# Global Information Assurance Certification Paper

# Indelicate Balance

The Challenge of Content Filtering Systems in a Litigious Society

By

Grant Streeter

Government Communications Security Bureau (GCSB)

**Summary**

The Internet is often viewed as a place where there are no boundaries to the flow of information, and where there are no rules as to the type, amount and nature of information that can be found there. While this may be true in many ways, it is also true that much of the information is placed there by people with a specific agenda for doing so, and that most of us remain completely unaware of that fact until something unexpected happens when we have acquired some of that information. It is only when a file that contains a virus wreaks havoc on our machine, or we find that someone has loaded a key-logging Trojan on our computer to steal our ISP username and password, do we actually consider where that information came from, who gave it to us and for what purpose.

It is very easy to look at what can be accessed and downloaded from the Internet, it is much harder to take the time to think whether accessing or downloading that information is actually the best thing to do.
One way of both assisting people in making better choices and preventing unwanted, un-useful or potentially damaging information from entering or leaving our computer systems, is to implement a content filtering system that blocks unwanted content and also restricts access either away from potentially harmful sites, or allows access to only those sites deemed to be safe by the organisation.

The use of content filtering systems for restricting access in this away has sparked a long-running debate over censorship and who, if anyone, has the right to determine what consenting adults may choose to view or not view. In particular, where governments and government agencies have presumed to speak on behalf of all their citizens by introducing blanket bans on certain types of sites and categories of information, there has been a growing amount of concern from those who regard it as their right to be able to have access to all the information, good, bad, legal and illegal, that exists on the world-wide web.

There is also been an increasing amount of discontent within the IT community relating to the nature and perceived quality of the content filtering systems available. It seems there is a new ‘arms race’, where just as a supplier brings a new product to market, someone else quickly develops a way to exploit and ultimately defeat it. Many are now questioning if there is not a simpler and better way of safeguarding our information and protecting ourselves from those seeking to cause us damage, without impinging unnecessarily on the rights of our users and denying them access to information that may be potentially useful.

Protecting what and for whom?

With the growing number of viruses, Trojans and an every increasing amount of spam to deal with, it is easy to start having a siege mentality and begin to view everyone, including our internal users as threats to the security of our systems and our information.
Indeed there are examples of organizations that view internal users as the prime enemy. Statistics New Zealand state quite clearly in a presentation they have posted on this website, http://www.govis.org.nz/forums-pres/govis-mume.ppt that they subscribe completely to this view. When you look at the information presented, with respect to the amount and nature of unwanted information being brought into not only their agency, but other agencies as well, their fears seem well justified. Is it any wonder that corporations, government agencies and other organisations want to stop this torrent of illegal, questionable and often objectionable material from entering their premises, possibly exposing them to the risk of legal action by the parties who are injured by this material?

My question is how exactly did things get to this point? Are all those people employed by government departments and agencies intentionally seeking to bring themselves and their employer into disrepute? Are they all lazy and don't want to work at their 'real' jobs, but instead surf the Internet and be paid for it? Or is there something else going on?

If we were to look closely at Statistics New Zealand, with respect to their hiring policy, their training policies and their acceptable usage policies, I wonder what we what might find? It is my view that rather than blame our users, we should ask ourselves if we have the right people using the right tools in the right way for the right reasons. If our users do not really understand what they are responsible for, and what the possible consequence to them and our organisation can be if they go outside the rules and bring unwanted material through our email and Internet gateways, then maybe we have only ourselves to blame.

So then, what, and or whom, are we protecting and why? Depending on the organisation, looking at it's aims and goals, the nature of the work it performs and for whom this work is performed, will go a long way to answering this basic question.

In terms of the tools to be used, it can be useful to understand the difference between URL blocking and other forms of content filtering.
URL blocking is where all information from an entire domain is blocked from entering the organisation's gateway. This is a simple way of ensuring that any and all unwanted information that a particular site may contain, cannot be accessed, viewed or downloaded. The downside is that this is an inexact tool and will often block potentially useful information along with the not-so-useful. It also does not check information leaving the organisation as to the nature of it's content and whether it is suitable or appropriate for the intended destination.

Other forms of content filtering rely on more refined ways of sorting the information, both coming into and leaving the organisation, usually based on a set of rules that have been either imported or developed by the organisation.

Understanding the different requirements, not only for different organizations, but also different divisions and departments within an organization, will point towards the different kinds of protection that must be afforded to them. We must be able to clearly define exactly what is important to us as an organisation, before we can begin to take steps to make all our people understand that everything we do is targeted towards those goals, and then we can start to put meaningful policies, backed by appropriate technology in place to support those policies. Too often, a technological measure is put in place to overcome what is essentially a Human Resources issue.

The potential for the over-reliance on technology

Your CEO is breathing fire because Internet costs are ballooning and 'everyone knows' that employees are surfing for personal reasons. You need to do something, and fast.
The solution? Put in another appliance, or install some software to start getting rid of that unwanted content, and at the same time start apportioning Internet traffic costs to those areas and specific staff members who are actually using it.

But hold on. There are an astounding array of products available, from a huge number of different companies, all promising a safer online experience, and an easier life. So how do we know what to look for a content filtering solution? What if the glib marketing speak is being frugal with the truth?
At an even more fundamental level, do we have the willpower, the know-how and the money, to implement and manage a content filtering solution on a proactive, ongoing basis? For there is one thing all the companies hawking their products agree on. This is a new Cold War, an arms race, with those of us protecting our networks wearing the white hats, and those bent on defeating our security measures, including our own internal users (we are told), wearing the black hats.

The only way to stay ahead, the vendors tell us, is to purchase more complex and increasingly more expensive devices and software, spend more money on training your IT security staff to manage those devices and software, to keep making things more complex and difficult. Technology can be used to overcome human issues, you just need to continually change it, as those pesky users learn ways around what you have just implemented.

There are many occasions in human history where a complete reliance on technology has led to catastrophic results. The Titanic was deemed to be "unsinkable" and yet sank on its maiden voyage. There have been two tragedies

involving the Space Shuttle, that at their root were a breakdown in technology that was caused by a failing in human control systems.

As the race to bring better, more comprehensive products to market, the cost and complexity involved with implementing and managing these systems also increases dramatically. The best device or piece of software will offer no protection at all if it is not installed, configured and maintained correctly.
Even the installation and management manuals of many of these products are now so complex, that they require IT staff to go on training courses before they are competent to be able to begin to get the best from these products.
An example of a complex manual can be seen at:
http://docs.sun.com/source/817-0534-10/contents.html.

While Sun have done an excellent job at including all the required information with respect to configuring and installing their product, and made it readily accessible, it does not alter the fact that implementing, configuring and managing, what is essentially a straightforward proxy server, has now become a task that only a highly trained professional would want to attempt, in order to have a high level of assurance that the device and the software are actually going to provide an appropriate level of protection.

The value of effective policies

So do we have to continue to develop and implement increasingly sophisticated systems? The broad answer to this question is no. However, in order to stop going down this path, you first need to ask some fundamental questions about how your organisation works, what it is that you truly value and stand for. From this point you can start to map what it is your users actually need to see and do when they are online, and from there start to build policies and processes to communicate this to everyone in your organisation. It is only at this point that you can make a rational, informed decision with respect to the infrastructure, resources and technologies that are going to support your policies and processes.

How do you develop, implement and get 'buy in' to your Internet usage policies? Do you regulate and promise harsh punishments for transgressions, do you go through a consensus gathering exercise and produce policies that has input from all areas of your organisation, or do you just say "It's all too hard" and hope for the best?
This is one case where doing nothing is not a good option. If you are aware that there may be a problem, then you can be assured that it is much more significant than you think. For example, 70% of traffic to porn sites occurs during the period of 9.00am to 5.0pm each day. Add this to the fact than an estimated 30-40% of worker's online activities have nothing to do with their job, and an unpleasant

picture begins to emerge – from pages three and seven of “The hidden legal dangers of email” http://www.nabarro.com/uploads/files/113.pdf.
.
The design of any Internet usage policy should begin with the statement that the purpose of the policy is for the protection of the user and the protection of the organisation. Most usage policies seem to go out of their way to be harsh, restrictive and to leave the user with the feeling that the organisation does not trust them at all, and would much rather they did not use either email or the Internet in general.

Rather than your policies sounding as though you regard your workforce like children, by making them read a simple list of do’s and don’ts, try this radical idea; describe in detail what the user will see on their screen and what they will not. Define the Internet experience the user will have while operating their terminal at work. Be specific, say things like “You will have access to the business tools and information you need” and “You will not see pornography, you will not be pestered by instant messaging”. Make sure that if the user feels they require access to a specific site, on either a temporary or permanent basis, that there are simple and quick mechanisms for making this happen.
Say, in clear and simple terms, what your organisation stands for and why. For example you may say something along the lines of “This Company protects its intellectual property and respects the intellectual property of others”, or “We do not allow others to make illegal copies of software we use, and do not make illegal copies of software used by others”. Just spell it out in a straightforward way.
The definition of the user experience should probably include descriptions of the systems in place to protect their experience, the filters, the ‘real-time’ monitors, the audit trails, and the reports. Big brother is watching, not you, but everyone else, in order to keep you safe.
Of course if the user then chooses to attempt to create their own online experience, this will look to Big brother like an attack from outside, and will be treated as such. This will cause the user to have a new online experience – disconnection.
That is the other part of a good usage policy, simple and clear consequences for those who choose, as many do, to not play by the rules. For example, the system will automatically disconnect a suspected rogue connection and will suspend the email and Internet access of the affected user, until such time as the anomaly can be explained. If a user is unable to explain the anomaly, they may have their access disconnected until they have successfully completed an Internet safe usage course. Continued or repeated breeches of security will be treated the same way as the misuse of any company assets and will be subject to standard disciplinary procedures.

A good example of a simple and understandable policy can be viewed at the Cascade College site, http://www.cascade.edu/index.asp?id=32, and while I may

not necessarily agree with the philosophies of this organisation, their policy on Internet use and just what is acceptable, is loud and clear:

Content filtering and censorship

One growing area of concern for many people is that content filtering systems are being used to restrict access to information and ideas. The reasoning is that the Internet represents complete freedom, all the good along with all the bad, and that it is up to the individual to be responsible for what they choose to look at and not look at, it should not be up to the state to pre-determine what we can or cannot see.
A group dedicated to this idea is the Centre for Democracy and Technology (CDT). A visit to their site located at: http://www.cdt.org/speech/ will yield and enormous amount of information as to why blocking content on the Internet is a violation of free speech.

Nice idea in theory, but what would happen if we applied this thinking to other areas. For example, if there were no more road rules and you can now drive on whatever side of the road you want at whatever speed you see fit. Of course it is up to the individual to drive responsibly and probably most of us would. But there are more than enough people who would choose to do otherwise and endanger both themselves and us. The result of this would be a level of death, injury and damage that would be completely unacceptable. So, is this not also true of the Internet? There are far too many people who use the freedom it offers to exploit and injure many other people, so many that it requires action to be taken to protect us from them. Remember there are two types of freedom: the freedom to perform a particular act, and the freedom from having a particular act performed upon you. When damage likely to be inflicted from the latter outweighs the benefit likely to be accrued from the former, it is time to act.

There are a number of self-appointed watchdogs and neigh-sayers that in some cases merely present their views on the matter of the use of content filtering, and in other cases, go to the lengths of publishing weaknesses and exploits within content filtering software and systems. These range from those with only a small amount of specific information available, such as The Censorware Project, http://censorware.net/ and The Free Expression Policy Project, http://www.fepproject.org/factsheets/filtering.html.

In addition to the restriction to specific sites by individual organizations, there is a far more insidious from of censorship on the Internet. That is the deliberate and sustained attempts by Governments to prevent their citizens having access to information that the Government deems to be contrary to their political views. The Electronic Privacy Information Centre (EPIC), located at http://www.epic.org not only backgrounds the rise of state censorship, but has specific instances of it that have been implemented by governments worldwide.

The most noticeable of these is the Chinese government. Even in this case, they are subject to scrutiny by outside parties. In the project C report which is available at http://www.chass.utoronto.ca/~citizenl/assets/articles/ProjectC-r1.pdf the Chinese Governments' various attempts to completely block access from within China to websites containing information about such things as democracy, Tiannamen Square and Falun Gong, are documented along with the results. Although last updated in 2002, it shows clearly that despite having complete access and absolute control of all communications channels, they have not been successful in blocking access to most of these sites.

How successful can content filtering be?

If a highly motivated, very well funded and resourced enterprise like the Chinese Government, fails to block the majority of specific content, then what chance is there for the rest of us?
There are a number of documented cases where supposedly highly protected computer systems have been compromised. Examples of some of these, from the BBC website are:

- May 1999 - U.S.. Senate and FBI websites are hacked and defaced.
- February 2000 - Yahoo, Amazon.com, E-Bay, CNN.com, ZDNet and many others, are hacked via "denial of service" attacks.
- May 2001 – CIA website is defaced by Chinese hackers

There are many people and organisations dedicated, for differing reasons, to the removal or circumvention of content filtering systems and software. One of the most well known is peacefire (www.peacefire.org). This site includes detailed instructions on loading and configuring software that "Defeats all Internet censorship programs". So why do they do this? On their site the following page, http://www.peacefire.org/info/why.shtml, states the prime reason as being "to advocate for First Amendment rights of people under 18 on the Internet. Courts and politicians are generally hostile towards rights of minors (the U.S. is one of only five countries in the world that has the death penalty for people under 18), but courts have said that people under 18 do have First Amendment rights, though most judges believe that minors' rights are not as broad as those of adults."
Not all the sites are operated by self-appointed protectors of the public good, others, such as Seth Finkelsteins site, http://sethf.com/anticensorware/ are aimed more at exposing the holes and failings of the software and systems that are commercially available. While Seth describes himself as "an honoured member of Peacefire", most of the material available on his website is not directly aimed at defeating content filtering systems, rather it is more informative as to how the products work, and how they fail, in many cases to actually perform the function for which they were intended.

There are still other sites are fully directed towards documenting the flaws and issues related to systems and software solutions, such as the Builder.com site, http://builder.itpapers.com/abstract.aspx?&scid=904&docid=88937 .

So, with such a large number of sites exposing weaknesses and many others actively seeking to circumvent the controls you want to put in place, how do we go about deciding which, if any, content filtering solutions will provide the assurance we are after?
When you want to purchase a used car, getting someone who knows what they are doing to check under the hood before you buy the car, can save you from a very costly mistake. So how can we 'check under the hood' of content filtering software and systems?
Fortunately the Internet provides many sites that have already done the work. Or have they? When assessing the performance of a piece of software or hardware, a number of sites have strikingly similar reports. It begs the question of who did the original research and were they completely independent of any specific producer? If the site has either paid for a report that was developed by someone else, or one or more of the producers that have products under scrutiny funded the research, then the impartiality of the information must be questioned. Establishing both the impartiality and the credentials of the original producer of product reports can be difficult, so checking for sites that do their own research, and do not have links to any of the product suppliers, is more likely to yield a fair and accurate assessment of a particular product. Provided, of course, that the person doing the actual work has the credentials necessary to conduct a meaningful investigation. Even using some of the sites mentioned earlier that will describe weaknesses in particular products can be useful for assessing what is likely to work and what is likely to not work.

For the sake of comparison, I researched the following four review sites, to see what they recommended, and why.
The first site is the Top 10 Reviews site, for full details go to - http://internet-filter-review.toptenreviews.com/?ttreng=1&ttrkey=Internet+filters . The first five features they say makes a good content filtering solution are:

1. Ease of use
2. Effective at filtering
3. Filtering algorithm
4. Activity reporting
5. Client-server based

The top five solutions they recommend, in order are:

1. ContentProtect, from ContentWatch
2. CYBERSitter, from Solid Oak
3. Net Nanny, from BioNet
4. CyberPatrol, from Vantage Software
5. FilterPak, from SF4

The second site on my list is the library filters site, see - http://libraryfiltering.org/ . The first five features they highlight are:

1. Categories vendor recommends for CIPA compliance
2. Block page displayed or blocking transparent to user
3. Items that can be included on the block page
4. Can filter by file type
5. Can have multiple user/filter profiles

Their top five recommendations are:

1. i:filter, from DynaComm
2. Netpure, from Allot Communications
3. iPrism, from St. Bernard Software
4. Engage IP Content Filter, from LogiSense Corporation
5. The Internet Filter IF-2K, from Turner & Sons Production

The third site I checked was the PC Magazine site, for full details go to - http://www.pcmag.com/article2/0%2C1759%2C1538518%2C00.asp. They only had four rating criteria:

1. Configuration and deployment
2. Administration
3. Blocking
4. Monitoring and reporting

Their top five products:

1. Sentian, from Secure Computing
2. SurfControl Web Filter 4.5, from Vantage Software
3. Web Inspector 7.0, from Zix Corporation
4. 8e6 R3000 Enterprise Filter, from 8e6 Technologies
5. iPrism 3.5, from St. Bernard Software

The fourth site was the oldest, the Infopeople.org site, full details are at - http://www.infopeople.org/howto/filtering/filtering_chart_updates.html . Their first 5 rating criteria were:

1. Purchase Price
2. Subscription rate for 50 users
3. Smallest group license price
4. Requires configuring each client?
5. In use by a library somewhere?

Their top 5 products, from 2002:

1. CyberPatrol 5.0 for Microsoft Proxy Server, from Vantage Software
2. i-gear 3.5 for Microsoft proxy Server, from Symantec Corporation
3. i-Prism Internet appliance, from St. Bernard Software
4. N2H2 for Microsoft Proxy Server 2.0, from N2H2 Incorporated
5. S4F v.6.02 for remote proxy server, from Family Connect Incorporated

As we can see, each site had very different criteria for rating the various products, and came up with differing top 5 products, although if we check the sites for a top 10 or even more, then a number of specific products are

mentioned repeatedly. If the picture weren't confusing enough, I decided to also look at five of the larger producers, and check their reviews of their own products.

The first of the five I chose was Symantec Corporation, at the following address http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=60. Their core product is Symantec Web Security and they describe the key features as being:

- Ensures maximum protection by combining list-based techniques with heuristic, context-sensitive analysis for both virus protection and web content filtering
- Secures web traffic with high-performance, integrated virus scanning and content filtering of HTTP and FTP traffic at the gateway
- Simplifies administration and enhances management flexibility with new centralized multi-server policy management capabilities
- Provides highly manageable and scalable protection for individual users and groups via secure support for external directory services
- Improves network performance and user productivity while eliminating unwanted content and malicious code
- Backed by Symantec Security Response - the world's leading antivirus and Internet security research and response organization

The second site I went to was Vantage Software at this address: http://www.vantagesoftware.com/products/content_patrol/index.html . Their core product is ContentPatrol, which appeared in three different top five lists in the previous part of this section. This is how they describe their product:

- Content Patrol is a software utility that will allow you to easily scan and clean objectionable content on your PC.
- In general, most objectionable files are difficult to find and therefore almost impossible to delete.
- In addition, Content Patrol helps you free up valuable disk space on your hard drive thus improving the performance of your PC.

The third manufacturer was netIQ, whose core product is WebMarshal. Details are available at http://www.netiq.com/products/wma/default.asp. Their main points are:

- Improves productivity by preventing employees from wasting time and computing resources.
- Reduces legal and security risk by controlling web access.
- Delivers rapid return on investment (ROI).
- Integrates with NetIQ's security products.

The fourth on my list was F-Secure, at http://www.f-secure.com/products/anti-virus/fsigk/. Their product is F-Secure Internet gatekeeper. Here's what they say are it's main features:

- Virus protection for e-mail (SMTP) and web traffic (HTTP, FTP over HTTP)
- Content filtering
- Spam filtering
- Access control
- Interoperable with any firewall and e-mail system
- Local or remote user interface
- High performance and reliability
- Automatic virus definition updates

My fifth and final manufacturer was Secure Computing. Their site revealed three different products, the most notable being Bess. Details of their products can be found at http://www.securecomputing.com/index.cfm?skey=22.
Bess's highlights are:

- Easy-to-use software – powerful enough for the largest networks
- De-centralize filtering with exclusive Bess features!
- Tightly integrated filtering solutions
- The features and functionality you need
- Additional features that don't cost extra

To conclude, my investigation, as limited as it was, shows that not only are there a wide range of products, there are also a wide range of views on how effective those products are.
In selecting a product that will support the policies and systems that have been place, a significant effort is required to investigate not only the products, but also the claims and the reviews of those products. For example, one product that showed up on many of the reviews sites, but not in the top five was Bess. Reading the reviews and the information provided by the manufacturer shows the product to be useable and effective. However, reading the anti-content filtering websites describes the product as flawed and difficult to manage see http://censorware.net/reports/bess/.
In providing the technical infrastructure that supports the organizations stated objectives and goals, careful and deliberate selection of a vendor and a product is a key element.

## Conclusions

Content filtering systems and software seem like an excellent technological solution to the issue of how to maintain the integrity of our networks and information, and a good way of keeping our users safe from unwanted and potentially damaging material. While it is tempting to rely solely on such a sophisticated technological solution, it pays to be aware of past instances where these have failed catastrophically. It also pays to be aware that there are individuals and organisations that have dedicated themselves, for various reasons, to finding ways of circumventing and depleting the effectiveness of content filtering solutions.

The prime issues that need to be addressed when considering the need for a content filtering solution, relate to what the organisation does, what is has to protect, and how users are expected to operate their email and Internet sessions. With good training and well thought-out policies, there is a framework in place to then develop the infrastructure that will support and maintain the integrity of those policies.

There is most certainly an issue with respect to restricting access to unwanted material, and at the same time inadvertently censoring an amount of potentially useful information and thus creating a user-unfriendly environment.
With a vast array of software and hardware producers all claiming to have the best solution, it is difficult to obtain truly objective information as to just how effective many of these products are. Some of the most useful information in this area actually appears on the websites of those who seek to circumvent these systems.

When planning a content filtering implementation, these factors, along with the costs associated with managing a complex solution on an ongoing basis, create a difficult and indelicate balancing act.

**References**

Fitzgerald-Irons, David. “My user, my enemy” 17 March 2003. URL: http://www.govis.org.nz/forums-pres/govis-mume.ppt

Unknown Author. “Sun One: Open net environment” 2002. URL: http://docs.sun.com/source/817-0534-10/contents.html

Ellacott, Sara. “The hidden legal dangers of email” August 2001. URL: http://www.nabarro.com/uploads/files/113.pdf

Unknown Author. “Web Content Filtering Policy” 2003. URL: http://www.cascade.edu/index.asp?id=32

Multiple Authors. “Free Speech Online” October 2004. URL: http://www.cdt.org/speech/

McCarthy, Jamie. “The Censorware Project” 2 November 2004. URL: http://censorware.net/

Unknown Author. “The Free Expression project” 1 November 2004. URL: http://www.fepproject.org/factsheets/filtering.html

Unknown Author. “PEACEFIRE” 24 October 2004. URL: Http://www.peacefire.org

Unknown Author. “Electronic Privacy Information Centre” 6 November 2004. URL: http://www.epic.org

Villeneuve, Nart. “Advanced Research – Project C” September 2002. URL: http://www.chass.utoronto.ca/~citizenl/ar/projectc.htm

Finklestein, Seth. “Seth Finklestein’s Anticensorware Investigations” October 2003. URL: http://sethf.com/anticensorware/

Unknown Author. “Why Spammers Outwit Content-Filtering Programs” December 2003 2002. URL: http://builder.itpapers.com/abstract.aspx?&scid=904&docid=88937

Unknown Author. “Internet Filter Review” October 2004. URL: http://internet-filter-review.toptenreviews.com/?ttreng=1&ttrkey=Internet+filters

Ayre, Lori Bowen. “Library Software Filters” October 2004. URL: http://libraryfiltering.org/

Lipschutz, Robert P. “Web Content Filtering: Don’t Go There” 16 March 2004. URL: http://www.pcmag.com/article2/0%2C1759%2C1538518%2C00.asp

Ayre, Lori Bowen. “Filtering the Internet: Product Comparison Chart with Updates” 18 October 2002. URL:: http://www.infopeople.org/howto/filtering/filtering_chart_updates.html

Unknown Author. “Symantec Web Security” June 2004. URL: http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=60

Unknown Author. “NetIQ WebMarshal” November 2003. URL: http://www.netiq.com/products/wma/default.asp

Unknown Author. “Content Patrol 2004” April 2004. URL: http://www.vantagesoftware.com/products/content_patrol/index.html

Unknown Author. “F-Secure Internet Gatekeeper” 14 June 2002. URL: http://www.f-secure.com/products/anti-virus/fsigk/

Unknown Author. “The web you want. The control you need.” July 2004. URL: http://www.securecomputing.com/index.cfm?skey=22

Last Updated: July 21st, 2017

# Upcoming Training


| | | | |
|---|---|---|---|
| SANSFIRE 2017 | Washington, DC | Jul 22, 2017 - Jul 29, 2017 | Live Event |
| SANS Boston 2017 | Boston, MA | Aug 07, 2017 - Aug 12, 2017 | Live Event |
| SANS Prague 2017 | Prague, Czech Republic | Aug 07, 2017 - Aug 12, 2017 | Live Event |
| Community SANS Omaha SEC401* | Omaha, NE | Aug 14, 2017 - Aug 19, 2017 | Community SANS |
| SANS Salt Lake City 2017 | Salt Lake City, UT | Aug 14, 2017 - Aug 19, 2017 | Live Event |
| SANS New York City 2017 | New York City, NY | Aug 14, 2017 - Aug 19, 2017 | Live Event |
| SANS Chicago 2017 | Chicago, IL | Aug 21, 2017 - Aug 26, 2017 | Live Event |
| SANS Adelaide 2017 | Adelaide, Australia | Aug 21, 2017 - Aug 26, 2017 | Live Event |
| Community SANS Trenton SEC401 | Trenton, NJ | Aug 21, 2017 - Aug 26, 2017 | Community SANS |
| Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style | Virginia Beach, VA | Aug 21, 2017 - Aug 26, 2017 | vLive |
| SANS Virginia Beach 2017 | Virginia Beach, VA | Aug 21, 2017 - Sep 01, 2017 | Live Event |
| Community SANS Pasadena SEC401 @ NASA | Pasadena, CA | Aug 23, 2017 - Aug 30, 2017 | Community SANS |
| Mentor Session - SEC401 | Minneapolis, MN | Aug 29, 2017 - Oct 10, 2017 | Mentor |
| SANS San Francisco Fall 2017 | San Francisco, CA | Sep 05, 2017 - Sep 10, 2017 | Live Event |
| SANS Tampa - Clearwater 2017 | Clearwater, FL | Sep 05, 2017 - Sep 10, 2017 | Live Event |
| Mentor Session - SEC401 | Edmonton, AB | Sep 06, 2017 - Oct 18, 2017 | Mentor |
| SANS Network Security 2017 | Las Vegas, NV | Sep 10, 2017 - Sep 17, 2017 | Live Event |
| Community SANS Albany SEC401 | Albany, NY | Sep 11, 2017 - Sep 16, 2017 | Community SANS |
| Mentor Session - SEC401 | Ventura, CA | Sep 11, 2017 - Oct 12, 2017 | Mentor |
| Community SANS Columbia SEC401 | Columbia, MD | Sep 18, 2017 - Sep 23, 2017 | Community SANS |
| Community SANS Dallas SEC401 | Dallas, TX | Sep 18, 2017 - Sep 23, 2017 | Community SANS |
| Community SANS New York SEC401 | New York, NY | Sep 25, 2017 - Sep 30, 2017 | Community SANS |
| Rocky Mountain Fall 2017 | Denver, CO | Sep 25, 2017 - Sep 30, 2017 | Live Event |
| SANS London September 2017 | London, United Kingdom | Sep 25, 2017 - Sep 30, 2017 | Live Event |
| SANS Baltimore Fall 2017 | Baltimore, MD | Sep 25, 2017 - Sep 30, 2017 | Live Event |
| SANS Copenhagen 2017 | Copenhagen, Denmark | Sep 25, 2017 - Sep 30, 2017 | Live Event |
| Community SANS Boise SEC401 | Boise, ID | Sep 25, 2017 - Sep 30, 2017 | Community SANS |
| Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style | Baltimore, MD | Sep 25, 2017 - Sep 30, 2017 | vLive |
| SANS DFIR Prague 2017 | Prague, Czech Republic | Oct 02, 2017 - Oct 08, 2017 | Live Event |
| Community SANS Charleston SEC401 | Charleston, SC | Oct 02, 2017 - Oct 07, 2017 | Community SANS |
| Community SANS Sacramento SEC401 | Sacramento, CA | Oct 02, 2017 - Oct 07, 2017 | Community SANS |