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.

It's Time to Rethink your Corporate Malware Strategy

Due to a variety of reasons which will be outlined in this paper, signature-based antivirus scanning is becoming largely ineffective as the main tool against newer varieties of malicious computer code. Scanning performed at the gateway and server level, while still valuable, is proving inadequate as well. It is becoming evident that behavior-based policy enforcement middleware, deployed at the edge of the corporate network (PC workstations), will be required in the near future to handle known and unknown threats. Unfor...

Copyright SANS Institute
Author Retains Full Rights

AD
Symantec™
Endpoint Protection 12
The next generation of reputation-based security
Download the beta
Symantec.
Confidence in a connected world.

It's Time to Rethink your Corporate Malware Strategy

Nick Del Grosso

GSEC Practical Assignment v1.3
February 24, 2002

Summary

Due to a variety of reasons which will be outlined in this paper, signature-based antivirus scanning is becoming largely ineffective as the main tool against newer varieties of malicious computer code. Scanning performed at the gateway and server level, while still valuable, is proving inadequate as well. It is becoming evident that behavior-based policy enforcement middleware, deployed at the edge of the corporate network (PC workstations), will be required in the near future to handle known and unknown threats. Unfortunately, the big players in this industry currently are not incorporating the required technologies into their product lines, nor does it appear that they will be doing so in the near future. IT managers wanting to utilize these technologies today will have to take a chance on the smaller security software vendors.

The purpose of this paper is not to review specific existing behavior-based policy enforcement middleware products or technologies in detail, but to make a case for their immediate further evaluation and incorporation into a corporate strategy. Specific evaluations could be the subject of a future paper.

Background

Traditionally, hostile code has been classified into three categories based upon the behavior of the code: viruses, worms, and trojans. These lines of distinction are now blurring, partly because of many recent instances of malicious code that incorporate numerous methods of infection and transmission.

Newer threats include ActiveX, Java, and JavaScript code in HTTP data streams, which are often referred to as "mobile code" since these programs are written to run on a wide variety of computer platforms. This term, however, seems to be going out of favor since it confuses users into believing there is an exclusionary association with wireless or portable devices.

The term “active content” includes ActiveX, Java, JavaScript/JScript, VBscript, macros, browser plug-ins, scrap files, Windows scripting host files, and Postscript. This code runs in the context of the user signed on to a PC, and thus can do everything that the user can do. Another term that seems to be gaining in usage, “vandal”, is defined as any malicious auto-executable application, which includes the above-mentioned active content.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Because Java applets are considered to be untrusted code, they are run within a virtual machine that uses a sandbox approach to theoretically restrict what they can do, preventing inappropriate actions on the users' computers. ActiveX is widely considered to be the greater threat because it's essentially a compact version of OLE, which permits direct access to native Windows calls and links them to system functions. Unlike Java, there are no built-in language restrictions controlling code behavior. ActiveX controls can be built utilizing many different programming languages.
A term which includes all forms of malicious code is "'malware"', short for "malicious software" and will be used throughout this text.

Many Internet web sites now rely on Java applets and ActiveX controls to create their look and feel. For these schemes to operate properly, these bits of mobile code are downloaded to the user's PC, where they gain access to the hard disk. Whichever component is used, outright blocking is no longer a viable possibility. Active content technologies have become necessary for businesses to function and compete effectively. Without these web components, web sites are reduced to static text and graphics with little or no interactivity.

Common corporate strategies today

In addressing a corporate strategy, it is important to define all of the functional points in the internetwork where malware detection and/or prevention can be implemented. These functional points include:

- corporate desktop PCs
- corporate network servers
- corporate Internet gateways
- the Internet itself as a transmission medium
- remote servers and connecting remote clients

A common and relatively effective strategy (up to now) used by many corporate environments is to incorporate two or more signature-based antivirus packages from different vendors. Using different packages improves the chance that a virus would be stopped since one product is usually more effective than another at detecting a particular virus. Also, vendors vary in their development and delivery of antivirus signature definitions.

One of the antivirus packages is installed at the desktop, the other typically at an email gateway. A third package could be installed on all network servers. Frequent signature updates are applied to all installations of the packages at a significant expense of time and money. This strategy, while expensive, was relatively effective in the past, but is becoming markedly less so now.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

As for active content security, corporations often rely on user education, and sometimes lockdown restrictions on browsers by using such tools as Microsoft's Internet Explorer Administration Kit (IEAK) or Netscape's Mission Control. In some cases, gateway-level blocking is performed to strip out all active content. This can be done by using a gateway product with a proxy, or by using a plug-in product in conjunction with a firewall. An example of this is Trend Micro's InterScan AppletTrap Content Vectoring Protocol (CVP) product utilized with Checkpoint Firewall-1.

The Problems with Conventional Methodologies

There are two main problems with conventional methodologies used against malware. The first includes deficiencies related to signature-based scanning technology, especially as associated with active content. The second deals with deficiencies of gateway and server-based scanning solutions.

Signature-Based Scanning Technology

The conventional method of malware scanning relies on recognizing known signatures by comparing the code in question to a proprietary signature database. This technology is tried-and-true and is very good at detecting known viruses. It should be noted that this is a detection technique as opposed to a prevention technique and is necessary to specifically identify malware for the purpose of cleaning or eradicating the code. Continual update of the signature database is required in order to maintain effectiveness. Someone always suffers with signature-based scanning since signatures have to be developed after an attack has occurred. Signature-based scanning technologies are becoming ineffective for many reasons:

- Vendors are slow to develop and distribute virus detection strings.
- Doesn't detect malware in ActiveX, Java applets, and JavaScript.
- Reactive technology.
- Sheer number of malware elements being released (databases are growing too large in size to rapidly scan; the need for frequent updates is becoming burdensome).
- Virus "toolkits" commonly available to make it trivial to generate new viruses.
- Technology is successfully being incorporated by malware authors to prevent detection: encryption, multipartite, polymorphism, stealth, etc.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- Corporations are often not timely in implementing new signature strings as updates to their gateways, network servers, and desktops.

- Malware taking advantage of email address books and almost universal connectivity have propagation rates measured in hours as opposed to the historical days and weeks. Malicious code can now infect corporations across the world at an unprecedented rate, much quicker than antivirus vendors can respond by releasing signature strings. An example is the LoveLetter incident occurring in May 2000, which infected millions of users within a matter of hours and cost corporations billions of dollars in lost time and productivity.

- The usage of packers or compression tools such as NeoLite, Shrinker, PKLite, AS-pack, Petite, and WWpack can change the binary signatures of executables, making it difficult or impossible for malicious code to be detected by conventional means. The inclusion of computer code to read every type of file compression software would cause the scanning programs to be significantly larger and slower.

- Applying updated antivirus signatures to mobile laptops is a very difficult task. Also, the size of antivirus signature databases is becoming prohibitive on devices such as Palms and Windows CE units.

Gateway-centric filtering and/or monitoring

The tried-and-true technique of filtering and monitoring at all access points, while still useful, is becoming less effective for several reasons:

- Gateway filtering slows down or "chokes" traffic. "Digitivity pioneered applet security using central servers to run and monitor code entering the network. But this struggling company realized the hard way that centralized monitoring is too slow. Executing the thousands of applets entering Ford's network would slow a Cray supercomputer to a crawl". (The Forrester Report, Network Strategies, Volume 12, Number 7, June 1998).

- Most products have a narrow focus on viruses, Java, and ActiveX. Other types of active content are usually ignored.

- Upcoming web services technologies such as Microsoft .NET and Sun Microsystems ONE, which will allow application-to-application communications using XML data constructs, will prove difficult to scan and

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

are not conducive to scanning delays. Increasingly, corporations will link their internal applications with those of their external partners and suppliers.

- Malicious code is now blending virus and wormlike capabilities and is designed to take advantage of multiple software vulnerabilities.

- Companies are opening new ports on their firewalls to enable application connectivity, often without due consideration of the security implications.

- Wireless connectivity is becoming much more prevalent, creating new demands on security infrastructure and personnel.

- Encryption will be built in to all TCP/IP protocols in the future (VPN, PKI, IPSEC). A solution at the gateway could be to decrypt the code, scan it, and encrypt it again, but this would be very inefficient.

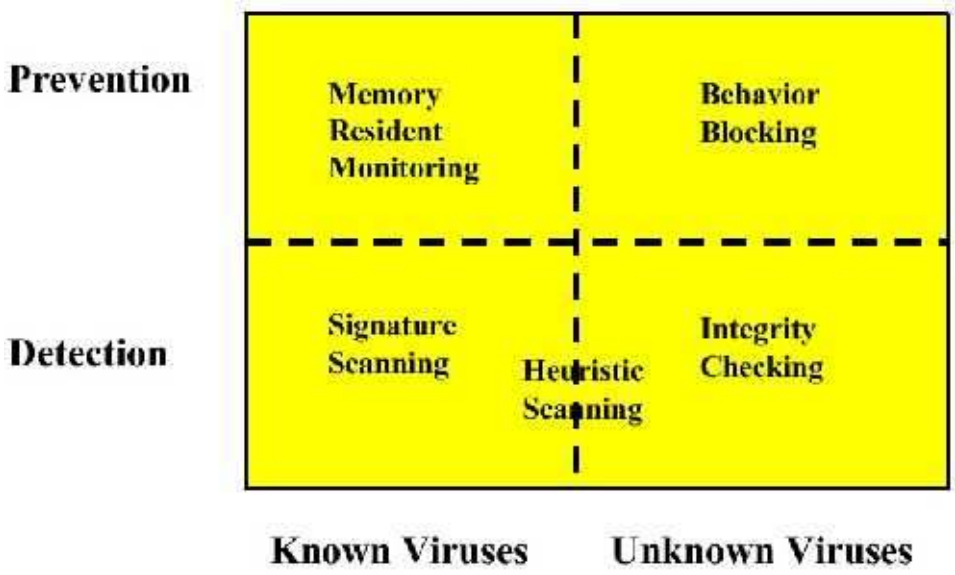
- Users often bypass the centralized access points by using dial-up modems and personal ISP accounts.

- Users often bypass the centralized email malware and content filtering servers (products as MailSweeper) by using Web-based email or instant messaging services. The latter services often utilize file-transfer features (some even unattended), greatly exacerbating the problem.

- Videoconferencing and Internet-collaboration technologies will soon become the norm, further increasing the requirements for bandwidth and the corresponding strain on gateways.

Potential Solutions

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.



Source: Joe Wells, Wells Research Workshop, May 1999.

This chart from Joe Wells (referenced from Browde and Smith) depicts how various technologies can be classified according to their prevention and/or detection characteristics, and their usefulness in malware recognition. (While the chart mentions viruses, we can logically extend this to include all malware). These technologies are further discussed below:

- Signature scanning – This technology has already been discussed. The chart capably depicts that it is a useful technology only for the detection of and prevention against known malware (this excludes most active content).
- Heuristic scanning – Heuristics extends the capabilities of scanners because it is not limited to known viruses. It uses rules and/or algorithms that identify suspicious looking code. There is a greater risk of false alarms as compared to standard scanning. While this is a detection technique, some call heuristic scanning "intelligent guessing". Heuristic scanners do not eradicate viruses since they don't have enough information to remove or clean the code.
- Integrity checking – This is a detection technique which checks the state of every application file for changes in the CRC. If the state has changed a possible malware alert is generated. Some products will create several small program files on startup as bait for viruses. The files will be immediately closed and examined for tampering. While integrity checking is a very useful technology, the problem is that alerts occur after the infection has taken place; there are no prevention capabilities. False

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

alarms are common and this technology cannot eradicate malware by itself.

- Trusted content – A technology not depicted on the chart is a prevention technique that uses the philosophy “deny all except that which is explicitly allowed”. PCs can be locked down tightly to only allow trusted software to be executed. This requires an advanced operating system, requires that users do not have administrative privileges, and places a significant administrative burden on the IT organization. A similar method is code signing, which requires all executables to be digitally signed by a trusted authority. This places a similar burden on the IT organization, as all executables will have to be centrally tested and signed before allowing it to be run. If code from a particular company is trusted across the board, this technique will not prevent hostile code from that organization (whether intentional or not).
- Behavior blocking – A prevention technique which attempts to distinguish between malicious and normal activity by utilizing common characteristics of malware code (trying to attach their code to program files or boot sectors, hooking certain interrupts, accessing the registry, volume lock tampering, etc.). Usually accompanied by a memory-resident program, behavior blocking can stop both known and unknown malware, though it is incapable of identification. As a further enhancement, suspicious code can be set aside in a "sandbox", keeping it from causing harm. The concept of a sandbox is similar to the Java programming language's use of a virtual machine environment. The code's actions are monitored and compared to actions allowed by a predefined access control list. Any unauthorized action is blocked. The products offer either application-level or system-level monitoring. Application-level monitoring terminates all of the programs interacting with suspect code. System-level monitoring will block suspect actions without stopping running applications. For example, a browser session may be allowed to continue, while a suspect ActiveX control is blocked. Behavior blockers will, however, create alarms that will require attention by either a user or a system administrator.
- Policy enforcement middleware – Though also not depicted on the graphic, this prevention technique uses software that is instructed through policies that network administrators set to let benign actions take place but to intercede when unauthorized actions occur. These policies can include such rules as not allowing any application to delete the contents of the hard drive, or to replace another executable. Another rule can prevent an application from automatically using the email address book to email multiple recipients. Rules can be set that allow only certain types of signed active content from certain vendors to be allowed to run on certain machines. Communication filters can be included to create desktop-level personal firewalls, controlling which ports can be accessed in which

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

direction, IP addresses that are filtered, which URLs or newsgroups are blocked, etc.

Current technologies focus mostly on the lower-left grid quadrant. What is needed to successfully defend against the latest malware threats are products which effectively cover the entire grid. The following is a list of available products which offer capabilities in the behavior blocking and policy-enforcement middleware categories. The careful selection of one of these products could “fill in the gaps” in your corporate malware strategy. Most of the products should currently be considered to augment an existing signature-based scanner strategy, rather than as a comprehensive fully-functioned solution.

Available Products

SurfinShield Corporate 5.7 from Finjan Software
Until recently, Finjan has offered only an Internet Gateway product and a desktop version designed for home use. The Corporate Edition (which is new) is designed for large business environments, and includes a central database control unit, and client modules. The central server stores corporate, group-level, and local security policies, and incorporates extensive logging and centralized alerting capabilities. The software can accommodate different profiles, so administrators can allow various types of known non-malicious ActiveX content to flow to the end user. This is called "white listing". A sandbox approach is used by Finjan to control access to the file system and registry. Signature scanning is provided through an agreement with F-Secure. Malicious macros are not addressed.

eSafe Enterprise by Aladdin Knowledge Systems, Inc.
This product incorporates its own signature-based antivirus scanner as well as application-specific and general purpose sandboxing. It also offers a personal firewall and built-in file integrity checker. Heuristic scanning identifies new malicious macros as they are encountered. When installed on a server, console-based deployment is supported, and security configurations can be customized by individual users and groups. Centralized reporting and alerting is included as well. This is a very comprehensive product with a wide variety of features.

Pelican SafeTNet 2.0 from Pelican Security, Inc.
Like other products, this one detects and isolates downloaded malicious active content. But unlike Finjan, the product lets users secure applications and systems by determining who has access to make changes. It blocks content by determining what can be changed, as opposed to what can be let through. Like other behavior-blocking tools, the SafeTnet software builds a sandbox around any applets or other code that is downloaded. Unlike Aladdin's sandbox

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

technology, the company claims that its software uses a dynamic approach in that the sandbox is only run when active content is downloaded, thus saving CPU cycles. The product uses SNMP traps to allow integration with enterprise management frameworks such as Tivoli and OpenView.

Secure4U by Sandbox Security
This is another product incorporating sandboxing. Its policy-based restrictions are similar to those of Windows NT security access control lists, allowing system administrators to enforce a consistent network-wide access policy. An interface is provided to allow conventional signature type scanning with a third-party product. A personal firewall is included. Malicious macros are not addressed.

Achilles' Shield by InDefense, Inc.
This product is similar to SafeTnet, although it incorporates DOS-level protection for system sectors, a module for scanning known viruses, and a function for detecting missing conventional memory. The product includes a built-in file integrity checker which can detect unapproved file modifications. Any macros present are checked against the policy database and are locked out until they are certified.

Stormwatch by Okena
Stormwatch doesn't look at specific threats, or specific code, but at overall system performance. It checks every command, network, or system registry operation for any deviance from normal system behavior. Stormwatch combines behavior analysis with static and dynamic heuristics.

Other Vendors
Symantec plans to eventually add behavior blocking to its Norton AntiVirus line. Trend Micro (as previously mentioned) offers a product called AppletTrap, which monitors malicious code at the gateway, and then sandboxes it at the desktop. However, most vendors have stated that their tools will remain signature-based for the near future. This includes Computer Associates, Network Associates, Sophos, and Symantec.

Predictions and Recommendations

- Malware protection needs to be built into a corporate infrastructure.

- Detection methodologies should be used primarily at the corporate gateways and network server level. Here there is a high level of traffic and little execution or activation of applications, documents, or attachments. Scanning of email is still one of the most critical components of a corporate malware strategy since most malicious code is received in this manner.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- Blocking methodologies should continue to be utilized where appropriate. Access to .exe and VBScript files should be restricted to all but the few employees who really need to be able to download them.

- Prevention technologies should be used primarily at the edge of the network (desktop). Products at the desktop that incorporate real-time monitoring of inbound active content and policy-based behavior-analysis middleware should be implemented.

- Consolidation will continue in the security industry to create comprehensive and encompassing "security suites".

- Symantec is working on building a digital immune system for the Internet that can develop new virus signatures within two hours. The company is also working with IBM on an even more automated strategy that has a 30-minute turnaround time. This strategy intends to propagate the cure faster than the virus or worm can spread. These technologies will put the pressure on all malware vendors to speed up their release of new signatures. This will not, however, negate the need for the implementation of other technologies.

- Major ISPs will adopt "clean pipe" solutions, which will greatly assist in the blocking and even eradication of known malware. "A clean pipe is a communications pipeline that has been sanitized of both malicious code and undesirable content. With clean pipe solutions, the Internet company (such as an ISP), rather than the customer, deals with all the issues of signature updates, scanning, and cleaning, resulting in a steady flow of clean information to the user. By the time content reaches its destination (e.g. an end-user's computer or an entire corporate network) it has been cleansed." (Trilling, Stephen).

- At the current time, products that incorporate both behavior-based policy enforcement middleware and signature-based scanning are rare. A final desktop configuration may require the inclusion of software from more than one vendor. This is expected to change in the near future.

Conclusion

For now, the traditional signature-scanning technologies hold prominence in the anti-malware marketplace. Market demand for behavior-based policy enforcement middleware software products will probably not become a reality until the next major malware incident occurs which bypasses the traditional signature-scanning technologies. Your company can stay ahead of the game by

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

alerting your management and users of the risks associated with active content, by planning on alternate malware strategies, and by actively investigating this new breed of products.

References

Armstrong, Illena. "Mobile Code Stakes its Claim." SC Magazine November 2000.
URL: http://www.scmagazine.com/scmagazine/2000_11/cover/cover.html (23 Feb 2002).

Browde, Ian and Smith, Camille. "Virus Protection: All Roads Lead to a Multi-Modal, Modular Approach." May 1999.
URL: http://www.indefense.com/downloads/Security.pdf (23 Feb 2002).

Bussa, Toby. "The Future of Fighting Viruses: A History and Analysis of the Digital Immune System." 8 May 2001.
URL: http://rr.sans.org/malicious/immune_system.php (23 Feb 2002).

Chen, Anne. "Putting up Virus Fences." eWeek June 18, 2000. URL: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2587075-4,00.html (23 Feb 2002).

Dembart, Lee. "Makers of Protective Software Try to Get Ahead of Scofflaws." International Herald Tribune April 16, 2001.

Galarneau, Lisa. "Anti-virus Software: The Challenge of Being Prepared for Tomorrow's MalWare Today." 17 October 2001.
URL: http://rr.sans.org/software/antivirus_software.php (23 Feb 2002).

Hallawell, A. and Pescatore, J. "Signature-Based Virus Detection at the Desktop is Dying." Gartner Research Note August 31, 2001.

Harrison, Ann. "MiniZip Worm Highlights Weak Antivirus Defenses." Computerworld December 02, 1999.
URL:
http://www.computerworld.com/cwi/story/0,1199,NAV47_STO43251,00.html (23 Feb 2002).

Higgins, Kelly Jackson. "Sandbox the Hackers." InternetWeek April 17, 2001.
URL: http://www.internetweek.com/indepth01/indepth041701.htm (23 Feb 2002).

Jansen, Wayne and Karygiannis, Tom. "Security Implications of Active Content." March 2000. URL: http://www.itl.nist.gov/lab/bulletns/mar00.htm (23 Feb 2002).

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Julian, Ted. The Forrester Report Network Strategies Volume 12, Number 7 (1998).

Lemos, Robert. “Lessons of “Love” virus still sinking in.” 4 May 2001. URL: http://news.com.com/2100-1001-257095.html?legacy=cnet (23 Feb 2002).

Messmer, Ellen. "Behavior Blocking Repels New Viruses." NetworkWorldFusion News January 28, 2002. URL: http://www.nwfusion.com/news/2002/0128antivirus.html (23 Feb 2002).

Phillips, Ken. “Pre-Emptive Security Strike.” eWeek June 14, 1999. URL: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,399715,00.html (23 Feb 2002).

Sanders, Russel. "Active Content - Administrators Beware." 26 May 2001. URL: http://rr.sans.org/malicious/beware.php (23 Feb 2002).

Szerszen, Dennis. "What Will We Learn from the Love Letter?" 19 May 2000. URL: http://www.finjan.com/hurwitz.cfm (23 Feb 2002).

Trilling, Stephen. “Understanding Clean Pipe Solutions." 8 August 2000. URL: http://enterprisesecurity.symantec.com/article.cfm?articleid=192&PID=na&EID=0 (23 Feb 2002).

Vamosi, Robert. "Alternative Protection against Malicious Code." 22 May 2001. URL: http://www.zdnet.com/products/stories/reviews/0,4161,2702096,00.html (23 Feb 2002).

Vibert, Robert. "AV Alternatives: Extending Scanner Range." Information Security Magazine February 2001. URL: http://www.infosecuritymag.com/articles/february01/features_av_alternatives.shtml (23 Feb 2002).

Vijayan, Jaikumar. "Web Services, Internet Collaboration Pose Security Challenges for 2002." Computerworld January 3, 2002. URL: http://www.computerworld.com/storyba/0,4125,NAV47_STO67064,00.html (23 Feb 2002).

© SANS Institute 2002, As part of the Information Security Reading Room. 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**