Global Information Assurance Certification Paper

Patrick Foster

Version 1.4b

TITLE:

Multi-level AntiVirus Protection How We Accomplished it.

The purpose of this paper is to show how one organization approached the unprecedented task of protecting itself against virus attacks. It will show how and why we decided to install this multi-level form of protection. The Symantec suite of programs was chosen to be implemented after evaluating in real time other antivirus software. It is not the purpose of this paper to go into depth about what and how viruses work or spread. I hope to show how we can significantly reduce the risk of malicious code/virus's by implementing a multi-level protection that all work together. The three products that we are currently using are Symantec AntiVirus Gateway Solution, Norton Antivirus Corporate Edition (NAVCE) and Norton Antivirus for Microsoft Exchange Servers (NAVMSE). I will go over how we implemented each product to work together to reduce our risk.

THE INFRASTRUCTURE:

The organization is set up with a corporate headquarters (HQ), remote corporate office (CO) and remote satellite offices (RSO). The CO is comprised of approximately 120 employees and 130 computer systems. The 18 RSO's average 80 employees and 90 computer systems. Each site is connected via Wide Area Connections to the CO. Fig. 1

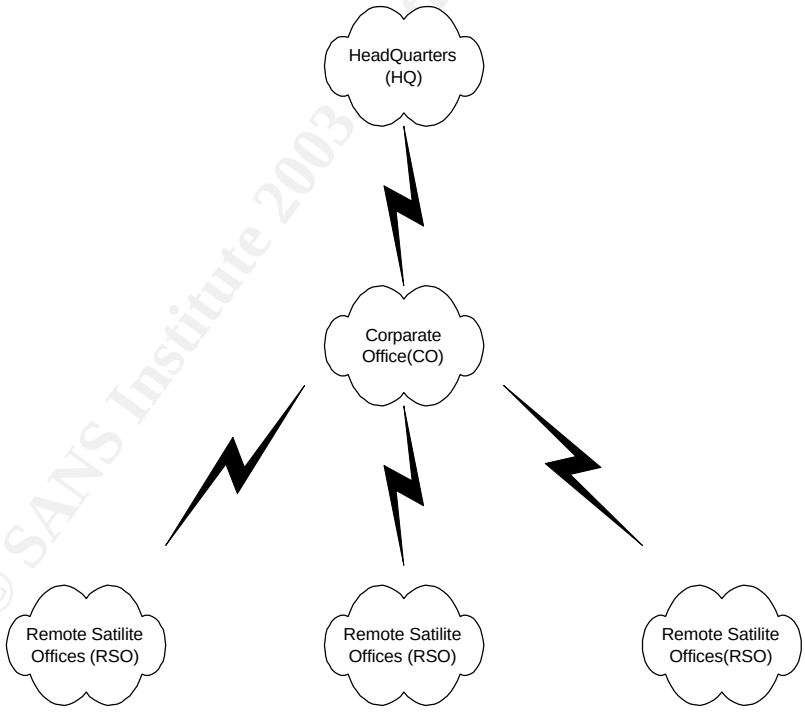

Fig. 1

Prior to the "I LOVE YOU" virus of May 2001 the level of virus protection was very haphazardly organized. We did at the time have approximately 40% level of

desktop coverage and an E-Mail antivirus program installed. HQ was involved with the purchase of software that was to be installed and set policy on what needed to be accomplished but offered no direct support of the project at the CO level. On the other hand the CO was fully responsible for the support and installation at the RSO's level. The main problem was having several sites with many PC's that have to be protected with minimal onsite staff to maintain and install the antivirus program. To complicate and make the situation even harder to maintain is that there was internet access and E-mail being accessed on each PC across the organization. We realized that with Web-based e-mail (yahoo mail, hotmail and E-mail from almost every ISP that exists) and downloaded files off the internet, the risk of infection with viruses was greatly increased for our desktop systems. There was an early attempt to block as many of these e-mail sites as possible in an effort to reduce the risk. We found out very quickly that there were too many legitimate uses for these external e-mail sites within our organization. There was also use of desktop messaging programs such as AOL instant Messenger that was used within the organization to communicate with HQ and the RSO's. Desktop protection always will be the most important line of defense for an effective antivirus strategy. If SMBs (small and medium sized business) have no control over the desktops, they should at least ensure that up-to-date security signatures get to the SMTP gateway.[1] So, at this point we realized we needed at least three levels of protection. One was for the PC's (desktop and servers) themselves, second was to protect against E-Mail borne Viruses and the third was at an organizational level to provide antivirus protection at the gateway level. But, the implementation of this was not quite as easy as knowing what needed to be done.

Prior to the "I LOVE YOU" Virus the organization had bought mass licensing to install McAfee antivirus on all PC's and servers. At that time our only avenue was to manually install the program on each of the PC's across the organization. With over 1,500 desktops this proved to be a major task especially with very minimal IT staff at each site. So, we began to look at products that could help to automate the process. The first product we looked at was from Network Associates – ePolicy Orchestrator. We downloaded a free trial version from them and proceeded to try to install the product on one of our less critical servers. The installation failed. After 8-10 tries on various servers and hours on the phone with technical support we abandoned our efforts. As for scanning E-mail we had also looked at the Network Associates product and were able to successfully install and configure the product. Even though the product functioned very well, HQ had decided to go with the Norton Antivirus for MS Exchange (NAVMSE). This sent us back to square one to install, configure, test and implement an antivirus solution to scan our E-Mail. Shortly thereafter they also changed the desktop protection from McAfee to Norton Antivirus as well. We had just installed NAVMSE with the only change in the configuration being to notify the administrators of found viruses at the time of the dreaded "I LOVE YOU" virus attack in May of 2001. Of course most of the HQ staff as well as myself were on travel back from a conference when this occurred.

The entire CO (along with the RSO's) were brought down and isolated from the rest of the network for approximately two days. Unlike other CO's we had already installed NAVMSE and it was operational at the time. Once the virus definitions were available we were able to download them and start scanning the Mail to eliminate the virus. But, as long as other Mail servers within the organization were infected we still had a flood of infected E-mail. Although we were not getting infected it still took a toll because of the large load of E-mail. It was this event that caused HQ and CO management to enforce a policy that would require that NAVCE be installed on each and every PC in the organization. Each Exchange server would also be required to have NAVMSE installed and operational.

Desktop installations:

The first step to try to automate installation of desktop computers was a way to control them once we had them installed, for this NAVCE came with Symantec System Center (SSC). We were able to successfully install this program with very minimal effort or problems. After testing this tool we were able to move on to issues dealing with the desktop installations.

The first issue that has to be considered is if you want to maintain a managed or unmanaged network of PC's. The short definition of each are :

Managed clients are those that are a part of the network and logon on a regular basis. Managed clients can:

- Communicate with a parent server and download configuration and virus definitions file updates as often as necessary.
- Be seen from Symantec System Center under their parent server.
- Immediately send alerts if Norton AntiVirus Corporate Edition detects a virus. Client log information is also available from Symantec System Center.
- Lock the configuration settings that you set from Symantec System Center so that the user cannot change them.
- Automatically install to a user's hard drive through logon scripts.
- This is useful for new installations and for program updates. [2]

Unmanaged clients are those that are not a part of the network and although they may log into the network occasionally they do not login on a regular basis.

- They will NOT appear in Symantec System Center (unless you change them to being a managed client by updating their GRC.DAT file)
- They do not have a parent server
- They will NOT get their definitions from the Network
- They will need to download their definitions manually via LiveUpdate or Intelligent Updater

For a corporate type install such as ours the only logical choice is to have managed clients.

We began our installation at the CO and worked our way down to the remote PC's. Norton AntiVirus Corporate Edition (NAVCE) version 7.5 and Symantec System Center (SSC) were installed on a CO server as the master parent server of the group. Then using SSC we were able to remotely install NAVCE to one parent server at each RSO. By modifying the sample script included with NAVCE we were able to add this to the startup script used by the CO. The script checks the remote PC to see if NAVCE was installed (if it was installed but a lower version, it would install the newer version). If NAVCE was not found, it would evaluate what the operating system is and then install the appropriate version of NAVCE. We set it to do a silent install on all systems at start up. [Although this was good in that the end-users were not given the opportunity to exit out of the installation, it caused a lot of calls to IT. After the installation completed (which took anywhere from 10-30 minutes) the PC would reboot itself. This created a lot of complaints that users were in the middle of documents that had not been saved.] Figure 2 shows the downward path of the installation.

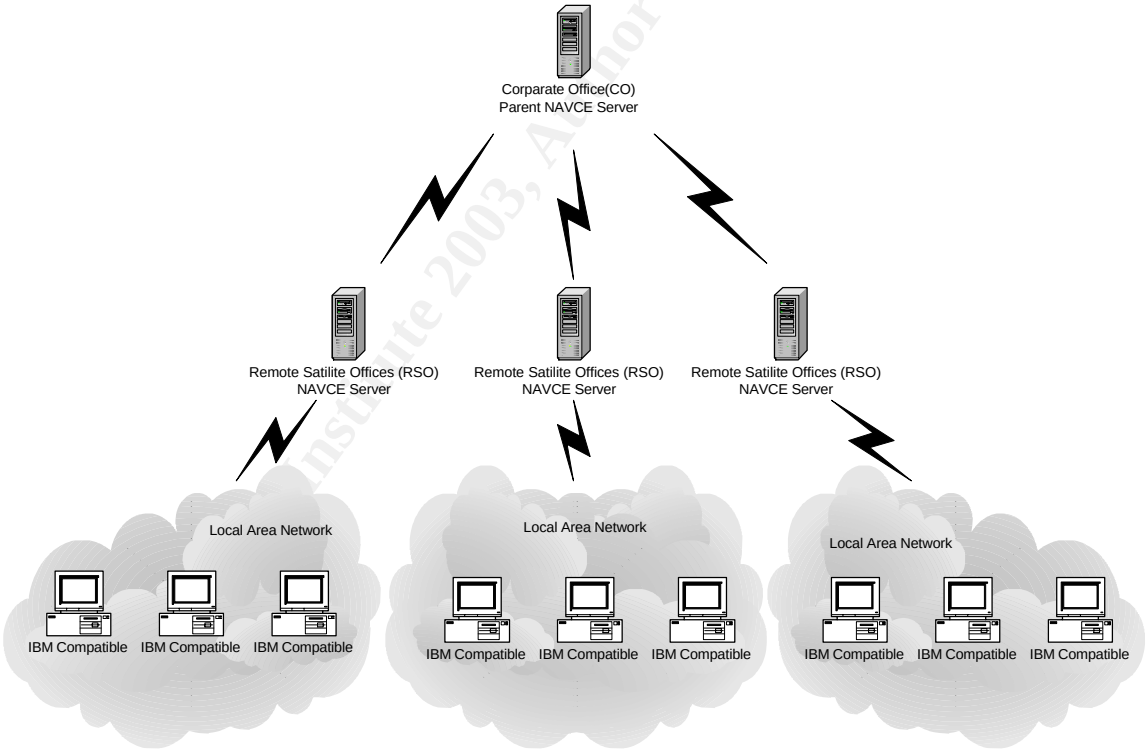

Fig. 2

Keep in mind that if you are using a script to install clients, a different script will need to be made for each RSO parent server. The script identifies who the parent server will be for that PC. This is done via a file called GRC.DAT. So if you need to change a computer from one RSO to another you just have to install

the GRC.DAT for the new parent server. In the NT domain set up, if all computers are a part of the same domain each script must be on each and every Primary Domain Controller and Backup Domain Controller's across the domain.

Once NAVCE was installed on all clients in the group or domain we had to decide how we were going to keep the virus definitions up to date. There are various methods available for downloading virus definitions and setting up servers and clients to retrieve them:

- Virus Definition Transport Method (VDTM)
- LiveUpdate
- Intelligent Updater

Using the VDTM method there is the advantage of only having to update the master primary server. The master primary server then pushes the definitions out to the primary servers which in turn push the definitions to their clients. There are a couple of advantages to this method. The first one is called backdating the virus definitions. On some occasions after virus definitions are installed they will create a large number of false positive notifications. In this situation you can backdate the definitions to the previous known good definitions. Then once Symantec releases corrected definitions you can install them. Another advantage is that the master primary server is the only server that will be updated from the Internet. The remainder of the traffic will be within the Local Area Network (LAN) and Wide Area Network (WAN). For organizations that have smaller bandwidth internet connections this can be a very major consideration. The major disadvantage with this type of update is that it sends a full set of definitions when it updates a server or PC. So, a very large file is pushed to each PC every time there is a new set of definitions. In our organization the LAN and WAN were made up mostly of T1 and high end Frame Relay connections that could adequately accommodate this additional traffic.

LiveUpdate is not a full set of virus definitions rather it is an incremental update. Beings this is only incremental the size of the update is significantly smaller then with VDTM. LiveUpdate can be set up to either get the definitions directly from Symantec or from an Internal LiveUpdate server. Using Symantec directly will create an enormous amount of internet network traffic. Thus with a lower bandwidth internet connection this would not be an advisable type of update. Symantec recommends: "If you manage 1000 or more nodes, use the LiveUpdate Administration Utility to update virus definitions files and the Norton AntiVirus Corporate Edition program". [1]

The third method is to use the intelligent updater. Intelligent Updater files are self-extracting executables and must be downloaded directly from the Symantec site. This requires users to first download a 4-6 Megabyte file and second run the executable file on each computer. This creates a two step process for each end-user to perform. So we did not find this to be an acceptable method of update.

Currently Symantec publishes new virus definitions Monday – Friday via the Intelligent Updater method. Every Wednesday the definitions from the previous week are available via LiveUpdate. The exception to this is when there is a virus outbreak, Symantec will release the definitions via LiveUpdate as soon as they become available. Our organization has a policy that we get the intelligent updater definitions daily Monday – Friday. Once this is installed on the master parent server it will push the definitions out to the RSO's and PC's via VDTM.

We chose to use the VDTM method of updating the virus definitions.

Once we had assured that the virus definitions were up to date, we had to decide how we where going to configure the installations. Here are a few items that we configured to help protect our network.

- All PC's would do an Administrative Scan daily at 12:00 noon. These scans were performed in the background and were set to not allow the user to disable or stop the scan. If the user turns off the computer we have NAVCE set to "handle missed events for 8 hours". What this means is that if the computer is not on or is disconnected from the network at noon, when it does get turned on or logs into the network the scan will start for up to 8 hours after it was scheduled.
- We would not use the concept of a Quarantine Server. Files would first be set to clean the virus and if that failed the file would be deleted.
- All PC's at the RSO's level would look to their parent server for updates.
- All RSO parent servers would look to the CO master parent server for virus updates.
- Policy in the organization was that within 24 hours of new virus definitions becoming available they would be installed on PC's and servers in the organization. Thus it is my responsibility to daily make sure that the master parent server is up-to-date.
- File System Real-time Protection would be enabled and set so that infected files if not able to be cleaned would be deleted. This option was locked so that the user could not disable it.
- We enabled Microsoft Exchange Real-time Protection. We locked this option and set it to delete files/messages that could not be cleaned. When a virus was found it would notify the network administrators but no one else. (We learned with the "I LOVE YOU" virus that when a major outbreak occurs it creates additional traffic if we send a message to the sender and the recipient. Also during an outbreak a user's box would be filled with a very very large number of messages that just added to the virus hysteria.)

In theory we have all of our bases covered. File System Real-time Protection covers the PC from network threats from diskette sharing, FTP, downloading from the internet, messaging and from hackers. Microsoft Exchange Real-time Protection covers us from E-mail type viruses. So this should be good enough .. right? Well maybe, but we also decided to put in place one additional level of

security. As I mentioned in the beginning HQ had also bought NAVMSE and mandated that it be installed and operational.

MS EXCHANGE SERVER INSTALLTIONS:

Now we switch our attention to the E-mail side of virus protection. In our organization we have 10 Microsoft Exchange servers. We installed NAVMSE on each of them. The installation was very simple and there were very few items to configure. Now we had to decide on a mode of operation. The choices were:

- MAPI mode alone: Uses the Messaging API (MAPI) that was used for previous versions of Norton AntiVirus for Microsoft Exchange.[3] This mode actually logs into each mailbox and scans each piece of mail as it is delivered to the inbox.
- VAPI mode alone: VAPI is used to scan every attachment as it is saved or loaded from the Exchange information store. There is no information, however, about the sender, recipient, message subject, or message location. [2]
- VAPI/MAPI mode: It uses VAPI to guarantee that all attachments are scanned, and it uses MAPI to determine more information about the source of an attachment for logging, alerting, and reporting. [2]

We chose to initially implement the VAPI/MAPI mode of operation. We found that on some occasions though, we do switch to MAPI mode to try to get more information about particular attachments that appear to be reoccurring. Further settings were to notify the system administrators whenever a virus was found. We turned off the notifications to the sender and the recipients as well.

The next task, just like with the desktop installations, was to decide how vigilant we were going to be about keeping the virus definitions up-to-date. With our version of NAVMSE the only options for LiveUpdate is to have it enabled or not. If it is enabled you can choose the time of day you want it to run and how many times per month you want it to update. The maximum number of times per month is 10. I found this to be completely inadequate. So, I update the NACMSE whenever I update the master parent server.

Although scanning every message with the most current virus definitions is extremely important, it does little to stop outbreaks from new groundbreaking viruses. To further enhance our protection we added blocking policies. We started out with just a few attachment types being blocked such as *.exe, *.bat, *.pif, *.vbs, and *.lnk. Currently though we are blocking over 30 attachment types. A partial list is as follows: *.bat, *.ceo, *.chm, *.com, *.cpl, *.dll, *.eml, *.exe, *.hta, *.jar, *.jpeg, *.lnk, *.pif, *.scr, *.sct, *.shb, *.shs, *.vb*, *.vbe, *.vbs, *.wsc, *.wsf, *.wsh.

As a note on how NAVMSE handles the blocking of attachments. Keep in mind that as far as Norton is concerned a message with a blocked attachment is

considered a virus. Thus the administrators are notified each and every time someone sends a message with an attachment with a blocked extension. This is partly why we decided not to send notifications to the sender and the recipients. We found that the end users would become overly concerned and perform additional virus scans or would not use their system until someone of IT would come and look at their system. So we have a set of administrators that get the mail instead. They will look at the message and if a legitimate file was indeed being sent they would notify the sender of the situation and instruct them how to get the file through the Antivirus filtering. Below are the two messages that would be received by the administrator:

Sender of the infected attachment: XXX, ZZZZZZ
Recipient of the infected attachment: YYYYYY, XXX\Inbox
Subject of the message: I LOVE YOU
One or more attachments were deleted.
Attachment Love-letter-for-you.txt.vbs was Deleted for the following reasons:
Virus VBS.LoveLetter was found.

Sender of the infected attachment: Unknown Sender
Recipient of the infected attachment: Unknown
Subject of the message: Unknown
One or more attachments were deleted.
Attachment Bees.exe was Deleted for the following reasons:
Virus UNAUTHORIZED FILE was found.

As you can tell the second message is from the VAPI portion of the scan. Thus, very little information is available about the sender or recipient. When we get several of these types of messages we will temporarily change to MAPI mode to try to figure out who the sender and recipient are.

We also have NAVCE installed on our Microsoft Exchange servers. At the time we were unable to get a clear answer from Microsoft or Symantec on whether or not the Exchange directory should be excluded from the Realtime protection and from the administrative scans. So, we excluded them on the theory that if the scan was able to scan inside the Information Store it might corrupt it if it found a virus during an outbreak.

The last component to mention is that at the HQ level there is also installed Symantec AntiVirus Gateway Solution at the Organization level. So, all E-Mails entering and leaving the organization are scanned for viruses. They have also implemented an attachment blocking policy to block the types of extensions that are being blocked at the CO and RSO Exchange servers. To pull it all together the following figure shows how our organization is set up for Virus protection. Fig. 3

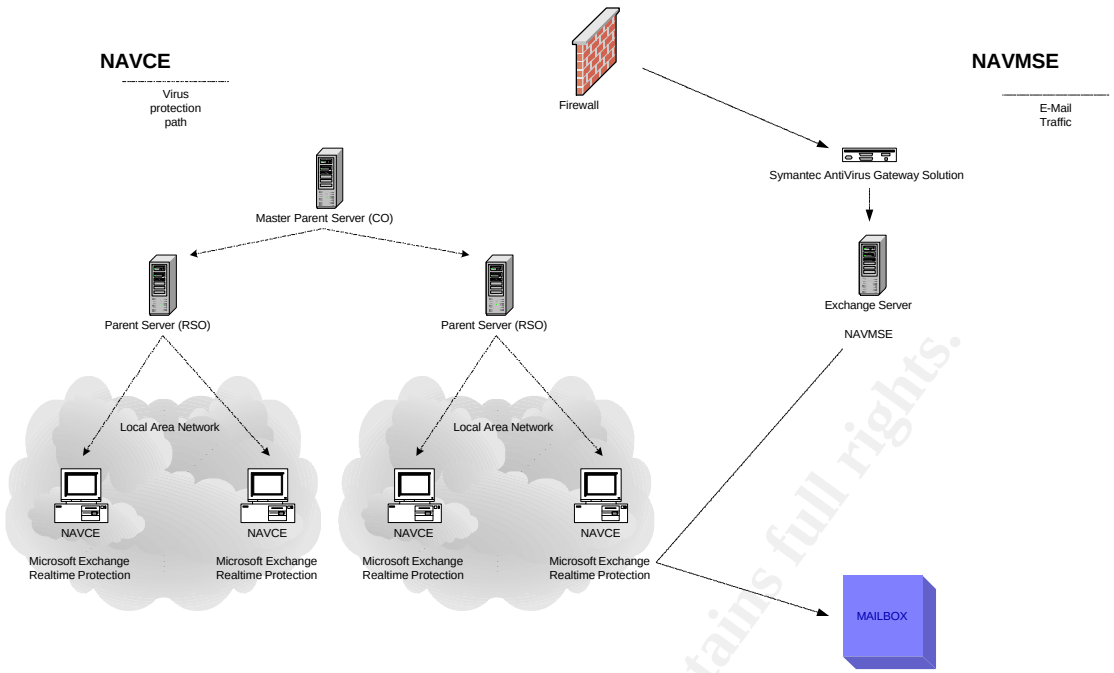

Fig. 3

The Results:

With all the mentioned installed programs and our configuration of these programs, we have been able to significantly reduce the numbers of virus infections for our organization. As far as E-Mail, greater then 98% of all the notifications sent to the administrators since July 2001 have been for invalid file types. Granted because we block most of the extensions associated with a majority of the virus types we do not know how many true viruses we have stopped. We do know that we have not had a major virus outbreak since the "I LOVE YOU" virus. We also know that we have not had as high a number of new viruses in the past year as well. "Experts have different theories as to why there have been fewer major virus attacks in 2002 than the previous year, but there is no denying that the difference has been marked. F-Secure (UK) ranked nine attackers in 2001 as Level 1 –the most serious ranking—but only two as of late 2002."[4] As far as the desktops go we have also seen a very small number of virus infections since we have implemented all of these programs.

What I find frustrating is that we have been forced to completely change the way we do business and we end up finding "The end result is an organization focused on defensive measures. You deploy physical security, firewalls, honey pots, virus protection, and usage policies, and hope for the best. It's the typical, common sense approach to protecting digital assets, but it can also strangle an organization."[5] In our organization we have had to create "public" drives on servers to allow the share of programs and files from within the organization that once were just sent through the E-Mail. When we do business with technical

support with outside companies, we have to have them change the way they do business as well. An example is, if we need to update a nonfunctioning program with a patch (exe) or dll, and it is not available via and intranet site, we have to have them change the extension on the attachment so that it will pass through the gateway. We are significantly more secure then we were 2 years ago. I often wonder what the cost is to make all the changes needed to get legitimate files transferred across the gateways and internal LANS and WANS. In conclusion I feel that we have significantly reduced the number and seriousness of the risk for virus infections in our organization.

Reference:

[1] Guarding Against Viruses is Getting a Lot Harder URL: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2871689,00.html

[2] Norton AntiVirus Corporate Edition™ Implementation Guide. URL: ftp://ftp.symantec.com/public/english_us_canada/products/norton_antivirus/navcorp/manuals/navce75i.pdf

[3] Norton AniVirus for Microsoft Exchange. URL: ftp://ftp.symantec.com/public/english_us_canada/products/norton_antivirus/navmse/manuals/navmse.pdf

[4] Virus Outlook: Bigger Trouble ahead. URL: http://zdnet.com.com/2100-1105-979066.html

[5]Strangled by security? URL: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2907848,00.html

Last Updated: July 28th, 2017

Upcoming Training

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
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
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
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event