Global Information Assurance Certification Paper

McAfee's Proactive Threat Protection Strategy

Jason Tidswell
GSEC v1.4b, Option 1
April 19, 2003

Abstract

This paper will research McAfee's proactive threat protection strategy to reduce the "Window of Vulnerability" (McAfee Security, Feb 2003) and attempt to discover if the product suite provides synergistic controls. I will also examine the products to be implemented, deployed and managed and then present an example to illustrate how they all compliment each other. This paper will not go into details about blended threat technology but is more concerned with the tools available for defeating them no matter what their propagation method.

Introduction

The GSEC tutorial states that '*one of the most effective attacks that penetrates standard perimeters is malicious code. These are things like viruses and Trojan software*'.(SANS Security Essentials, Network Security Overview, p. 1-2).

As the standard virus has now been superseded by the blended threat, what tools are available to organisations to effectively manage this anathema that in the end can and will affect bottom line profits? How do products offer an elegant, comprehensive, integrated, centralised management and reporting suite that are proactive to these threats?

So what is McAfee's strategy?

In essence this is a strategy to proactively manage the combination of the speed of attack, the blended attack mechanism and the evolving network environment. This is achieved by securing the enterprise against new threats in advance and to assist security personnel to quickly close the "Window of Vulnerability."

The "Window of Vulnerability" is described as the period of time when an enterprise is susceptible to attack and the ensuing damage. The window opens when the threat is created and does not close till all systems are protected from that threat (McAfee Security, p.3)

The strategy encompasses threat and risk management principles. The methodology is based on context establishment, threat assessment, risk analysis and risk management. The disciplines of the methodology are reflected in the product suite and are focussed on reducing the threats to a manageable level.

The primary focus is proactivity. Traditional reactive measures are insufficient due to the reduction in time for the threats to propagate and assault networks. The challenge is to

proactively reduce the speed of attack, the chance of attack success and the exposure to attack.
The secondary focus of the strategy is centralised management. The distributed nature of today's networks and the complex infrastructures of servers, workstations and network appliances, requires a robust powerful system that will not only manage anti-virus effectively, but take it to the next level of sophistication. Added to this is the almost impossible task of manually auditing and updating potentially thousands of machines

In addition to the management dilemma, it has been said that "*perhaps the greatest pitfall to centralized AV management is that it may impede a defense-in-depth AV strategy. The challenge is to move away from the proprietary model and provide the single console managing a number of AV applications*." (Information Security, Koziol, Jack. May 2002)

And, "*In addition to using AV scanners as a primary control, we need to build a more robust defense-in-depth architecture utlizing practical "synergistic controls*." (Information Security, Tippett, Peter. May 2002)

Another question that may be asked is, why aren't perimeter firewalls and IDS enough? It would seem that because the threats have evolved to a higher plane, the defenses must change as well. This is not to say dispatch of those perimeter firewalls. It is more along the lines of utlising different products to compliment existing ones, where they can protect against attack vectors not previously seen due to the nature of these evolving threats.

The primary products complementing McAfee's blended threat security arsenal include:

1. ePolicy Orchestrator 2.5.1
2. Desktop Firewall 7.5.1
3. ThreatScan 2.1
4. VirusScan Enterprise 7.0

I will now explore these products in a little more depth and look at their architectures and features.

ePolicy Orchestrator 2.5.1 (ePO)

ePO is the window to the network, it is the foundation for a multilingual, centralised management and policy enforcement for McAfee's proactive threat protection strategy. The security products are all deployed after policy configuration from the ePO console. This is made possible by the ePO Agent. Administrators manage policies, deploy relevant products and report on operational and threat activity from the ePO console.

The architecture of ePO consists of:

- the Console that allows a single control point for the server and agent;
- the Server that stores accumulated program data and software;

- the Agent that enforces software policy at the client machine; and
- the Database for storing information regarding outbreaks, agent installations, alerting data etc. which is then utilised by the reporting interface. (McAfee ePolicy Orchestrator Product Guide Version 2.0, p.11).

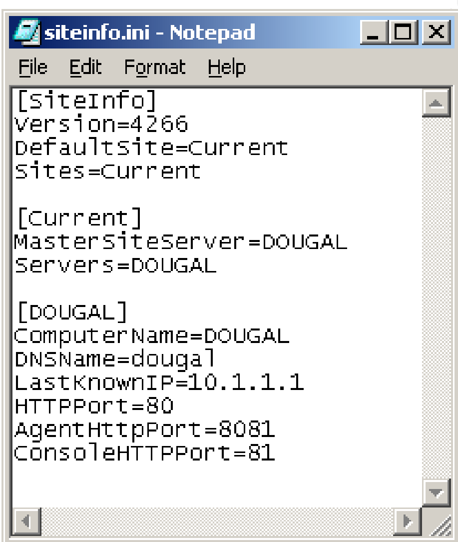
ePO utilises HTTP over IP and employs a proprietary algorithm to transmit data in a secured manner. Built for Internet use, it allows for agent-to-server communication over untrusted networks (McAfee ePolicy Orchestrator Product Guide Version 2.0, p.181).

ePO allows for cross-product management, currently ePO will manage Symantec's AV suite with further integration of products under development. This divergence from the proprietary model helps resolve the impeding of a defense-in-depth strategy mentioned previously. This is vital as many organisations' policy is to have dual AV implementations, especially in the Government and Defence arena.

ePO Communications

For the purposes of this paper it is important to understand how the security products installed on client machines interact and communicate with the ePO server to provide the alerting, reporting and operational data.

This is achieved by the ePO Agent. This 530kb program is fundamental to the architecture of ePO. It must reside on all machines on the network that you wish to manage for policy enforcement and operational control. The Agent is the workhorse of the system and works with the ePO server to monitor virus and threat activity on the network, install the security products, record threat events and enforce policies. Agent functions include installing itself, status communication, event and property collection, public key management, scheduling task execution and product installation.



The Agent is created when installing ePO and is pre configured to contact the ePO server via its IP address. A file within the executable "siteinfo.ini" contains this IP address of the ePO server and the HTTP port number the Agent should use to communicate back to the server (default is HTTP port 80 but recommend this is changed). In addition, on Agent initiation a unique Agent ID is produced containing a 64bit key that ensures each client has only one entry in the ePO database.

Should the Agent fail to contact the ePO server using the IP address, the Agent will establish communications utilising the DNS name of the ePO server and change the IP address within the "siteinfo.ini" file if required. (Day, p.2).

In reverse, the ePO server uses the IP address, DNS name, or NetBIOS computer name, in this order, to determine the network location of client computers for server to client communications.

The Agent collates all information pertaining to the client via Agent properties files (e.g. Fullprops.ini). The Agent is also cached on the client machine to record any local changes and in particular to enable the forwarding of Alerting events i.e. Threat Alerts.

For example, if a Threat Alert occurs on a client, the installed security product will detect this and generate an event. The Agent will react to this event and forward to the ePO server. There are various methods for advising security personnel of an event (network messaging, e-mail, pager etc.) but the data forwarded, is stored in the centralised database for report generation.

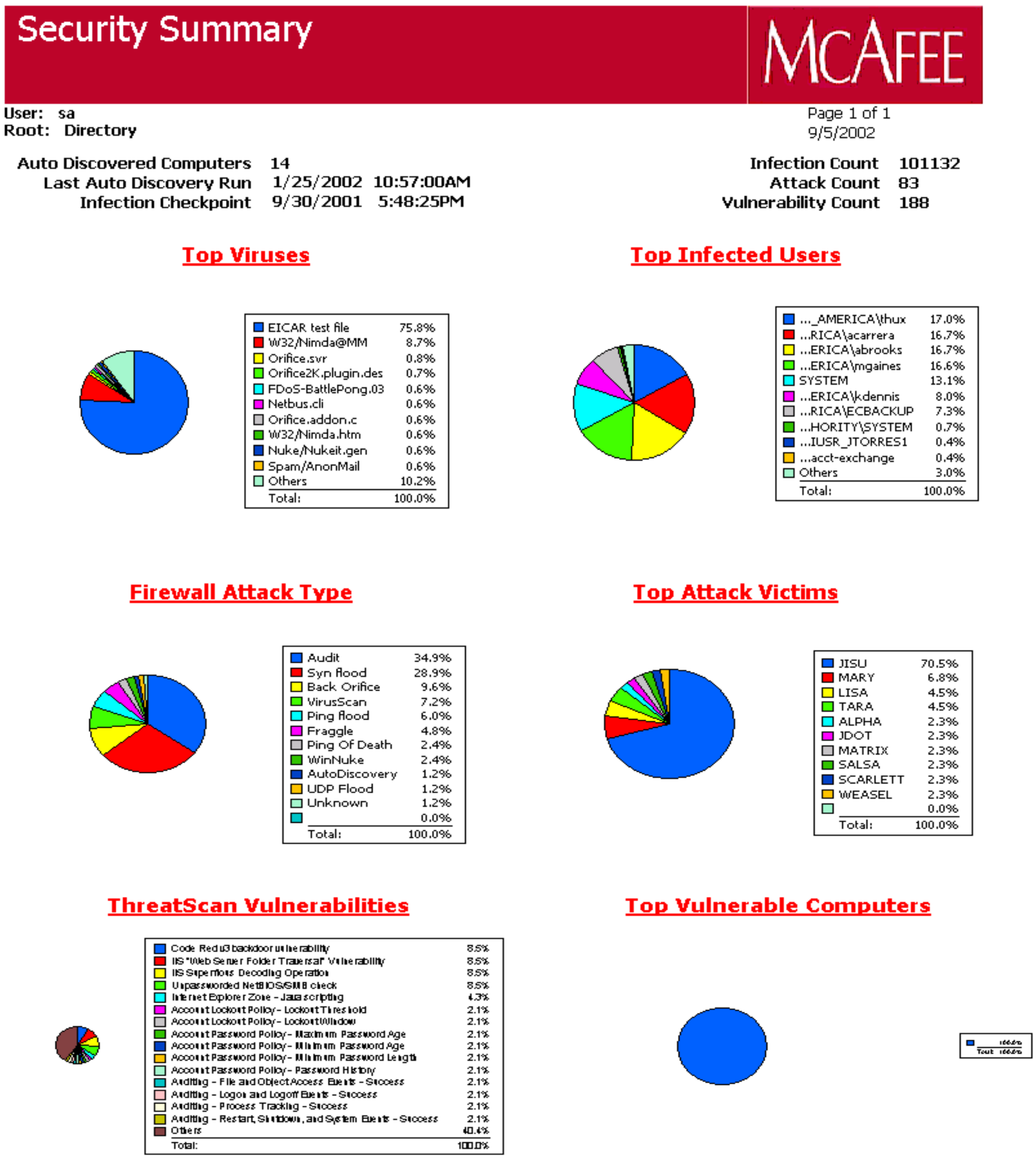
ePO Security Model

The security of communications between the Agent and the ePO server is achieved using PGP's PKI digital signing and authentication on messages traversing the network. When the Agent is first installed it generates its key pair. The first time the Agent communicates with the ePO server it sends its public key certificate. The ePO server stores all the Agents' public keys in the database and uses these keys to authenticate all future communications.

From the opposite direction, Agent installation software contains the ePO server public key. All messages received from the ePO server are authenticated by the Agent. If the package authentication fails, communications is halted and the package is discarded. (Day, p.4).

ePO Reporting

Reporting from ePO is considerable and comprehensive. It would seem that much development has been applied to this process to provide a wide array of different reporting options for all the products managed by ePO to complement the proactive requirements. Below is an example of a summary report.



In all, administrators are able to manage virus and threat protection from wherever they choose on their company network. ePO consoles and servers can be distributed allowing for management of regional topologies. It is important to keep in mind that all these rules, policies and procedures can be implemented silently in the background via the ePO Agent, allowing adherence to organisational and system specific policies.

VirusScan Enterprise 7.0

VirusScan 7.0 is installed, managed, deployed and reported on from ePO.

VirusScan 7.0 is the latest in McAfee's anti-virus suite and in addition will scan processes in memory for viruses, worms and trojans. For proactively defending against the blended threat scenario, this is vital as we know not all threats write their code to disk. The product resides on both servers and workstations eliminating the need for two separate anti-virus products.

Of importance is the AutoUpdating feature to ensure the VirusScan engine and signatures are up to date. There are many ways to achieve this updating task. The most recent enhancement is to create and maintain an internal software repository where you define exactly which McAfee anti-virus software updates to deploy to the machines on your network. (McAfee VirusScan Enterprise Product Guide Version 7.0.pdf).

Desktop Firewall 7.5.1

Deployed from ePO and an integral addition to McAfee's threat protection arsenal, Desktop Firewall and the included Intrusion Detection System (IDS) are used to detect and block attacks on individual systems, alert owners and administrators and to block any future traffic. The Firewall operates at the application and packet filtering level while the intrusion detection component is bi-directional defending against malicious code from spreading to other machines. The remote manageability of the Firewall/IDS from ePO allows for the creation of silent installations and the ability to enforce policy changes and commit them remotely to networked machines.

A point to mention is that the name Desktop Firewall is a little misleading as the product is deployed to servers as well.

The need for Desktop Firewalls is exemplified by the requirement to protect individual computers against attack from inside company networks, as perimeter firewalls only defend and block traffic from the outside, untrusted network.

The firewall utilises predefined protection levels and rule sets that allows for the control of the types of packets received and the ports that receive them. The functionality is extended to the creation of custom protection levels identifying the protocols, services, addresses and applications you wish to block or deny. (McAfee Desktop Firewall Product Guide Version 7.5.pdf, p.7)

Learn Mode is a particularly useful tool. Before deploying Desktop Firewall to all machines on the network, you allow a couple of machines to operate in Learn Mode for a few days to get a detailed view of all traffic and applications traversing the wire. This gives one a template for policies and rules that you wish to enforce. With this template in hand, you then turn off Learn Mode and deploy via ePO, this organisational protection level to your networked machines. There is a synergy here between the Firewall and ThreatScan, in that you can implement ThreatScan scanning results to create Desktop Firewall rules for blocking vulnerable applications.

The bi-directional IDS looks for suspicious activity and logs an alerting event if such activity is detected. The IDS can be configured to display an alarm when a threat event is detected, and to block the attack and any further events that may occur. This protection is applicable to attacks originating from both trusted and untrusted networks.

The IDS feature looks for specific traffic patterns used by attackers. It checks each packet that your computer receives to detect suspicious or known attack traffic. A template of known attacks is also used and updated regularly. Just like autoupdating signature files for VirusScan, this IDS attack template is updated the same way through ePO. For example some of the known attacks represented within these templates are Back Orifice, IP Spoofing, Fraggle, Bonk, Ping of Death, Port Scanning, SYN Flood, Teardrop etc. (McAfee Desktop Firewall Product Guide Version 7.5.pdf, p.99).

These templates make it much easier for personnel who are not security experts to use, deploy and understand these tools.

ThreatScan 2.1

ThreatScan is a viral vulnerability management add on solution to ePO and could be thought of as the risk analysis tool in McAfee's security suite. The product performs scans against intranets, Web servers, firewalls and routers to identify blended threat and virus related vulnerabilities in networks (McAfee ThreatScan Product Guide Version 2.0.pdf, p.21).

Rather than having to audit individual machines on the network, ThreatScan allows viral vulnerability scans to be accomplished from the ePO console. It scans and reports on unprotected, unmanaged, infected and virus vulnerable machines.

It achieves this by deploying three types of scans from the ePO console:

Resource Discovery Scans – find active machines on the network providing the standard configurations that may require further analysis. These include open ports and shares. It is recommended to perform this function first as the task just probes the network to detect responsive hosts without scanning for vulnerabilities. The scan can be configured to do the following for each and every host:

What hosts are responsive?
What operating systems are out there? .
Perform a trace route to the host.
Is the machine running the ePO agent?
Any open shares on Windows machines?
Service pack level on Windows machines
What services are running on Windows machines?

Which TCP and UDP ports are open?

The results of these scans are sent to the ePO reporting repository for analysis and further troubleshooting and for use in later detailed scans. Additionally you can schedule Resource Discovery scans on a regular basis to ensure you report on new machines being added and removed.

Remote Host Audit Scans – primarily checks that machines are compliant with the companies security policies e.g. minimum password length.

> Account Policy- This scan checks for violations in the account policy. The scan will check for password age, uniqueness, length, lockouts and disconnects.
>
> Audit Policy- One sets audit policy parameters to match local audit policy parameters in your Windows environment. For example Logon and Logoff failures, File and Object Access, Security Policy Changes.
>
> Legal Policy- Checks for violation of company's legal policy.
>
> Browser Zones- Checks for browser zone policy parameters within the local intranet, trusted sites, Internet and restricted sites. Covering ActiveX controls, Java, Plug-ins and User Authentication. It is important to set the browser settings as defined by the desktop management team otherwise your report will display machines not in compliance with policy set on the scanner (McAfee ThreatScan Product Guide Version 2.0.pdf, p.50).

ThreatScan Vulnerability Scans – these scans ascertain whether machines are vulnerable to specific known attacks. These vulnerability scans launch known exploits against your network resources, therefore care and management permission would be advisable. ThreatScan contains a database of vulnerability modules in template format, similar to the Firewall IDS and are updated and downloaded accordingly. The list is too exhaustive to repeat but covers the Nimda's, CodeReds, Goners and Deloders of the world and it is these threats and many more that are run against the networked machines and reported on through ePO.

For Example

So, I anticipate that an example should highlight how these products working together can provide synergy between each other, and both a proactive and reactive defence to the assessed threat.

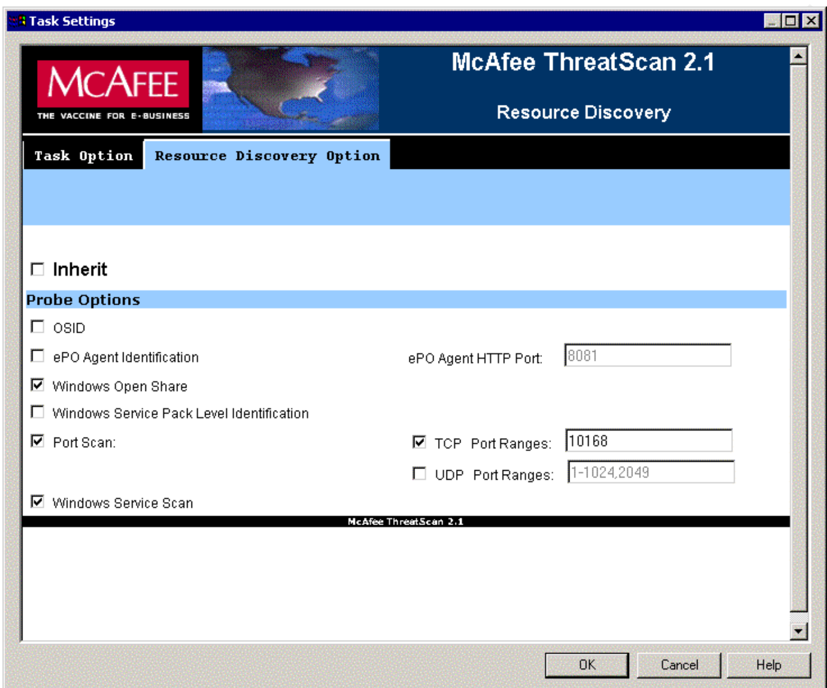
The LovGate Worm

LovGate was discovered on the 18th February 2003 and is a mailing worm that spreads itself via network shares, and drops a remote-access trojan. The worm is capable of sending a reply to all new messages found in the user's inbox (Outlook and Outlook Express) by using its own SMTP engine. It will also attach itself to the message. The technique is known as a 'reply mailer' which ensures the worm does not create spikes in mail volume, but is slower than a mass mailer.

AVERT advises "The worm propagates via email (it contains its own SMTP engine) and over network shares. It copies itself to folders/subfolders on open shares, and replies to messages in the user inbox. Additionally, it drops a backdoor component (port 10168, and 1192 on NT based systems, is opened on victim machines)." (AVERT Virus Information Library, February 2003.)

So, what pro-active tasks can be performed from the ePO console to address the LovGate threat?

The displayed screen dump shows the Resource Discovery options for ThreatScan from the ePO console. The following parameters are used to complete the task.



On first notification and pre-posting of updated ThreatScan module and VirusScan signature Dat's and to limit the infection rate:

1. Check for the scale of infection by running a ThreatScan Discovery scan to report on machines that have port 10168 open.

Check option 'Port Scan', check option 'TCP Port Ranges' and insert 10168 in the box.

2. Use ThreatScan to discover if these two services are running:

- Window Remote Service
- Windows Management Extension or dll_reg

They can be created and started by the worm on Windows NT/2000/XP machines.

Check option 'Windows Service Scan'. The report will list Windows services running on each machine.

3. Use ThreatScan to report on network shares as the worm may propagate via this vector.

Check option 'Window Open Share'. The report will identify open shares on Windows based machines.

With these options checked, deploy an immediate task from the ePO console to your networked machines (the task can be randomised for bandwidth considerations). When completed, the relevant ePO report will reveal the current state of the machines and additional configurations required.

In addition, OSID - will determine the operating system of remote hosts.
ePO Agent Identification - identifies if the machine is running an ePO Agent.
Windows Service Pack Level Identification - returns the service pack level.

4. Configure a desktop firewall rule to block port 10168, unless specifically being used by an application, and run an immediate task from ePO. It may open ports 20168 and/or 1192 to e-mail the hacker the machine has been compromised. Further traffic through these ports will generate a firewall alert and be reported to ePO.

Once updated ThreatScan modules and VirusScan virus signature are received:

1. From ePO perform an AutoUpdate task for ViruScan 7.0 to apply the virus signatures to all machines on the network. It is advisable to clean infected machines first, then update the remainder.

2. Run ePO infection reports to confirm progress on removal of the worm.

3. Run the ThreatScan module update to confirm vulnerabilities are diminished or non existent.

Conclusion

"It is widely acknowledged that blended threats provide the single biggest security risk on the horizon for businesses, and the single biggest challenge for security vendors." (SC Online Magazine, Viveros, Sal. November 2002.)

This being the case, a solution that allows us to proactively focus on the threat and provide data on infected hosts and potential victims from a centralised management system is providing the synergy we require. An elegant solution that is constantly evolving through best practice scenarios and making the product suite as sophisticated or as simple as you like could take us to a fully integrated almost hands free automated environment. However, no matter how proactive or reactive product suites are, sound incident and disaster management plans will never go away.

References

1. SANS GSEC Study Modules. SANS Security Essentials II, Network Security Overview, Defense in Depth. p. 1-2

2. Koziol, Jack. "Command and Control." Information Security. May 2002
URL: http://www.infosecuritymag.com/2002/may/commandcontrol.shtml

3. Tippett, Peter. "Building "Synergistic" AV." Information Security. May 2002.
URL: http://www.infosecuritymag.com/2002/may/synergisticav.shtml

4. McAfee Security. "Proactive Threat Protection: Reducing the Window of Vulnerability." White Paper. February 2003.
URL: http://www.mcafeeb2b.com/products/proactive-threat.asp

5. AVERT Virus Information Library, W32/Lovgate.a@M. February 19 2003.
URL: http://vil.nai.com/vil/content/v_100085.htm

6. Viveros, Sal. "Cooperation More Important Than Competition." SC Online Magazine. November 2002.
URL: http://www.scmagazine.com/scmagazine/sc-online/2002/article/49/article.html

7. Network Associates Technology, Inc. "McAfee ePolicy Orchestrator Product Guide Version 2.0.pdf.", 2001.

8. Network Associates Technology, Inc. "McAfee VirusScan Enterprise Product Guide Version 7.0.pdf." 2003.

9. Network Associates Technology, Inc. "McAfee Desktop Firewall Product Guide Version 7.5.pdf." 2002.

10. Network Associates Technology, Inc. "McAfee ThreatScan Product Guide Version 2.0.pdf." 2002.

11. Day, Greg "ePO Networking Explained.pdf" Network Associates, March 19 2002.

Last Updated: July 22nd, 2017

Upcoming Training

SANS Prague 2017	**Prague, Czech Republic**	**Aug 07, 2017 - Aug 12, 2017**	**Live Event**
SANS Boston 2017	**Boston, MA**	**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**
Community SANS Omaha SEC401*	**Omaha, NE**	**Aug 14, 2017 - Aug 19, 2017**	**Community SANS**
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 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**
SANS Adelaide 2017	**Adelaide, Australia**	**Aug 21, 2017 - Aug 26, 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**
Mentor Session - SEC401	**Ventura, CA**	**Sep 11, 2017 - Oct 12, 2017**	**Mentor**
Community SANS Albany SEC401	**Albany, NY**	**Sep 11, 2017 - Sep 16, 2017**	**Community SANS**
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**
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**
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**
Community SANS Sacramento SEC401	**Sacramento, CA**	**Oct 02, 2017 - Oct 07, 2017**	**Community SANS**
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**
Mentor Session - SEC401	**Arlington, VA**	**Oct 04, 2017 - Nov 15, 2017**	**Mentor**