Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Metrics for Operational Security Control

This paper aims to inform the reader on what metrics are, why metrics can be an important tool for controlling security systems; and, how metrics fit into the day to day IT operations to improve security by measuring, reporting and tracking key elements of systems that have an impact on security. The paper will include examples of systems for which metrics can be collected, what metrics can be collected for each system and how the metrics can be presented to provide control information on the system being examined. The...

Copyright SANS Institute
Author Retains Full Rights

AD

GIAC Security Essentials Certification (GSEC)

Practical Assignment
Version 1.4b (amended August 29, 2002)
Option 1 - Research on Topics in Information Security

Title: "Metrics for Operational Security Control"

By: Rich Cambra

Date: 4 July, 2004

Abstract:
This paper aims to inform the reader on what metrics are, why metrics can be an important tool for controlling security systems; and, how metrics fit into the day to day IT operations to improve security by measuring, reporting and tracking key elements of systems that have an impact on security. The paper will include examples of systems for which metrics can be collected, what metrics can be collected for each system and how the metrics can be presented to provide control information on the system being examined. The paper will also explore options to "build or buy" as well as list organizations that promote the use of metrics as a tool and organizations that have specialized experience using metrics for security.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

A metric is defined as:

> A measurement, taken over a period of time, that communicates vital information about a process or activity. A metric should drive appropriate leadership or management action. Physically, a metric package consists of an operational definition, measurement over time, and presentation.[1]

Units of measurement for a metric can include counts, frequency, percentages as well as physical values. A metric is different than a measurement in a couple of ways: it is collected over time and is used to compare with previous values. These values that are collected are then compared to the desired value, or "baseline" of the system we want to control. It is the ability to control a process when you use metrics that make it a valuable tool to IT operations and information security.

Lord Kelvin had a quote that shows us why we need metrics –

> When you can measure what you are speaking about and express it in numbers, you know something about it. But when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meager and unsatisfactory kind. It may be the beginning of knowledge but you have scarcely advanced to the stage of science

This was also summed up very simply and elegantly by Tom Demarco, who said: "*You can't control what you can't measure."* In the world of security and operations it is important to be able to control systems, and metrics provide us a means to ensure we have control or to identify when we may have lost control. The ability to identify a loss of control can be important in addressing a security issue quickly and limiting the impact(s) resulting from the loss of control.

Many processes use metrics, one of the most prominent and widely known is simply called Six Sigma. It focuses on controls that eliminate waste and was originally developed at Motorola to improve the quality of their output (reduce the number of failures/problems per attempts) The concept of Six Sigma is to reach a failure rate of 3.4 problems per million, or 99.99966% accuracy. With the emphasis of "five nines" reliability for IT systems, you can see there is a great deal of commonality that can be leveraged. Avoiding waste and downtime save money and make your company more profitable. Using metrics is one way to help achieve these levels of accuracy and reliability.

It is important to use "good" metrics, a good metric is ***S.M.A.R.T***

Specific: Targeted to the area being measured, not a byproduct or result
Measurable: Data can be collected that is accurate and complete

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Actionable: Easy to understand the data and take action on it
Relevant: Measure what's important with the data
Timely: The data is available when you need it

A metric that is specific must measure a property of the system directly, it can't be derived from a combination of different measurements and it should not rely on measurements from other systems. Anti Virus is a key element of any operations security policy and there are many specific metrics that can be gathered on the number of viruses detected, the number of machines protected, and the number of machines lacking current virus definitions.

Ensuring a metric is measurable seems too obvious, except the industry we work in has so many relative terms and descriptions to identify security status. Being able to put a value to something that can be measured permits us to graph it and compare it over time, which enables us to see if we are controlling our system, and to what degree we are able to control our system. Using our example of anti virus we can easily see that getting a percentage of machines that have virus definitions out of date is measurable and provides more value than saying "we have anti virus software installed on all our machines so we must not be at risk".

Actionable metrics are important, for if we can't take action on the information the metric gives us, why bother to collect the data in the first place? If we can't decide on an action to take when we review the metric we do nothing but "cry wolf" and provide distraction from the things we can be doing something about. Knowing the number of systems that do not have updated anti virus definitions is something we can take action on and use to evaluate our risk in case of a virus outbreak. Knowing there were 3000 new viruses released last month just tells us there is a valid threat, but there is nothing we can do to reduce that number, it is beyond our control to affect the number of new viruses that are released. Actionable can also result in measures being taken that don't directly affect the metric that is being analyzed, but are systems that might be impacted by the metric if it is not in compliance.

Having relevant data is another "obvious" requirement, but can be more difficult to accomplish than it seems. We often will look at data and see what we can easily collect. We then learn that what we have collected isn't relative to what we want to control. Knowing the number of new viruses released each month may tell us how great the threat is, but does it allow us to control the virus threat? It may help us "sell" the fact we need Anti Virus protection but in the end it does nothing for us to actually control and improve our own process to prevent viruses in our own environment

Timely access to the data and reporting of the data is important because we are attempting to control a process or system. Given a process or system changes over time, we cannot use data that is too dated to attempt to control what is happening now. Each process has to be evaluated on its own merits to

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

determine the frequency at which data must be collected and reported on. Data collection intervals and reporting may be by the hour, day, week or even month, depending on what is being reported on. For normal operations it may be sufficient to have a weekly report showing the percentage of systems lacking the latest Anti Virus definitions; but, if a virus out break is reported, it may become necessary to have hourly reports on the status of virus definition updates. This would be necessary to ensure all systems have the latest protection as soon as possible. This would also tie into actionable measures for this metric. It may be decided to shut down internet connections, block e-mail or take other actions until the number of systems with updated anti virus definitions is back within acceptable levels as shown by the metric.

Knowing what makes a "smart" metric, we must also take care to limit the number of measurements we will commit to take and analyze. When creating a metrics program to monitor and control a system or process, it is easy to become overwhelmed with the collecting and analysis of the data. It is important to limit initial efforts to a few key areas that can provide the greatest return for the effort expended in collecting the data that will provide the metrics on the system you want to control. Understanding what you are measuring, why you want to measure it, who you are going to present the results of these measurements to and how you will present those metrics is the first step in developing a successful metrics program.

Get management buy in. This cannot be overstated. Without the support of management, the metrics program will not be given the resources to be successful. You must know what your "sponsor" will want out of your efforts and how it will benefit him to have you collect and analyze these metrics. Metrics should enable you to reduce waste and improve reliability, which decreases overall IT costs and that is the language management understands. Management will also need to be aware of actions that may be required to bring metrics that are not within the desired range back into control. If management will not be able to act on the information the metrics show, it can cause frustration to continually see an out of compliance system that is not improving.

A simple way to start a metrics program is to create two lists of systems. The first list of systems would be those you want to control. The second list of systems would be those you can find and collect metric data on. By comparing the two lists you will be able to identify the systems that you can collect "SMART" metrics from and which you desire to control. Then the "customer" in management who would be interested in the collection and analysis of these metrics must be identified. Be prepared to tell them what information they will be provided, how often you will provide the information, how the information will be presented, what value the information provides and what actions may be taken on the information. These are some basic step in the process of building your own metrics program.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Identifying sources to collect metric data from can be a challenge. There are many places to look when you start the process of collecting data. Some example sources to collect data from include:

- Application data sources: Many applications collect data that can provide metrics as part of their function that can then be analyzed. An example would be an anti virus application running on servers that can report all the machines that are managed, and which of those machines have updated virus definitions.
- System logs: Log can be parsed for relevant data or events to provide metrics on a variety of security areas, use of a log shipping server, with automated log reviews can collate and provide data to use as metrics. This can be very valuable to evaluate metrics such as password resets, locked accounts, access failures or other security events that can be tracked to evaluate cost and risk to IT systems.
- Systems designed to collect & report on other systems. There are a number of commercial applications that will collect and report on a wide variety of system information. The results of these products become much more useful when metrics are created that permit control and action to be applied to what is being measured. Without this element the collected information is so much "noise" that provides no benefit.

Some simple general rules can be followed to create a metrics program for a system you want to control.

- Start with a system you know is important to your company's security policies and for which you can gather reliable data
- Pick 3-5 metrics you can use to evaluate the effectiveness of your security policy
- Establish how often the data will be collected, analyzed and reported.
- Know who the information will be reported to, how it will be reported and who will be responsible for taking action if the information dictates it.

An Example metric program formulation – Anti Virus systems metrics

- Anti-Virus systems and security measures are a key element in any companies security policies
- Successful application of Anti-Virus measures are critical to prevent significant impacts to the business
- A centralized anti-virus solution has logging and reporting that can be leveraged to create useful metrics to gage the effectiveness of the companies anti-virus efforts

Given we know anti virus is important to the company, the following are our 3-5 metrics of interest we can collect every week for analysis

- Number of systems running anti virus software & total number of systems that should have anti virus software installed
- Number of systems without updated virus definitions
- Number of systems without a recent virus scan (weekly)

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Knowing the number of systems that are running anti virus software and the total number of systems that require protection ensures all systems are protected with anti virus software or informs you of systems at risk for infection from viruses. Knowing the number of each type of system also permits us to normalize the other data being collected so it is easier to evaluate. In the example below we will normalize the data by dividing the number of systems without updated virus definitions by the number of systems running anti virus software to give us a percentage of managed systems with outdated virus definitions. Then if the total number of systems changes over time, we can still compare the percentages to see if we have an increase in the rate of systems with dated virus definitions.

It can be noted that the list of Anti Virus metrics did not include any counts of the number of infected systems, the number of virus detections or the number of e-mails with virus attachments. It is important to remember that one of the reasons for collecting metric data is the desire to control a system or process. When we look into what drives the "numbers" for each of these anti virus values, we can't control them. They are subject to the number of systems that are infected and propagating the virus, the number of new viruses written and manage to spread "in the wild" as well as many other factors beyond our control. What we can measure and control are the metrics listed above, for instance the percentage of systems that are protected against known viruses. Thus we also have to accept the risk that we can't protect against the unknown, but we can at least make sure we are protected against the known virus threats by using metrics to report on our percentage of unprotected systems and taking action on that data to drive it to as close to zero as possible.

Example of collecting, analyzing and presenting metric data on "*Systems without updated virus definitions*". A simple spreadsheet can be used to record the relevant data captured by the Anti Virus servers. Attempting to analyze the numbers by looking at the raw data of the number of systems without updated virus definitions each week makes it difficult to arrive at any significant conclusions. By also recording the number of PC's reporting at each site, and then normalizing this to arrive at a percentage of PCs infected at each site we begin to get a better feeling for each sites rate of infection.

# of systems without updated virus definitions

	1	**2**	**3**	**4**	**5**
Site A	25	33	28	32	31
Site B	5	6	6	5	6
Site C	5	7	11	11	12
Site D	7	6	7	7	8

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

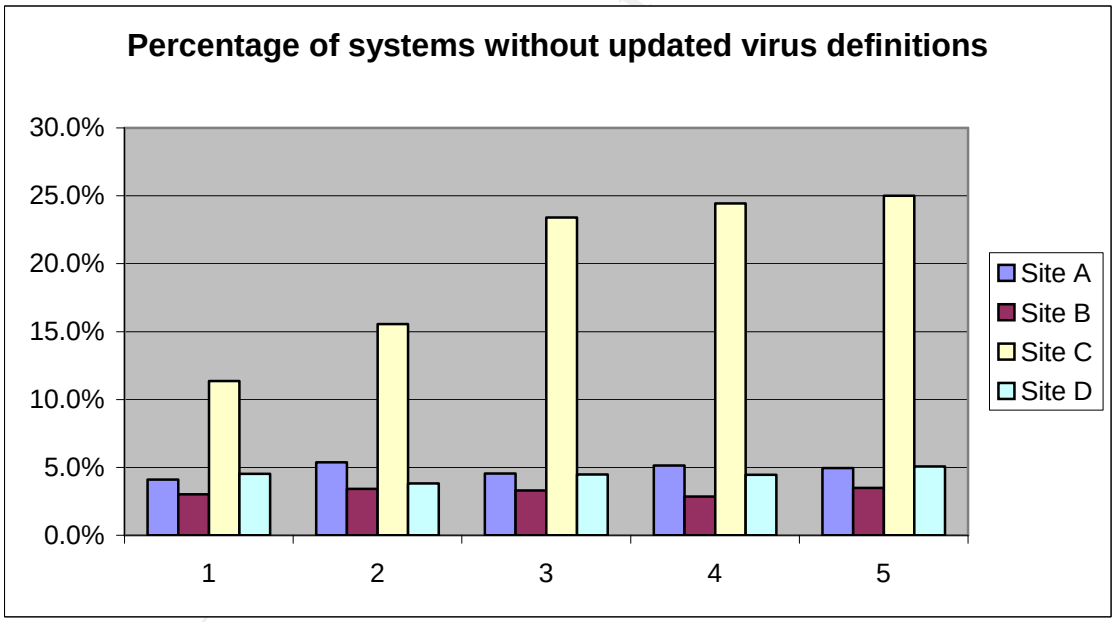
# of systems at each site

	1	2	3	4	5
Site A	611	615	616	622	625
Site B	166	175	182	176	172
Site C	44	45	47	45	48
Site D	155	157	156	157	158

% of systems at each site without updated virus definitions

	1	2	3	4	5
Site A	4.1%	5.4%	4.5%	5.1%	5.0%
Site B	3.0%	3.4%	3.3%	2.8%	3.5%
Site C	11.4%	15.6%	23.4%	24.4%	25.0%
Site D	4.5%	3.8%	4.5%	4.5%	5.1%

The next step is to create a graph from the data in this spreadsheet to give a quick visual image of the percentage of systems at each site that don't have updated virus definitions.



The graph shows the percentages for each site over time and we can see that Site C has an increasing number of systems each week that lack current virus definitions. Given this information we can investigate the cause of this trend and correct it before it causes a major disruption to the business. We can also evaluate the remaining sites compliance and compare it to historical trends and say less than 5% of systems having old virus definitions is normal. This can be attributed to employees on travel or vacation and the systems may be off or not connected to the network to get the updated virus definitions.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Presentation of your metric data can be as important as its accuracy. This doesn't mean you manipulate the data in ways that are false, but that you ensure the way the data is presented makes it easy to understand its meaning. If management cannot quickly see what the data is "showing" them, it may be ignored with potential consequences. Ensure the presentation of the data is clear, and make recommendations when the data warrants it so the time and effort spent to collect, and analyze the data isn't wasted.

Anti virus systems are only one area where useful metrics can be collected and analyzed. Examples of other systems for which relevant metrics can be gathered include:

- Account management & control
- Firewalls
- Anti Spam / E-mail content management
- Web content management
- System security policy monitoring

Account management & control is important because one of the primary sources of security breeches comes from internal sources. By monitoring and controlling accounts you help to prevent the use of those accounts for attacks into your systems. Unused or "orphaned" accounts are an invitation for someone to attempt access for which they are not authorized. Metrics that can be collected and analyzed include:

- Total number of accounts
- Number of accounts never logged in
- Number of accounts not logged in last 30 days/60 days
- Number of Administrator accounts
- Number of service accounts

Firewalls have a number of metrics that can be monitored for control. Knowing what is occurring on the firewall can give timely notification of attacks, or abuse of a company's internet connection.

- Number of authorized connections (by type)
- Number of connections dropped (by type)
- MB processed by connection type
- Count of attack patterns detected

Anti Spam / E-mail content management have become an important part of a company's security systems. The amount of spam that comprises all e-mail on the internet continues to grow and the loss to business because of bandwidth, storage and employees time is significant. Knowing that spam controls are set to the appropriate levels to keep out the majority of spam, while permitting legitimate business e-mails is vital to the operation of the business.

- Number of e-mails processed
- Number of e-mails rejected for spam/content restrictions

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

- MB of e-mail rejected (bandwidth)
- Number of outbound e-mails with inappropriate content
- False spam identification rate

Internet Access management has an important place in reducing employee distractions and preventing lawsuits because of inappropriate internet use. The cost of internet bandwidth, lost productivity to web surfing and potential legal liabilities mean these systems provide valuable metrics that can be acted upon.

- Top abusers (time/MB of internet use)
- Restricted/banned site access attempts
- "Surf time" statistics by user
- "Surf time" statistics by site visited
- File downloads restricted/blocked

System security policy monitoring is important to ensure all systems meet corporate standards. An active program of monitoring can identify systems that are non compliant and the tracking of the metrics can show how effective a company is at preventing and/or eliminating non compliant systems.

- Percentage of systems compliant to OS hardening standards
- List of systems non-compliant and issues to be addressed by system
- Patch status verification, percentage of systems patched to requirements

These are just some of the areas that can be controlled by the proper use of metrics. Understanding the systems in your company and what data is there to be collected is an important element and should enable you to choose which systems and data to start a metrics program with. There must be a commitment to metrics at all levels of the organization. Lack of support from the people required to collect the data may result in data being lost or the accuracy of the data being suspect. Metrics will only provide value if they are consistently measured on a regular basis. If metrics are not used to control and improve the systems they are monitoring, it is a waste of time to collect them and will be abandoned for more productive work. Metrics are only of value if they are used to drive improvements to the systems you are monitoring and desire to control. Taking the time to collect the data and analyze the metrics and then not taking action on the information when required makes the effort much less valuable.

Efforts to implement a metrics program can fail for a number of reasons. I have pointed out some of the more common issues with implementing a metrics program, but Karl E. Wiegers has created a "top ten list" in which he not only gives a list of ten problems a software metrics program may encounter, he describes the symptoms and the solutions for escaping from each of those "traps" While his list was focused on software metrics, it still contains many elements that apply to any metrics program, including those relating to security systems.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Software Metrics: Ten Traps To Avoid

Trap #1: Lack of Management Commitment
Trap #2: Measuring Too Much, Too Soon
Trap #3: Measuring Too Little, Too Late
Trap #4: Measuring the Wrong Things
Trap #5: Imprecise Metrics Definitions
Trap #6: Using Metrics Data to Evaluate Individuals
Trap #7: Using Metrics to Motivate, Rather than to Understand
Trap #8: Collecting Data That Is Not Used
Trap #9: Lack of Communication and Training
Trap #10: Misinterpreting Metrics Data

There are a number of public organizations that provide resources and information about the use of metrics. The concept of Six Sigma was introduced earlier, and iSixSigma promotes certification, training and general awareness about Six Sigma. This organization has many papers that can provide valuable background on metrics and process controls that are not specific to Information Security. Information can be found at www.isixsigma.com Other organizations such as the National Institute of Standards and Technology (NIST) has published a guild on Information Technology Security Metrics. Other organizations exist or are being formed out of the commercial applications market. SecMet is an example of such an organization and information on SecMet can be found at www.secmet.org.

If time, skills and experience prevent an organization from building their metrics program on their own, there are also options to "buy" a commercial solution. There are several company's that have started to promote their commercial systems to prove the value of Information security through metrics (and thus the cost to purchase and implement their systems). Commercial systems can certainly jump start your efforts and provide a more "professional" result than a home grown system. Issues with commercial systems include having to learn their system, while also dealing with your own systems. You also have to understand that systems which are easier to set up "out of the box" may be less flexible than what you can build on your own. This may result in a program that is not exactly what you anticipated or desired. Building your own program by starting with a few key metrics can show the value of the information and could justify a commercial program at some later point. Some vendors that provide commercial systems are listed at the end of the references section for those who wish to investigate this option.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Summary:

Metrics can be a valuable tool to those who are in Operations and need to maintain systems in accordance with security policies. It can also provide valuable information on security systems such as anti virus, firewalls, spam, content management and the like. Metrics can measure compliance, show trends and reveal issues before they become significant security risks or result in losses. The information provided by metrics needs to be acted on for the metrics to be effective. Metrics programs can be built “in house”, or can be created with the assistance of commercial systems. As with any of the tools available, metrics are an option that must be weighed for its cost benefit. If the time and effort to collect and analyze the data does not provide a payback greater than the cost of those recourses, then metrics are not worth pursuing. When the proper metrics are chosen they can provide valuable insight and control into our systems to ensure they are secure in a very cost effective manner.

© SANS Institute 2004, Author retains full rights.

References:

[1] Service Quality Network "SQN - Glossary "2002/06/19 URL: http://www.oly-wa.us/sqn/Glossary.htm

[2] Wiegers , Karl E. "Software Metrics: Ten Traps To Avoid" URL: http://www.processimpact.com/articles/mtraps.pdf

Swanson, Marianne; Bartol, Nadya; Sabato, John; Hash, Joan; Graffo, Laurie "Security Metrics Guide for Information Technology Systems" NIST Special Publication 800-55. July 2003. URL: http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf

Pyzdek, Thomas "The Six Sigma Revolution" http://www.qa-inc.com/knowledgecente/articles/PYZDEKSixSigRev.htm

"SPC Resources – 8 Step Metrics Program" http://www.spc.ca/resources/metrics/8steps.htm

Robinson, Chad. "Collecting Effective Security Metrics" April 9th, 2004 http://www.csoonline.com/analyst/report2412.html

Hale, John. "IT Security Metrics" URL: http://esm.cis.utulsa.edu/SecurityMetrics.pdf

Burris, Peter; King, Chris. "A Few Good Security Metrics" 10/11/2000 URL: http://www.metagroup.com/metaview/mv0314/mv0314.html

Katze, Stuart. "Security Metrics" URL: http://philby.ucsd.edu/~cse291_IDVA/papers/rating-position/Katzke%20briefing.pdf

Frank, Diane. "Agencies Seek Security Metrics" June 19, 2004 URL: http://www.fcw.com/fcw/articles/2000/0619/pol-metrics-06-19-00.asp

Nygård ,Arne Roar "Security metrics in SCADA networks" December 16. 2003. URL: http://nislab.hig.no/Research/docs/arnern.pdf

Bicknell, Paul "Security Assertions, Criteria, and Metrics Developed for the IRS" http://www.mitre.org/work/tech_papers/tech_papers_01/bicknell_security/bicknell_security.pdf

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Metrics Security Organizations and Commercial Security Product Providers

Hachman, Mark. "Security Metrics Consortium Formed" February 25, 2004
http://www.eweek.com/article2/0,4149,1538410,00.asp?rsDis=Security_Metrics_Consortium_Formed-Page001-120180

http://www.secmet.org/
http://www.secmet.org/SecMet_Release.pdf

http://www.paladintek.com/Ppt/Security%20Metrics.ppt

"Using Foundstone's FoundScore$_{TM}$ to Assign Metrics and Measure Enterprise Risk" 2003 URL:
http://www.foundstone.com/resources/whitepapers/wp_securitymetrics.pdf

http://www.j2ktechnology.com/products_services/security/smart.html

http://www.sse-cmm.org/index.html
http://www.sse-cmm.org/metric/metric.asp

http://www.entityinc.com/collateral/smart.pdf

© SANS Institute 2004, Author retains full rights.

Last Updated: June 19th, 2013

Upcoming SANS Training

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

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**