing the security levels at those agencies and reducing the cost of demonstrating compliance. However, to be successful, the program must address the following: lack of awareness, low inspector general awareness and lack of information on how to use the program.
Continuous Diagnostics and Mitigation: Making It Work

A SANS Survey
Written by John Pescatore
Advisor: Tony Sager
August 2014

Sponsored by
FireMon, ForeScout, IBM and Symantec

©2014 SANS™ Institute
Executive Summary

Government agencies are very early in the process of adopting the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) program. Awareness is spotty, and those that are aware of the program anticipate difficulties finding the skills to implement and maintain the security controls responsible for meeting the CDM goals. The good news is: Those that are actually implementing CDM capabilities are experiencing better security as a result.

Security professionals in federal, state and local agencies face many unique challenges in protecting critical systems and information. The CDM program has tremendous potential for both increasing the security levels at those agencies and reducing the cost of demonstrating compliance.

To find out how well this program is being accepted by government agencies, SANS conducted a survey of government-focused IT professionals during the months of April and May to determine their awareness of the CDM guidance and their levels of implementation. SANS also asked respondents about their levels of adoption and integration, as well as their successes and the obstacles government security professionals are facing in using the CDM.

The survey was open only to qualified respondents who were employees, contractors or vendors at federal, state and local agencies. Although this limited the potential number of respondents, the final total of 81 qualified respondents also indicates a low level of awareness for the CDM effort.

According to results, government agencies are very early in the adoption level of the CDM program, awareness is spotty, and those that are aware of the program anticipate difficulties finding the skills to implement and maintain the security controls responsible for meeting the CDM goals.

These and other findings are in the following report.

- **Lack of awareness except at the top.** Although the formal DHS outreach to CIOs and CSOs at the top of federal government departments and agencies has been extensive, the “trickle down” of information to security administrators, analysts and operations staff has been limited. CIOs (49%) and CSOs (49%) had levels of awareness significantly higher than those of security (36%) or IT administrators (21%).

- **Low level of inspector general awareness and support.** Awareness and support of the CDM effort by inspectors general is very low (5%). Because a major goal of the CDM effort is to change the government focus from a yearly auditing approach to a continuous security monitoring approach, Office of Management and Budget (OMB) guidance to auditors and buy-in from the Office of the Inspector General (OIG) are critical. They must be made more aware of the goals of CDM and the changes required.
• **Better security a key benefit.** Most (56%) respondents are able to measure success in their CDM implementations, with 44% experiencing better security as a result of the CDM controls. Some (24%) expended increased procurement efforts, somewhat fewer (12%) reaped the benefits without increasing procurement efforts, and a few (8%) were able to increase security while reducing their procurement efforts.

• **Information needed.** Knowledge about how to implement CDM is lacking among 48% respondents. Training on CDM concepts and technologies (54%), better information flow from DHS to main line implementers (38%) and better guidance from DHS on how to implement CDM (38%) are the leading types of information needed.

• **Staffing and skills needed.** Concerns about budget (40%), staffing (32%) and skills (36%) are seen as the greatest obstacles to CDM adoption, once potential adopters have the needed information. While most of the technologies used in CDM are familiar, moving to continuous monitoring will require significant process change and skill enhancement.

• **Success stories needed.** Due to the sequestration and government shutdown of 2013, Phase 1 progress was limited. Only 5% of respondents have already used the BPAs (Blanket Purchase Agreements), which greatly limits the availability of “What Works” success stories and word-of-mouth momentum.
Before diving into the survey results, a quick background on the Continuous Diagnostics and Mitigation (CDM) goals and technical implementation phases is in order. The CDM program was established at the Department of Homeland Security (DHS) in 2012 to provide "... tools and services that enable Federal and other government entities to strengthen the security posture of their cyber networks." In 2013 a Blanket Purchase Agreement (BPA) contract called the continuous-monitoring-as-a-service (CMaaS) BPA was established.

The CDM program is an ambitious undertaking that provides a phased approach to changing and improving the way government systems are protected. The ultimate goal is faster scanning and reporting, with a goal of completely assessing a network within a 72-hour window, as shown in Figure 1.

![Figure 1. Continuous Monitoring, as Defined by DHS](www.gsa.gov/portal/content/177887)

These six steps rely on wide visibility into enterprise systems, risk scores, workflow remediation and other automated processes to fulfill this loop. Figure 2 illustrates the implementation phases planned by CDM to complete this loop, including specific technical areas of focus.

---

### Goals of CDM

The funding for this effort, managed by DHS and the General Services Administration (GSA), was justified by three major goals:

1. Increase the overall security levels at federal, state and local government agencies, measured by reduced numbers of breaches, reduced vulnerabilities and increased FISMA (Federal Information Security Management Act) compliance scores.

2. Provide better visibility of security posture and situational awareness at both the individual department/agency level and the overall/national level.

3. Facilitate moving the federal government from a yearly FISMA compliance focus to a continuous security improvement focus, with the end goal of eliminating the expensive requirement for recertifying government systems every three years.

---

1. [www.us-cert.gov/cdm](www.us-cert.gov/cdm)
2. [www.sans.org/score/fisma_nist.pdf](www.sans.org/score/fisma_nist.pdf)
3. [www.gsa.gov/portal/content/177887](www.gsa.gov/portal/content/177887)
In fiscal year 2013 (FY2013),5 “Phase 0” provided funding for government agencies to procure licenses for security monitoring products to increase coverage or close gaps. In FY2014, Phase 1 kicked off. Phase 2 deployment was delayed until early FY2015.6 OMB issued guidance for agencies to develop and document their CDM strategies by the end of February 2014.

---

4 www.gsa.gov/portal/content/177899
5 Throughout this paper, when we refer to a fiscal year, we are referring to the federal fiscal year, which begins on October 1 and ends on September 30.
The SANS Institute conducted an online survey on awareness and use of the DHS CDM program during April and May 2014. The survey was open only to qualified respondents who were either employees, contractors or vendors at federal, state or local agencies. Although this limited the potential number of respondents, the final total of 81 qualified respondents also indicates a low level of awareness for the CDM effort.

For analytical purposes, SANS grouped the responses to the survey questions into four areas:

1. **Awareness**—Who in the organization is aware of the CDM program, and who is supporting it
2. **Benefits and barriers to adoption**—Perceptions of gains expected from CDM adoption and obstacles seen to realizing those benefits
3. **Initial assessment**—Whether and how an initial foundational assessment was performed
4. **Implementation progress and procurement plans**—What functional areas in Phase 1 of the CDM program have been implemented, and what plans are in place for Phase 2 capabilities
Organizations Represented

Survey participation was limited to employees or contractors who work for federal, state, or local government or tribal entities (there was only one tribal respondent), as well as CDM product vendors or integrators. Government employees across agencies made up 57% of respondents. Contractors that support government agencies, excluding CDM vendors or integrators, accounted for 24% of total respondents, with CDM product vendors (9%) and integrators (6%) accounting for an additional 15% of total responses (see Figure 3).

Because the security challenges are very different at the federal level as opposed to the state/local/tribal (SLT) level, we have differentiated the responses based on agency type throughout this paper.
For example, the respondents from federal agencies were skewed toward large organizations. Federal organizations with workforces of more than 5,000 accounted for 32% of all respondents, and federal agencies with more than 25,000 employees made up 19% of the sample, as shown in Figure 4.

The SLT distribution was pretty much the exact opposite, with 43% of all respondents coming from SLT organizations with fewer than 5,000 employees and 16% of total responses coming from small SLT organizations with fewer than 100 people.
Who Responded to the Survey?

Security professionals represented the largest occupational group to take the survey. Security analysts (23%) and administrators (7%) accounted for 30% of survey takers. Senior management accounted for 18% of respondents. The category of CIO/CTO/IT manager or director was selected by 11% of respondents; and that of CSO/CISO/security manager or director was selected by 7%, as shown in Figure 5.

The remaining respondents were scattered across various operational roles, including the responses indicated as “Other.” Overall, 76% of the respondents were considered employees, and 24% were contractors.
Affected by the government shutdown, which shut down DHS and CDM for 17 days in 2013, CDM got off to a slow start after the initial award in August 2013. Although DHS awareness efforts ramped up considerably in calendar year 2014, survey results indicate that the level of awareness of the CDM program remains fairly low: 30% were unaware, and fewer than 5% had actually started an implementation (see Figure 6).

Given the delays caused by the government shutdown, it is not surprising that the level of procurement was low. However, with the extensive outreach efforts by DHS in calendar year 2014, the low overall level of awareness is somewhat surprising. Part of the lack of awareness may be due to the level of employees taking the survey: The largest group of respondents consisted of security administrators and analysts, yet the DHS outreach effort mostly reached the top levels of agency management (CISO/CSO).

---

The results showed that of the respondents who indicated awareness of the CDM program, CIOs (49%) and CSOs (49%) had levels of awareness significantly higher than security (36%) or IT administrators (21%). Another 31% reported that agency heads are aware and supportive, as shown in Figure 7.

One extremely troubling result is that only 5% indicated that the inspector general (IG) was aware and supportive of the CDM effort. Office of the Inspector General (OIG) awareness and support is critical to the success of the move to CDM, because one of the major goals of the CDM program, as well as one of the major financial justifications, is to reduce the cost of certification, accreditation and compliance efforts to provide more focus on actual security improvements.
Security, like quality, can only be improved if you know where you are starting from and identify the gaps that need to be addressed, in order of importance. For the CDM program, participating agencies must undergo a foundational assessment.

The survey found that only 21% of respondents had conducted such an assessment. Many (36%), however, did a gap assessment through a more informal procedure. Shockingly, 44% have never conducted a gap assessment (see Figure 8).

To be eligible for the first round of funding from the CDM contract, federal agencies were required to undergo foundational gap assessments. While we did not limit this survey to agencies that had signed memos of understanding/agreement with DHS, the vast majority of federal respondents came from agencies that had done so. Because DHS reports that the majority of federal agencies have undergone foundational assessments, this likely indicates a lack of information flow within those agencies down to the security operations personnel who participated in the survey.

SANS also asked respondents to rate the difficulties they faced in classifying assets as part of performing the gap assessment. Differentiating between unmanaged/managed and authorized/unauthorized devices connecting to the network was cited as the most difficult, while identifying and classifying servers, PCs and specialty devices were all rated as equally less difficult. Several products offered under CDM can play a key role in addressing this area.
The CDM program requirement for formal foundational assessments does not extend out to SLT, so it is not surprising that no state or local agencies have conducted formal gap assessments. States are doing informal assessments (see Figure 9), but no local government reports even having done an informal assessment.

This disparity points back to lack of manpower and budget, which are particularly difficult areas for smaller government agencies. Those lacking the resources are also less able to fund the education they need for program rollout and integration.
Procurement Plans

Of those who indicated they were aware of the CDM program, 50% indicated they had plans to procure through the CDM program in FY2014 or FY2015. At the time they took this survey, FY2014 was half complete, which places a lot of their procurement in FY2015, as shown in Figure 10.

While products led the procurements in FY2014, the demand for services will grow after those products are procured. In FY2015, most plan to procure both products and services (57%) or services only (also 57%), whereas 48% plan to procure products only (see Figure 10). At the time this report was being developed, DHS was in process of awarding task orders for services across six groupings of federal agencies.8

---

Implementation Status—Phase 1

Phase 1 of the CDM program focuses on four functional areas: hardware asset management, software asset management, configuration management and vulnerability management. Of those respondents that have begun deploying CDM, 22% have already deployed vulnerability management. To meet federal CyberScope reporting requirements, all government agencies had to use some form of vulnerability assessment product. However, many government agencies did not have full coverage of all network segments, and the FY2013 CDM funds allowed them to procure additional licenses to complete that coverage. The 22% figure likely represents the use of the CDM award to expand vulnerability management coverage. It does not mean that only 22% of respondents have deployed any vulnerability management.

Half as many have deployed hardware and software asset management, and fewer still have deployed configuration management, as illustrated in Figure 11.

The main goal of CDM Phase 1 is endpoint integrity, including servers, security devices, Department/Agency-managed devices and user-owned devices. Please indicate the status of your implementation of CDM Phase 1 capabilities.

Figure 11. CDM Phase 1 Deployment Status
Configuration management is, however, highest on their list of “procured,” and on the list of “deploying,” indicating that configuration management and vulnerability management are equally important to CDM efforts and are most likely the first functions to start working together. This is a positive sign. Vulnerability management is essentially used to detect failures in configuration management, such as missing patches, misconfigured systems and so on. When configuration management processes are improved, security goes up—and vulnerability assessment critical findings go down. This is particularly important in the configuration management of security controls, such as firewalls, intrusion prevention systems and others.

Meanwhile, software and hardware asset management were cited most highly as “planning to deploy,” at 48% and 44%, respectively. But they were also the least cited for either “currently deploying” or “already procured,” indicating that increases in deployment of hardware and software asset management capabilities are still some time away.

This is a negative finding and highlights where organizations need to make important improvements. It is impossible to manage the configuration of assets you are not aware of. Historically, part of the issue at federal agencies has been that the distributed nature of IT systems and governance makes it hard to deploy asset management tools and processes that get full coverage. Those issues need to be addressed as part of the services task orders to make effective use of CDM products and technologies.
Turning to Services

Ideally, government agencies would increase head count and training budgets to staff new skills for each step in each phase, but that is not always feasible in the current funding environment. One way to overcome this barrier is to use CMaaS offerings under the CDM contract—essentially outsourcing some of the first line of monitoring workload.

However, when asked about plans to use CMaaS, 46% of respondents skipped the question, and of those that did respond, 64% responded either “unknown” or “not planning to use.” Only 36% had near- or long-term plans to use the CMaaS offerings, with 12% planning to use them in FY2015 and another 12% planning to use them in FY2016, as illustrated in Figure 12.

The response is actually consistent with relatively low levels of government use of managed security services overall. Because the use of cloud services is essentially outsourcing, as the use of the Federal Risk and Authorization and Management Program (FedRAMP) for certified cloud services increases, we expect to see cloud-based security services obtain FedRAMP certification and plans for using CMaaS to increase as well.

TAKEAWAY: CMaaS use will not increase faster than government use of outsourcing and cloud-based services overall.

---

9 www.gsa.gov/portal/category/102375
Of the respondents already participating in the CDM program, 44% are experiencing better security as a result of the CDM controls: 24% improved security with increased procurement efforts; 12% increased security without changing their procurement efforts; and 8% increased security while actually reducing their procurement efforts, as shown in Figure 13.

Another 44% can’t measure success at this time. This number is derived from the 28% who can’t yet measure any increase in security or reduction in procurement effort and the 16% who responded with “other,” which includes the “don’t know” answer types as well.

In other words, those that can benchmark the impact of CDM on their organizations are primarily experiencing better security, while few have seen a reduction in procurement efforts. This can be attributed to the fact that the CDM award is in the early phases and procurement processes have not yet been streamlined.

Still, the group that either didn’t know or can’t quantify results points out the challenges organizations face in accurately measuring increases in security. Continuous monitoring by itself does not increase security—finding vulnerabilities faster without fixing or mitigating vulnerabilities faster just means more data was generated. To show meaningful, measurable increases in security from the use of CDM, agencies will need to use the increased visibility from CDM to drive improvements in configuration management, asset management and other operational processes.
Benefits: A Matter of Perception

The CDM approach has its roots in the Critical Security Controls effort, which began as a way to prioritize the security tools that are most effective in detecting, mitigating and blocking current threats.\(^{10}\) The phased CDM approach started with the security controls that increase visibility and vulnerability assessment of what is on the network, because you can’t protect what you don’t know exists. That benefit is clear to the respondents who ranked visibility and increased security at the top of the benefits of CDM. Their rankings follow this order:

1. Improved visibility into endpoint, network and security devices
2. Increased security and resistance to attack through reduced vulnerabilities
3. Easier FISMA compliance reporting
4. Reduced procurement burden for services we are already using
5. Reduced prices on products we are already using
6. Better, easier integration across our security tools and services
7. Elimination of the certification/accreditation burden
8. Use of security-as-a-service offerings/Relieve the burden on our department
9. Faster procurement of innovative products or contractor services

The next major goal of the CDM effort, easier FISMA compliance reporting, ranked third. However, unless awareness and support for the CDM effort increases at the inspector general level, this benefit is at risk for two reasons: First, if yearly OIG reports and FISMA “grades” continue to weight all controls in NIST 800-53 equally, as opposed to prioritizing those areas focused on by continuous monitoring, government security resources will remain focused on compliance instead of security. Second, for the elimination of the requirement for recertification every three years to become a reality, IGs have to buy into the CDM approach.

\(^{10}\) www.counciloncybersecurity.org/critical-controls
Confidence is somewhat lower in the reduced procurement burden of acquiring products and services that were already being used, as well as reduced prices for those products. This is consistent with respondents’ experience highlighted previously in Figure 13, which shows that only 8% were able to reduce procurement efforts while increasing security.

While it is early in the CDM contract to fully measure the ease of procurement, this finding likely represents the pragmatic view of most of the respondents who have seen other large-scale procurement vehicles pushed by the GSA or OMB in the past actually result in more complexity and higher prices. DHS has negotiated some aggressive and innovative pricing approaches in the CDM contract, but government security professionals are waiting to see if the walk matches the talk. As more success stories emerge, we predict such concerns will decrease.

That attitude also came across in the lower ranking of better integration between tools. The Security Content Automation Protocol (SCAP) effort in the government began back in 2006 and was overhyped. Although many tools have been SCAP-certified, real-world reduction in integration effort has been minimal for a variety of reasons. Realistically, we are unlikely to see major gains in achieving higher levels of useful integration among the various security tools in use until later phases of the CDM program.

Security professionals are also taking a wait-and-see approach to the elimination of the certification and accreditation burden. As mentioned earlier, the support of OMB and guidance to IGs are needed to make this benefit a reality. Increasing government use of cloud services that have been validated through FedRAMP will help in this area, as the use of continuous monitoring with cloud services has the same promise for eliminating the three-year recertification requirement.
Barriers: Lack of Information

Despite DHS outreach about the CDM program, the top-rated barrier to using it was insufficient information on how to use the program, noted by 48% of respondents. Lack of budget (40%) was the next most highly rated barrier. Figure 14 shows the key barriers to use of the CDM program.

Unfortunately, in the current government-funding environment, budgetary uncertainty is simply a continuing reality.

However, if you combine the responses related to lack of staffing (32%) and skills (36%), then skills and staffing turn out to be the top concern. This circles back to lack of funding to afford the skills needed to support new security processes.

Any change in processes initially requires training on the new approach and increased effort. While the annual FISMA reporting exercises have many deficiencies, the process is familiar and well understood. If continuous monitoring meant doing that same exercise every 72 hours instead of once a year, staffing levels would need to skyrocket. That is not what CDM is aiming to do: Its goal is to help organizations automate these processes in an architecture that relies predominantly on technologies that are already in place or being procured. Government security managers need more education (both training and case studies) on how CDM will work and how to reduce the compliance burden.
Benefits and Barriers (CONTINUED)

Overcoming Barriers

When asked what type of information would help them use the CDM program effectively, the top response (54%) was “training on CDM concepts and technologies,” as shown in Figure 15.

This is consistent with the perceived barrier of lack of information and skills. While the Phase 1 product areas (asset discovery, inventory and vulnerability management) are familiar to most government security professionals, technologies in later phases such as privilege management and behavior management are not. Also, moving from yearly or at best quarterly assessments to completing an assessment every 72 hours requires more knowledge of the data and analysis loads, as well as the security information and event management (SIEM) and other tools (such as dashboards) offered to manage that workload.

The next two most frequently selected answers were “Better information flow from DHS to my department” (38%) and “Better guidance on how to implement CDM” (38%). Together, these two response categories indicate that more information from DHS down to operational groups is the top need. This is consistent with previous responses. Although the DHS outreach has reached the top-level personnel at the majority of government departments and agencies, how-to information has not reached the operational levels to the same degree.

The open-ended responses gathered at the end of the survey reinforce this finding: More “continuous” information about how to use the CDM program, products and services is clearly identified as a need by respondents.
In some ways, organizations seem more prepared for Phase 2 than Phase 1 implementation. For example, 47% of the respondents indicated they had already deployed network/physical access controls, and 37% reported already deploying credentials and access management. Trust in people granted access (access control management) was most commonly selected (42% of respondents) as the focus of FY2015 plans. Security-related behavior management, quality management and privilege management, each selected by 37% of respondents, tied for the focus of FY2016 procurement plans (see Figure 16).

Access controls, access management and authentication have likely been in place in these organizations or under development since before the CDM program. DHS has not yet fully defined the quality management area in Phase 3, resulting in low levels of near-term procurement plans.
This survey highlighted several areas in which improvements need to be made if the CDM program is to meet its goals of improving security and reducing procurement effort:

**Increase awareness at the operational level.** The survey pointed out that much more awareness of CDM exists at the top level of government departments and agencies than at the operational level. Available information hasn’t been reaching the lower levels. For example, DHS has developed a series of training modules that offer information on how to complete many of the required tasks. Government agency CSOs and CISOs should increase their efforts to make sure information from the CDM program is widely disseminated. For example, at a recent Health and Human Services Quarterly Technology Day, several sessions were devoted to briefings from both DHS personnel on the CDM program and Health and Human Services (HHS) security managers on HHS activities relating to CDM.

**Guidance to inspectors general.** DHS, GSA and the Government Accounting Office (GAO) should specifically target inspectors general to make sure they are aware of and understand both the need to change the process and the specifics of the CDM approach. GAO needs to specifically work to develop and promulgate new guidance to auditors with CDM in mind.

**Additional incentives for moving to CDM.** The CDM program already has two powerful financial incentives for CDM adoption: reduced cost of products and services and the potential elimination of the three-year recertification requirement. However, these incentives are really only useful to those at the top of organizations who have budgetary responsibility. At the operational level, incentives should be introduced for becoming expert at architecting, deploying and managing CDM-based security programs. This could include career certification programs, case studies that highlight government security people who drove security improvements via CDM, or awards and commendations for the biggest improvements in agency security levels after each CDM phase.

---

12 A list of training materials available is provided at [www.us-cert.gov/cdm](http://www.us-cert.gov/cdm).
The survey results show that the CDM program has reached significant levels of visibility at the top levels of government agencies, but proponents have much work to do in reaching the broader security operations community and the offices of inspectors general. Most respondents understand the benefits of continuous monitoring but have not yet been able to measure increases in security or decreases in procurement effort. Given the early stages of the CDM contract, they have not yet seen examples of success stories of implementations that achieved those benefits. Moreover, they have no examples showing the levels of staffing and retraining required.

Change anywhere is hard; significant change is that much more difficult—and driving significant change in government is exponentially harder. The CDM program has the promise to be a real game changer in enabling government security professionals to focus first on securing critical systems and information, and then demonstrating compliance as a by-product of that focus. However, government security managers need more than access to products and services. They need more information, guidance and training at the how-to level instead of at the programmatic level.

This survey has highlighted the key areas where levers exist to remove obstacles from the path of CDM progress.

- **Information.** Agency CIOs and CSOs need to make sure information is flowing about the CDM program through the agency and down to the operational security elements. At a recent HHS internal security summit, several sessions were included that provided updates from the DHS program office and information about how HHS is using the CDM contract.

- **Metrics.** Meaningful metrics that demonstrate increases in security need to be developed and agreed upon. Reduction in vulnerabilities is the end goal, not just more data about vulnerabilities being available faster. The security dashboards being developed should be aimed at driving improvements in configuration management as well as vulnerability management.

- **IG awareness.** The inspectors general need to be made more aware of the goals of CDM and the changes required. DHS should increase outreach to IGs, and GAO should develop specific guidance.

- **Agency readiness.** Agencies need to make sure their processes allow them to take advantage of CDM capabilities. In addition, employee/contractor skills need to be enhanced to meet their new challenges.

The DHS program office has been very receptive to suggestions and participation from all interested parties. SANS and the survey sponsors invite you to participate in the continuing process.
John Pescatore joined SANS in January 2013, with 35 years of experience in computer, network and information security. He was Gartner’s lead security analyst for more than 13 years, working with global 5000 corporations, government agencies and major technology and service providers. In 2008, he was named one of the top 15 most influential people in security, and he has testified before Congress on cybersecurity.

Prior to joining Gartner Inc. in 1999, John was senior consultant for Entrust Technologies and Trusted Information Systems, where he started, grew and managed security consulting groups focusing on firewalls, network security, encryption and public key infrastructures. Prior to that, he spent 11 years with GTE developing secure computing and telecommunications systems. In 1985 he won a GTE-wide Warner Technical Achievement award.

John began his career at the National Security Agency, where he designed secure voice systems, and the United States Secret Service, where he developed secure communications and surveillance systems—and the occasional ballistic armor installation. He holds a bachelor’s degree in electrical engineering from the University of Connecticut and is an NSA-certified cryptologic engineer. He is an extra-class amateur radio operator, callsign K3TN.

SANS would like to thank this survey’s sponsors:

F I R E M O N

ForeScout

IBM

Symantec
# Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Location</th>
<th>Dates</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Oslo 2015</td>
<td>Oslo, NO</td>
<td>Mar 23, 2015 - Mar 28, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS 2015</td>
<td>Orlando, FLUS</td>
<td>Apr 11, 2015 - Apr 18, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>RSA Conference 2015</td>
<td>San Francisco, CAUS</td>
<td>Apr 19, 2015 - Apr 22, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>Security Operations Center Summit &amp; Training</td>
<td>Washington, DCUS</td>
<td>Apr 24, 2015 - May 01, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS London 2015</td>
<td>London, GB</td>
<td>Apr 27, 2015 - May 02, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS SEC401 London</td>
<td>London, GB</td>
<td>Apr 27, 2015 - May 02, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Bahrain 2015</td>
<td>Manama, BH</td>
<td>May 02, 2015 - May 07, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Security West 2015</td>
<td>San Diego, CAUS</td>
<td>May 03, 2015 - May 12, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure India 2015</td>
<td>Bangalore, IN</td>
<td>May 04, 2015 - May 16, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure Europe 2015</td>
<td>Amsterdam, NL</td>
<td>May 05, 2015 - May 25, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS/NH-ISAC Healthcare Cybersecurity Summit</td>
<td>Atlanta, GAUS</td>
<td>May 12, 2015 - May 19, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Pen Test Austin 2015</td>
<td>Austin, TXUS</td>
<td>May 18, 2015 - May 23, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Melbourne 2015</td>
<td>Melbourne, AU</td>
<td>May 18, 2015 - May 23, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS Security Training - Houston</td>
<td>Houston, TXUS</td>
<td>Jun 01, 2015 - Jun 05, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS410 Vienna in Association with IAEA</td>
<td>Vienna, AT</td>
<td>Jun 06, 2015 - Jun 10, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Dublin 2015</td>
<td>Dublin, IE</td>
<td>Jun 08, 2015 - Jun 13, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Houston 2015</td>
<td>Online, TXUS</td>
<td>Mar 23, 2015 - Mar 28, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>