

# Securing the Internet of Things Survey

# Securing the "Internet of Things" Survey

## A SANS Analyst Survey

*Written by John Pescatore*
*Advisor: Gal Shpantzer*

January 2014

*Sponsored by*
*Codenomicon and Norse*

# Executive Summary

The "Internet of Things" has been attracting a lot of buzz—the latest Gartner Hype Cycle for Emerging Technologies places it almost at the "Peak of Inflated Expectations" (see Figure 1).

**Hype Cycle for Emerging Technologies – 2013**

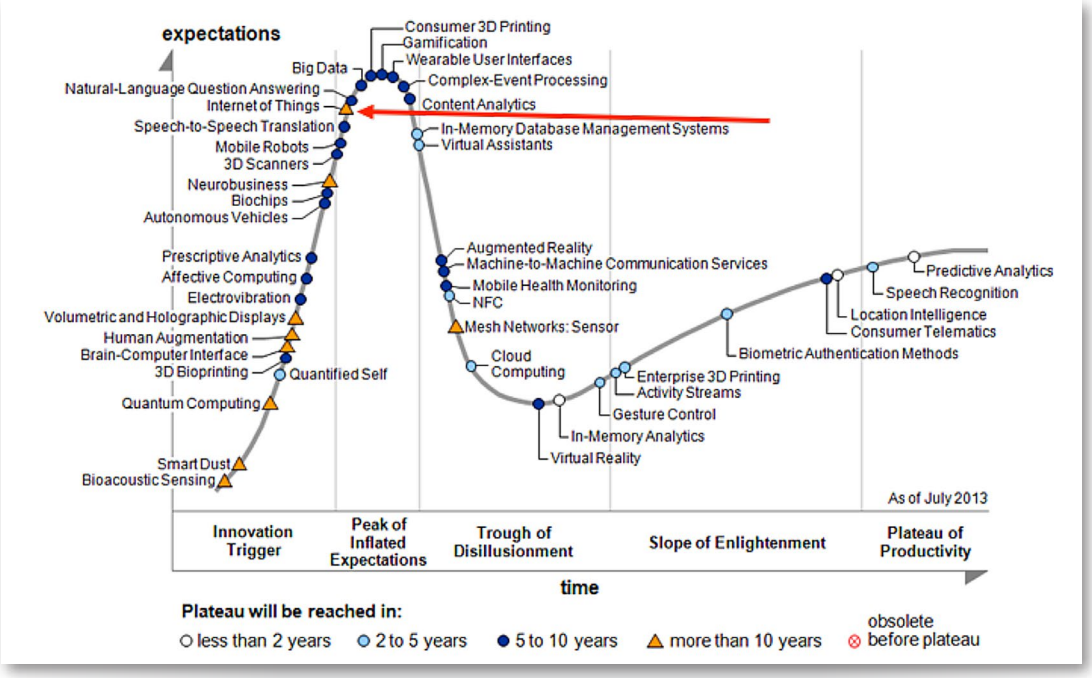



*Figure 1. Hype Cycle for Emerging Technologies (from www.gartner.com/newsroom/id/2575515)*

But what exactly is the Internet of Things? And what will it mean to cybersecurity? There are other terms in use that generally mean the same thing. The National Security Telecommunications Advisory Council (NSTAC) has initiated a working group to look at the national security implications of the "Industrial Internet,"[1] and the National Institute of Standards and Technology (NIST) has used the term "Cyber-Physical Systems."[2] Several vendors have also used the term the "Internet of Everything." However, Internet of Things (IoT) is the most widely used term.

SANS uses a simple definition of the Internet of Things:[3]

> *The Internet enables any-to-any connectivity. Smart buildings, HVAC and even physical security technologies are now connected, as are handheld smart devices and more. The latest wave of 'things' connecting to users, businesses and other 'things' using mixtures of wired and wireless connectivity, includes but is not limited to automobiles, airplanes, medical machinery and personal (implanted) medical devices, and SCADA systems (windmills, environmental sensors, natural gas extraction platforms, hydro systems, you name it).*

[1] www.dhs.gov/sites/default/files/publications/NSTAC%20Meeting%20Discussion%20Aid.pdf

[2] www.cybersecurityresearch.org/documents/CSRA_Workshop_Report.pdf

[3] For clarity, where we are discussing devices attached to the Internet as part of the Internet of Things, we have capitalized *Things*.

SANS defines four waves of devices making up the Internet of Things:

1. PCs, servers, routers, switches and other such devices bought as IT devices by enterprise IT people, primarily using wired connectivity
2. Medical machinery, SCADA, process control, kiosks and similar technologies bought as appliances by enterprise operational technology (OT) people primarily using wired connectivity
3. Smartphones and tablets bought as IT devices by consumers (employees) exclusively using wireless connectivity and often multiple forms of wireless connectivity
4. Single-purpose devices bought by both consumers, IT and OT people exclusively using wireless connectivity, generally of a single form

It is this fourth wave that most people envision when they think of the IoT, but many in the security community who responded to the SANS Securing the "Internet of Things" Survey recognized that they are already dealing with the security issues of the first three waves and have started to see the leading edge of the fourth wave.

Another important aspect of this fourth wave is the dramatic growth of embedded computing and communications capabilities into just about everything—automobiles, trains, electric meters, vending machines and so on. Many of these items have had embedded software and processors, but mobile Internet connectivity is being added and bringing them onto the IoT. The embedded nature of the software causes problems for enterprise vulnerability assessment and configuration management processes.

In October 2013, SANS set out to find out what the security community thought about the current and future security realities of the IoT by posting a survey for security personnel active in the IT space. This report documents in detail the results provided by the 391 respondents. Key findings include the following:

- The majority of the cybersecurity community is already familiar with the security issues around the IoT, largely driven by the impact they have already seen from smartphones, tablets and industrial control systems.
- After consumer devices (such as smartphones and tablets), smart building and industrial control systems are the most frequently cited near-term sources of new devices to secure, followed by medical devices.
- While 40% of respondents feel that securing the IoT will require only minor enhancements to their security controls, 78% either are unsure about their capabilities for basic visibility and management of Things they will need to secure or lack the capability to secure them.
- Because of the perceived difficulties in securing the IoT, the SANS security community would like to see the manufacturers of Things play a major role in responsibility for security of devices.

# Survey Participants

Participants responded to the electronic survey, which was available during the months of October, November and December 2013. Although many others accessed or started the survey, 391 completed the survey. In order to understand the results, it's vital to first understand the audience that participated in the survey.

Survey respondents came from a broad range of industries, as illustrated in Figure 2.

**What is your company's primary industry?**

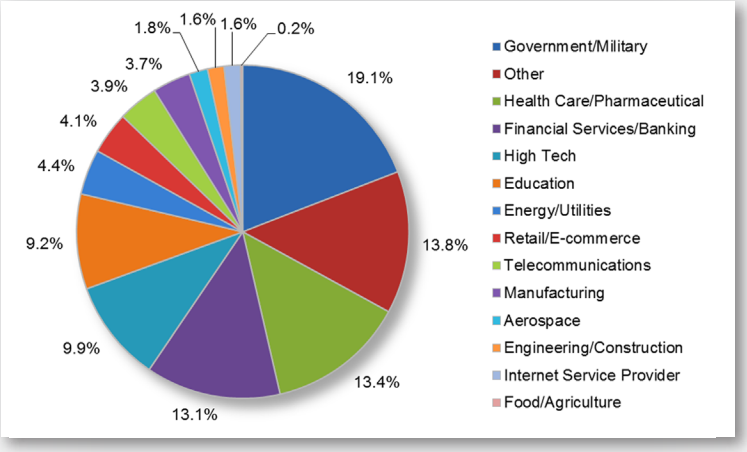



*Figure 2. Respondent Industry Representation*

The single largest vertical was government, at just over 19%. There have been several recent government efforts regarding the Internet of Things, explaining the high level of government interest.[4]

The next three largest verticals were equally spread across Other (14%), Health Care/Pharmaceutical (13%) and Financial Services/Banking (13%), followed by High Tech (10%), Education (9%) and Energy/Utilities (4%), perhaps due to active audiences within the SANS community. SANS expects the highest levels of near-term IoT deployments will be in Automotive (included in Other), Health Care/Pharmaceutical and Energy/Utilities. They represented organizations of all sizes, from large to small, with the largest companies representing international organizations, as shown in Figure 3.

[4] www.dhs.gov/sites/default/files/publications/NSTAC%20Meeting%20Discussion%20Aid.pdf and www.cybersecurityresearch.org/documents/CSRA_Workshop_Report.pdf

**What is the size of your organization?**

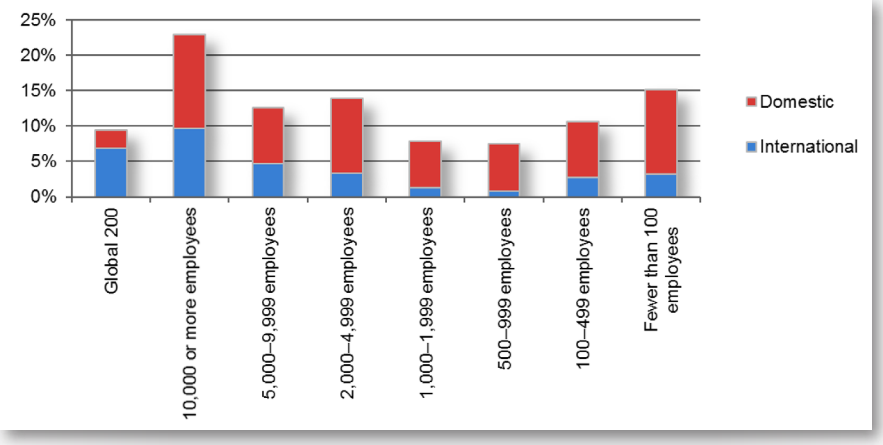
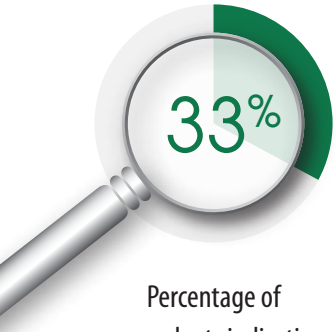



*Figure 3. Domestic and International Workforce Size*




Percentage of respondents indicating an international presence

Companies larger than 10,000 employees (23%) or in the Global 200 (9%) represented roughly one-third of respondents, as did companies with fewer than 1,000 employees (33%). The next largest segment (22%) of respondents came from the high end of the midsized organizations having between 1,000 and 5,000 employees.

The high interest by small businesses of fewer than 100 employees (15%) was surprising. Those respondents were skewed toward nonprofit organizations and high-tech companies, indicating interest in both the policy and market (selling) implications of the IoT.

Figure 4 illustrates the distribution of survey respondent roles.

**What is your primary role in the organization, whether as staff or consultant?**

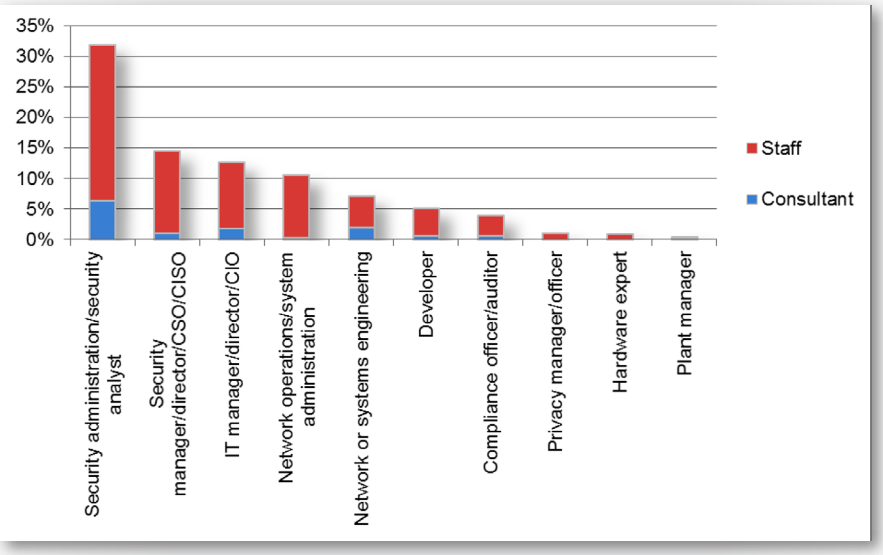



*Figure 4. Respondent Roles*

Security professionals represented the largest occupational group among the respondents, with the largest single occupational category in the survey being security administrators or analysts, at 32% of the total. Senior security professionals (security managers, directors or CSOs/CISOs) made up 15%, and the IT manager/director/CIO category represented slightly more than 13%. Network operations/systems administration personnel made up 11% of respondents, and compliance officer/auditors and consultants made up another 4%.

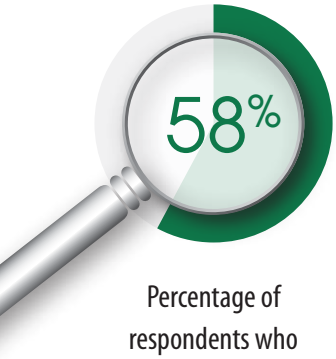
Numerous respondents in a broadly distributed "Other" category, not included in Figure 4, indicated they are also administrators, but many developers were also represented in the "Other" category. (Note that respondents were allowed to choose more than one option, representing an overlap in responsibilities in some cases.)

# Perception and Familiarity

When we look at preparedness for IoT, it is important to determine whether security professionals understand the technology and how it affects their organizations, as well as whether they grasp the security implications of such technologies.

## Level of Understanding

Almost 58% of respondents feel that they fully understand the term *Internet of Things*, and just over 7% fully understand the term, but consider it to be pure hype. A small percentage (5.1%) had no idea what it means, and just under 28% had a vague understanding. Figure 5 illustrates these results.




Percentage of respondents who feel they fully understand the term *Internet of Things*

**How would you describe your level of understanding of the term "The Internet of Things"?**

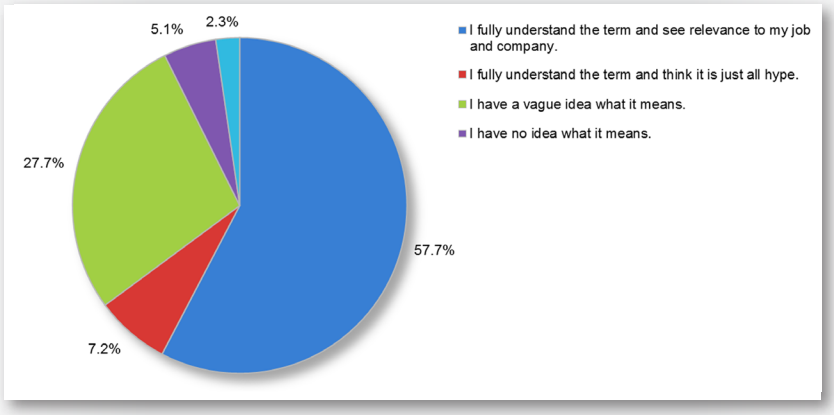



*Figure 5. Level of Understanding of What the* Internet of Things *Means*

The high level of understanding, and the low level of hype perception, are probably signs of self-selection in the survey. Those who chose to respond were likely to be experienced in this field. SANS believes a broader sampling type survey would likely show lower levels of understanding and higher levels of hype perception here. Recall that the Gartner hype cycle report mentioned earlier in the Executive Summary implies a high level of hype associated with IoT.

Reinforcing our interpretation of respondents' level of understanding, half were either currently active with IoT or will be next year. Fewer than 10% felt that IoT would never impact their organization, while just over 12% had no idea, as shown in Figure 6.

**Is your organization involved in any areas that fit into the SANS definition of the latest wave of connectivity to "Things"?**

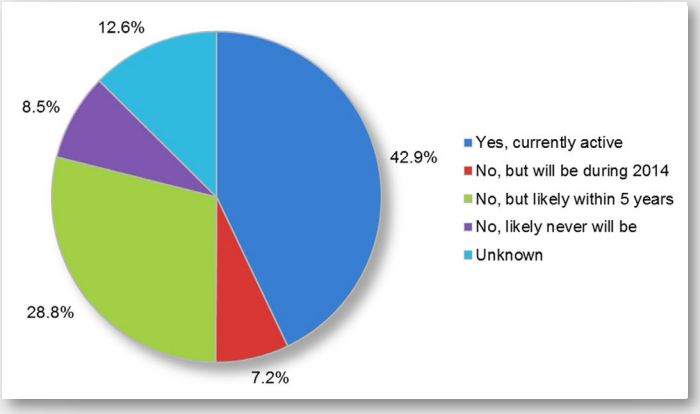
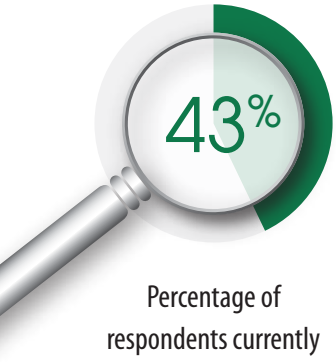



*Figure 6. Involvement with IoT*




Percentage of respondents currently active with IoT

## Level of Involvement

Because of their responses to the previous question, more than 60% of the respondents did not have the opportunity to answer this question or skipped it. Many respondents indicated they are "not sure" or "I have no idea" of the proliferation of the IoT in their long-form responses. One comment captured the issue succinctly: "Frankly I don't really know—mechanisms to audit 'Things' are very weak." This builds on the results of the SANS Critical Security Controls survey,[5] which found that 74% of respondents rely on manual processes for discovery and inventory of connected devices. Many of those processes rely on interrogating host-based agents or looking at Active Directory domain logins, neither of which are supported by emerging Things.

[5] www.sans.org/reading-room/analysts-program/csc-survey-2013

Of those who did respond, 27% have experienced a growth rate of 26–50% in Things, while 35% experienced less growth than that, and just under 16% said they saw between 51% and 100% growth in connected devices. Another 9% saw proliferation of more than 100%, as shown in Figure 7.

**How has the number of "Things" proliferated in your enterprise over the past 2 years?**

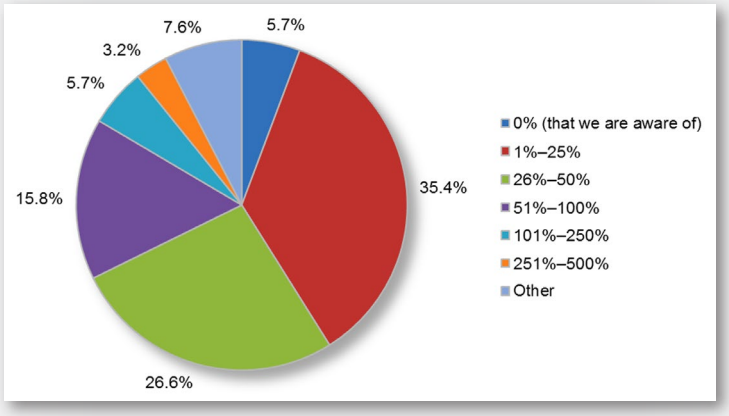



*Figure 7. Proliferation of Things*


Percentage of respondents seeing more than 100% proliferation of Things

Many of our respondents are either currently involved in or planning to be involved in IoT applications, as illustrated in Figure 8.

**What types of IoT applications is your organization involved in or planning to be involved in?**

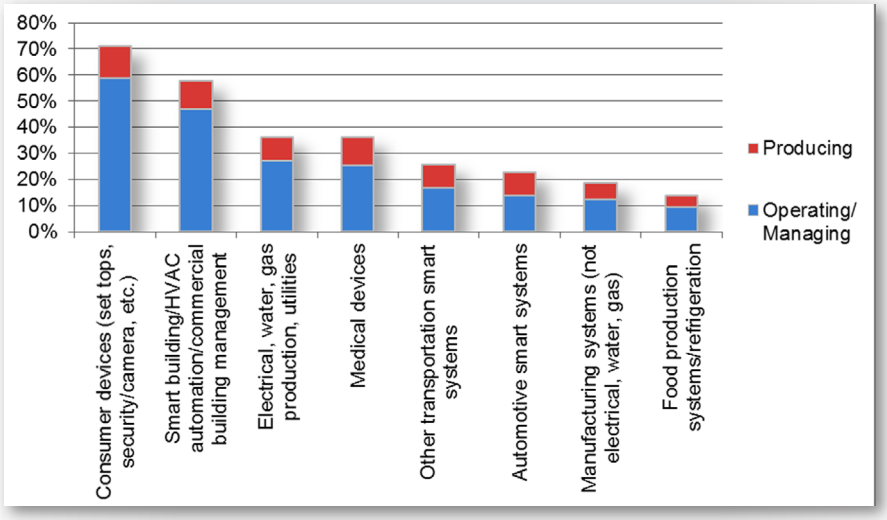



*Figure 8. IoT Applications*

Almost 66% of respondents indicated that they are either currently involved in or are planning to be involved in IoT applications involving consumer devices. This likely reflects the impact of BYOD and the "Consumerization of IT."[6] Surprisingly, the next largest area of involvement was smart building systems, which have not received as much hype as other areas of the IoT. This response likely represents the increasing handoff of operations technology management to the IT organization.[7]

Energy/utilities, medical devices and transportation were the next three most highly cited applications, reinforcing our belief that the highest level of near-term deployment of IoT devices will be in the automotive/transportation, health care/pharmaceutical and energy/utilities spaces. These areas, and smart building systems, all represent uses of Internet-connected devices based on embedded software and applications, which pose challenges to existing IT management and security practices.

[6] www.gartner.com/it-glossary/consumerization

[7] www.microsoft.com/government/ww/public-services/blog/Pages/post.aspx?postID=367&alD=112 and www.idc.com/getdoc.jsp?containerId=EI241783

Close to half (49%) of respondents felt that the IoT would have roughly the same level of security issues that previous waves of technology have had. Of those who thought differently, slightly more were optimistic (21%) than pessimistic (17%), as shown in Figure 9.

**Which statement best captures your feelings about the IoT and security?**

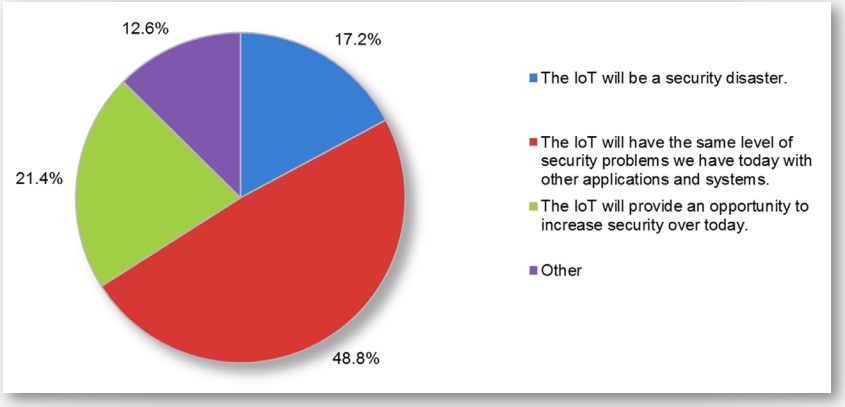



*Figure 9. Perceptions About IoT Security*

*The IoT is and will be a great security challenge and an opportunity for new ways of thinking about ecologies of security.*

The long-form comments to this question captured the wide range of opinions:

- "The IoT is and will be a great security challenge and an opportunity for new ways of thinking about ecologies of security."
- "IoT will increase vulnerabilities in a big way. Unintended consequences and all that...."
- "IoT is in its infancy, could be a disaster, or could be ok. It depends on emerging standards and acceptance. Clearly an ad hoc collection of IoT devices without security-oriented standards will be a total mess."
- "[IoT is] potentially a security disaster, but that will depend heavily on user education and due consideration of privacy and security from manufacturers."

## Greatest IoT Threat Vector

When asked what they perceived the greatest IoT threat vector would be, the most frequent response (31%) was an old bugaboo that will likely be exacerbated by the IoT and the high level of embedded operating systems and applications: patch management. Another familiar issue—malware—was the next most highly cited (26%), with the concern being that IoT devices would end up spreading malware into the enterprise. Denial of service (13%) and sabotage and destruction of connected Things (12%) were also concerns. Figure 10 shows all responses.

**What do you think the greatest threat to the Internet of Things will be over the next 5 years?**

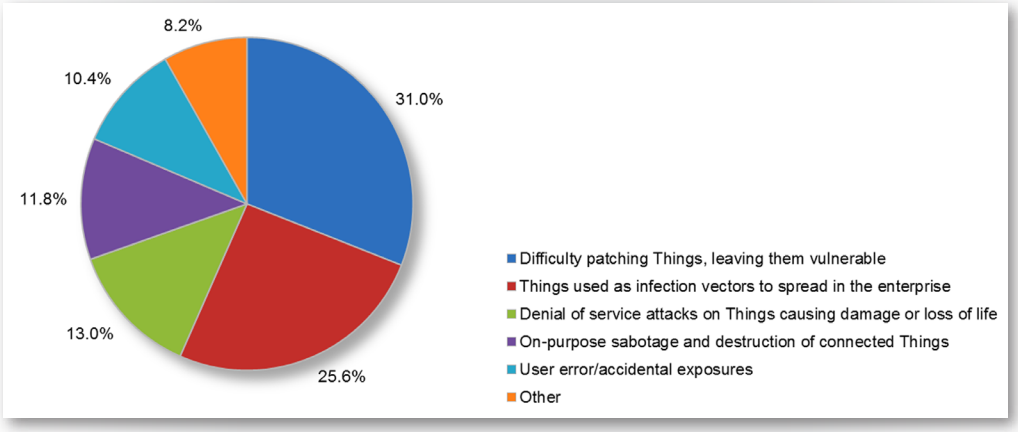



*Figure 10. Threats to the Internet of Things*

Interestingly, 10% see user error as the greatest threat vector. This is also in keeping with the expressed need for user education with respect to BYOD devices highlighted in the SANS Survey on Mobile Device Policy.[8]

[8] "Fear and Loathing in BYOD," www.sans.org/reading-room/analysts-program/fear-loathing-byod-survey

## Greatest IoT Risk

By definition, everything in the IoT has an Internet connection. So, it isn't surprising that half of the respondents rated Internet connection as the riskiest aspect of the IoT (see Figure 11).

**Where do you consider the greatest risk to be in "Things" connecting to your network and the Internet?**

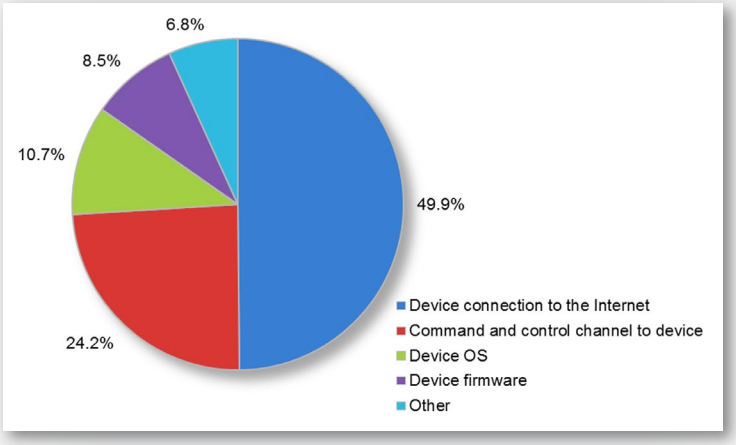



*Figure 11. Greatest Risk in IoT*

*Enterprises will need to emphasize manufacturer support for patching and updating as important evaluation criteria when selecting or certifying IoT devices.*

Because so many devices will be coming from consumer markets, the price, size and power constraints for many of those devices almost guarantee security will be an afterthought. Command and control channels to the devices were next most frequently cited (24%), with concerns about device operating systems (11%) and firmware (9%) rounding out the list. Organizations using IoT will need to add security around their IoT applications because, as previously noted, configuration and patch management will prove difficult for device maintenance. Enterprises will need to emphasize manufacturer support for patching and updating as important evaluation criteria when selecting or certifying IoT devices.

The IoT raises a number of security challenges compared to traditional IT systems:

- Many Things don't necessarily belong to IT; they are devices acquired and managed by their owners—individuals, business leads or others.
- Things that are acquired and managed by IT (such as medical machinery, SCADA and even corporate-issued smartphones and tablets) contain embedded operating systems and software that pose obstacles for IT to configure security and keep patched.
- Incidents involving Things (a hacked MRI machine or SCADA controller, for example) can carry physical consequences, as well as policy and financial impact.

These factors represent new challenges for policy development, configuration and vulnerability management, data collection and, above all, visualization of performance and status. In this section we explore these issues.

## Responsibility for Risk Management

Respondents could select multiple responses to the question about assessing responsibility for managing risk. The results, shown in Figure 12, however, demonstrate a shared responsibility for risk management.

**In your opinion, who should take responsibility for managing the risk imposed by new "Things" connecting to the Internet and your network?**

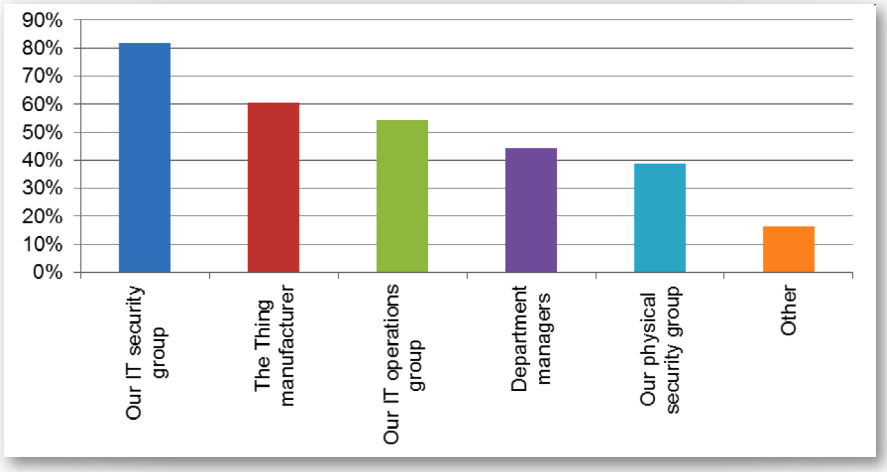



*Figure 12. Responsibility for Risk Management*

[15] www.fiercehealthit.com/story/state-level-data-governance-efforts-shaky-best/2013-06-13

This question allowed for multiple answer options to get a bigger view of all responsible parties involved in control system security. Not surprisingly, the vast majority (82%) of respondents felt the IT security group should be responsible for managing IoT risks; after all, that has been the case with every previous wave of IT and Internet technology. However, the next most highly cited selection was "The Thing Manufacturer," with 61%. Compare this to the PC/server wave of devices and software, when enterprises did not expect the device or software manufacturer to have responsibility for vulnerabilities in their products and rarely (if ever) included security requirements or specifications in procurement evaluations. If enterprises do place higher emphasis on security when acquiring Things, this response would indicate that enterprise security manufacturers will need to emphasize built-in security and demonstration of security in their procurements of IoT technologies. They will also need to provide or support common patching processes that work across their customer organizations with minimal disruption.

*If enterprises do place higher emphasis on security when acquiring Things, ... enterprise security manufacturers will need to emphasize built-in security and demonstration of security in their procurements of IoT technologies.*

Responses also indicate an awareness that responsibility is spread across the organization, with 54% of respondents citing the IT operations group as needing to be responsible for IoT security. Similarly, department managers were cited 44% of the time, generally as part of shared responsibility.

While smart building systems were cited earlier as the second most common IoT application already in use, only 39% cited the physical security group as the primary responsible party. This largely reflects the IT/OT integration movement discussed earlier.

## Ability to Secure IoT

While the majority of respondents are aware of IoT and the risks it presents, only 50% of respondents felt they were either totally unprepared to secure IoT use (14%) or would need major upgrades to do so (36%), as shown in Figure 13.

**Given the current state of your security program (people, processes, controls and technology), how would you rate your ability to provide security to an "Internet of Things"?**

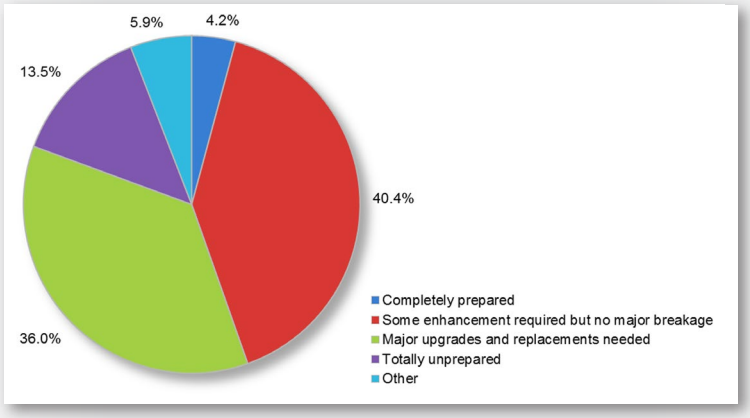
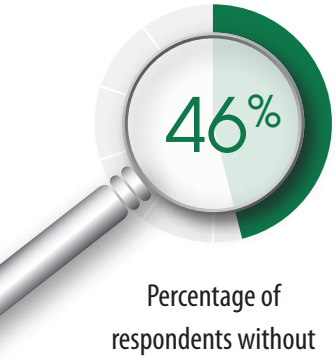



*Figure 13. State of IoT Security Programs*

Almost 45% either felt they were completely prepared (4%) or would only see minor breakage in their existing security program (40%) to prepare for Things in their environments. This number is actually higher than we would suspect, until you correlate it with the answer to our next question about their actual policies around managing the risk presented by IoT.

## IoT Security Policy

Nearly half (46%) of respondents did not feel they have a policy in place that could drive the necessary level of visibility and management of IoT devices, while one-third felt they did, as shown in Figure 14.




Percentage of respondents without a policy to drive visibility and management of IoT devices

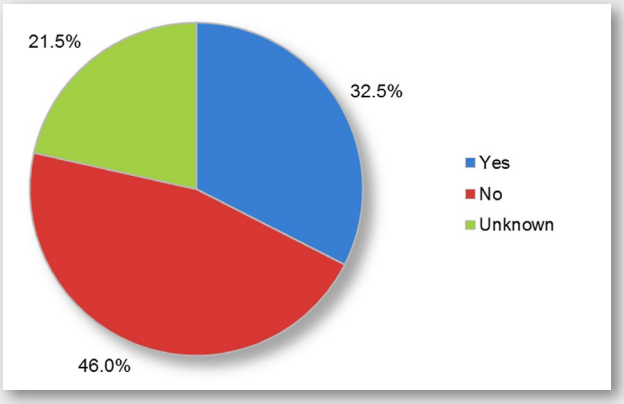



*Figure 14. Policies for Visibility and Management of IoT Devices*

However, 22% of respondents selected "Unknown," which likely means they do not have such a policy in place. It could be argued, then, that two-thirds of respondents don't have a strong policy foundation for secure IoT use.

## Monitoring IoT

Respondent organizations are clearly trying to achieve the visibility they need, with 41% of respondents actively collecting management or visibility information from Things on their networks (see Figure 15).

**Are you collecting management or visibility information from the "Things" on your network?**

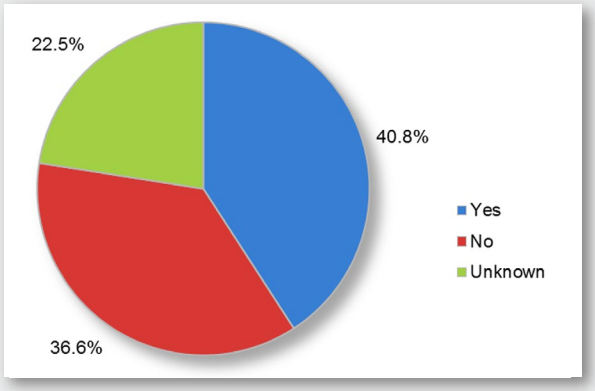



*Figure 15. Collection of Management or Visibility Information*

From these responses, it appears that some have skipped the policy development step and jumped right into visibility and inventory control implementation on their networks.

From an auditing/compliance point of view, this is a bad thing—policy should always drive process, which then drives architecture, which then drives control. However, one of the first steps in policy is knowing what you need to protect and how to protect it, which points back to visibility. Also, in the real world of rapidly changing technology, controls often have to be updated and modified more quickly than policy can be drafted, reviewed and approved. IoT adoption will only exacerbate this trend.

*In the real world of rapidly changing technology, controls often have to be updated and modified more quickly than policy can be drafted, reviewed and approved. IoT adoption will only exacerbate this trend.*

## IoT Security Data Collection

Again, a large percentage of respondents skipped this question; it appears that only those who were actively collecting IoT security data answered. As illustrated in Figure 16, log or security information and event management (SIEM) products are the dominant choice at 67%, with another 16% choosing log collectors, which may also indicate early log management-centric SIEM products.

**How are you collecting security and operations data about "Things" on your network?**

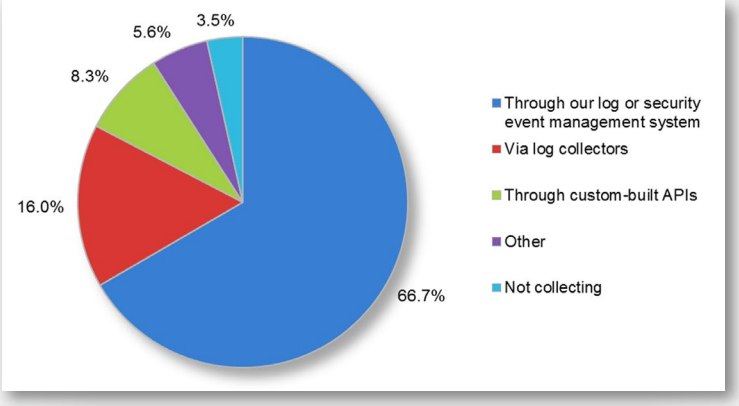



*Figure 16. Security Data Collection Methods*

*While 67% of respondents are using SIEM technology to collect IoT security data, only 55% felt the information was in a form usable for visibility and investigation.*

This response shows a high dependency on SIEM products for dealing with the vast number of devices and the jump in security data volume that the IoT may bring. Experience has shown that not all SIEM products and even fewer SIEM implementations are likely to be able to meet those performance challenges.

The embedded computing capabilities in many IoT devices will also present obstacles to the syslog- and agent-centric collection approaches used by SIEM products. For example, while 67% of respondents are using SIEM technology to collect IoT security data, only 55% felt the information was in a form usable for visibility and investigation, reflecting some realization of the limitations of existing SIEM deployments (see Figure 17).

**Is your monitoring and event data from "Things" normalized and usable for visibility and investigations?**

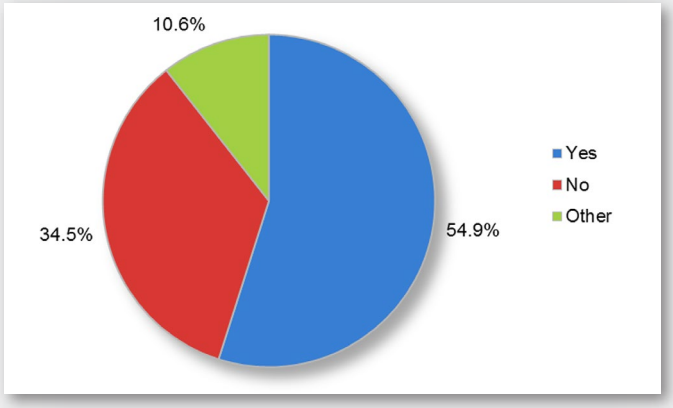



*Figure 17. Usability of Monitoring Data*

This suggests that SIEM vendors need to invest in making their monitoring and event data more usable and scalable for security professionals who will be faced with securing a multitude of diverse devices, many of which are using embedded operating systems and applications.

## Other Security Controls

When asked what security controls were being used to secure existing use of IoT, the top four categories were authentication/authorization (68%), system monitoring (65%) and, in a tie for third place, both encryption of communications and security evaluation and testing of new Things prior to production (52%), as shown in Figure 18.

**What controls are you using currently to protect against the risks imposed by new "Things" on your network? What controls do you plan on deploying in the next 2 years to address these issues?**

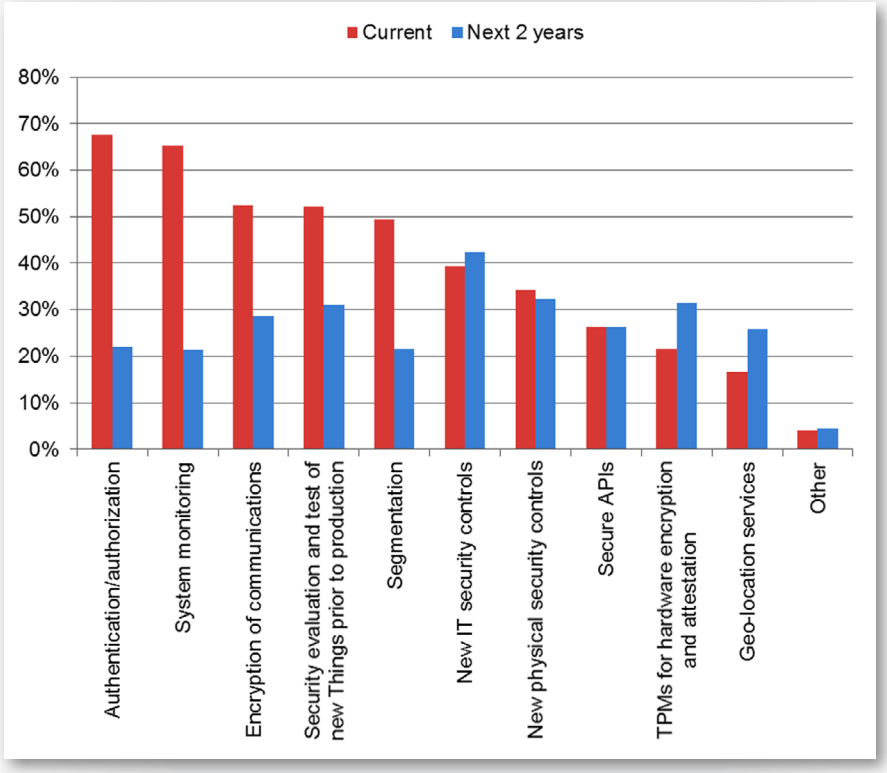



*Figure 18. Security Controls*

Because the most common current IoT application cited was consumer devices (as shown previously in Figure 8), the respondents are likely indicating existing use of remote access security for smartphones and tablets that users are allowed to connect. The high percentage (52%) of respondents indicating "Security evaluation and test of new Things prior to production" probably also reflects mobile remote access as the dominant existing IoT application. Testing is often done before approving smartphones/tablets for production use in an enterprise to determine if the device can support required corporate policy.

However, extending authentication and encryption out to devices that use embedded computing, such as medical machinery, building automation, process control and other similar devices, will be difficult because those devices do not have "users" in the traditional PC/smartphone/tablet sense, which complicates the initial authentication/key exchange process. We have already seen similar problems extending WLAN security such as WPA2 out to devices such as wireless printers. The wide array of devices on the IoT will exacerbate this issue.

System monitoring, mostly via SIEM products, was cited as the second most common security control (65%) currently in use to secure Internet Things. However, SIEM products generally rely either on syslog reporting capabilities or cooperative host-based agents on endpoints to collect information. Neither of these functions will be supported by many future Internet Things, which will cause blind spots in future monitoring processes.

Network segmentation was the fourth place control, cited by 49%, which is a good thing. Despite a decade of hype around the "disappearance of the perimeter," the reality for business is that there will always be perimeters, and there will always be different zones of trust. What changes is how and where the perimeters and zones are enforced. Different classes of IoT devices will most likely be connected via different DMZ architectures, using technologies such as air gaps to protect control systems from the rest of the network, or network access control (NAC) to determine the risk of a device connecting into the network and the appropriate access to grant it.

*Despite a decade of hype around the "disappearance of the perimeter," the reality for business is that there will always be perimeters, and there will always be different zones of trust. What changes is how and where the perimeters and zones are enforced.*

# Conclusions

The SANS Securing the "Internet of Things" Survey results show that while the term *Internet of Things* has been wildly overhyped, security professionals are already dealing with the first several waves of Internet-connected Things and have begun to plan for the challenges of the next wave of more diverse, more complex devices. Currently adopted internal controls are insufficient to deal with many of today's IoT devices; alternative controls or technological advances need to be adopted to maintain effective internal controls. Many are starting from security strategies and controls based on securing user devices, such as smartphones and tablets. Almost 90% of respondents recognized that changes to security controls will be required, with 50% believing major (if not complete) enhancements and replacements to many controls will be required.

Of survey participants, 67% rely on SIEM products and 16% rely on log collectors to collect data on IoT devices. Furthermore, of the 67% who rely on SIEM products, only 55% felt the information was in a form usable for visibility and investigation—a harbinger of the potential scalability and performance challenges that lay ahead for SIEM implementations in the IoT era. As summed up in the comments of one survey respondent, "… mechanisms to audit 'Things' are very weak."

*The majority of respondents expected IoT device manufacturers to take a larger level of responsibility for security than security professionals have expected of PC and server hardware and application vendors in the past.*

Internet-connected computing capabilities related to smart building and industrial control systems and medical devices were the most commonly cited concerns after consumer devices. While these type of devices don't receive much hype with respect to the IoT in the press, the use of embedded computing in those devices (versus layered operating systems and applications in PCs and servers that IT is accustomed to managing and securing) will cause major breakage in existing IT management and IT security visibility, vulnerability assessment, configuration management and intrusion prevention processes and controls.

Reflecting this change, the majority of respondents expected IoT device manufacturers to take a larger level of responsibility for security than security professionals have expected of PC and server hardware and application vendors in the past. More than half plan on having to do their own evaluation and testing of devices before allowing them on the corporate network. These results suggest that manufacturers who invest in secure development life cycles for their IoT products and provide both visibility into vulnerability levels and support for patching and updating will see competitive advantages when selling to enterprises.

The majority of respondents express concerns that SANS believes are dead on: The devices coming are very different from traditional PCs and servers. The basic critical security controls, such as hardware and software inventory, vulnerability assessment and configuration management, will face new barriers to success if manufacturers don't increase their level of attention to security and if enterprise security processes and controls don't evolve. Product managers should use these results as a driver to increase investment in secure development life cycles that result in more secure products. Security managers should analyze their current and planned security architectures to determine how well they are positioned to deal with the security issues of the current, and coming, Internet of Things.

# About the Author

**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 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.

Mr. Pescatore 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.

# Sponsors

*SANS would like to thank this paper's sponsors:*

CODENOMICON

NORSE

Last Updated: April 7th, 2018

# Upcoming SANS Training

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

| | | | |
|---|---|---|---|
| SANS Zurich 2018 | Zurich, CH | Apr 16, 2018 - Apr 21, 2018 | Live Event |
| SANS London April 2018 | London, GB | Apr 16, 2018 - Apr 21, 2018 | Live Event |
| SANS Baltimore Spring 2018 | Baltimore, MDUS | Apr 21, 2018 - Apr 28, 2018 | Live Event |
| Blue Team Summit & Training 2018 | Louisville, KYUS | Apr 23, 2018 - Apr 30, 2018 | Live Event |
| SANS Seattle Spring 2018 | Seattle, WAUS | Apr 23, 2018 - Apr 28, 2018 | Live Event |
| SANS Doha 2018 | Doha, QA | Apr 28, 2018 - May 03, 2018 | Live Event |
| SANS Riyadh April 2018 | Riyadh, SA | Apr 28, 2018 - May 03, 2018 | Live Event |
| SANS SEC460: Enterprise Threat Beta Two | Crystal City, VAUS | Apr 30, 2018 - May 05, 2018 | Live Event |
| Automotive Cybersecurity Summit & Training 2018 | Chicago, ILUS | May 01, 2018 - May 08, 2018 | Live Event |
| SANS SEC504 in Thai 2018 | Bangkok, TH | May 07, 2018 - May 12, 2018 | Live Event |
| SANS Security West 2018 | San Diego, CAUS | May 11, 2018 - May 18, 2018 | Live Event |
| SANS Melbourne 2018 | Melbourne, AU | May 14, 2018 - May 26, 2018 | Live Event |
| SANS Northern VA Reston Spring 2018 | Reston, VAUS | May 20, 2018 - May 25, 2018 | Live Event |
| SANS Amsterdam May 2018 | Amsterdam, NL | May 28, 2018 - Jun 02, 2018 | Live Event |
| SANS Atlanta 2018 | Atlanta, GAUS | May 29, 2018 - Jun 03, 2018 | Live Event |
| SANS Rocky Mountain 2018 | Denver, COUS | Jun 04, 2018 - Jun 09, 2018 | Live Event |
| SANS London June 2018 | London, GB | Jun 04, 2018 - Jun 12, 2018 | Live Event |
| DFIR Summit & Training 2018 | Austin, TXUS | Jun 07, 2018 - Jun 14, 2018 | Live Event |
| SANS Milan June 2018 | Milan, IT | Jun 11, 2018 - Jun 16, 2018 | Live Event |
| SANS ICS Europe Summit and Training 2018 | Munich, DE | Jun 18, 2018 - Jun 23, 2018 | Live Event |
| SANS Cyber Defence Japan 2018 | Tokyo, JP | Jun 18, 2018 - Jun 30, 2018 | Live Event |
| SANS Philippines 2018 | Manila, PH | Jun 18, 2018 - Jun 23, 2018 | Live Event |
| SANS Oslo June 2018 | Oslo, NO | Jun 18, 2018 - Jun 23, 2018 | Live Event |
| SANS Crystal City 2018 | Arlington, VAUS | Jun 18, 2018 - Jun 23, 2018 | Live Event |
| SANS Minneapolis 2018 | Minneapolis, MNUS | Jun 25, 2018 - Jun 30, 2018 | Live Event |
| SANS Cyber Defence Canberra 2018 | Canberra, AU | Jun 25, 2018 - Jul 07, 2018 | Live Event |
| SANS Paris June 2018 | Paris, FR | Jun 25, 2018 - Jun 30, 2018 | Live Event |
| SANS Vancouver 2018 | Vancouver, BCCA | Jun 25, 2018 - Jun 30, 2018 | Live Event |
| SANS London July 2018 | London, GB | Jul 02, 2018 - Jul 07, 2018 | Live Event |
| Pre-RSA® Conference Training | OnlineCAUS | Apr 11, 2018 - Apr 16, 2018 | Live Event |
| SANS OnDemand | Books & MP3s OnlyUS | Anytime | Self Paced |