Global Information Assurance Certification Paper

Chang Boon Tee
Version 1.0
Building a secure Internet Data Center Network Infrastructure

As a consultant in a System Integration company, I am exposed to various network and system architecture, which varies from industries to industries. Generally, I would categorize the market into three major areas:

i) Financial Industries – consists of financial industries like the banking sector, insurance and securities firms
ii) Non-financial industries – consists of manufacturing companies, government sector and the transportation sector
iii) Telecommunication industries – consists of telcos which provide Internet Access, phone and mobile access, as well as Data Center that provides hosting infrastructure

Each of these industries imposed different levels of risk in terms of its network and system architecture as well as its business requirements. In this paper, I will focus mainly on the telcos, which provide Internet Web hosting infrastructure to corporate customers.

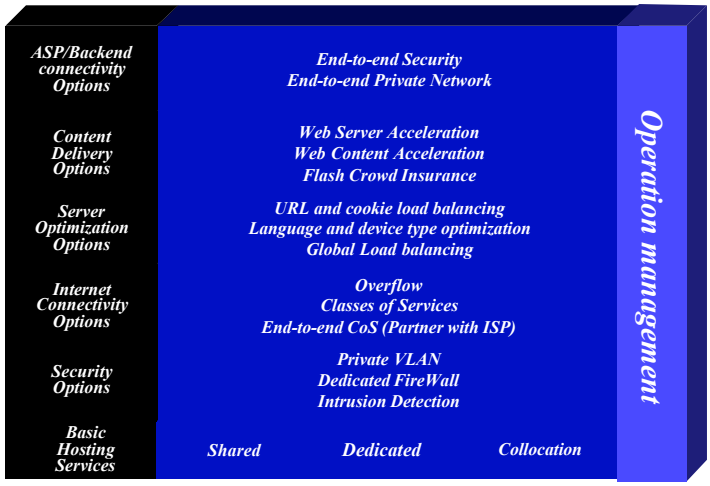
The principle goal of this paper is to provide best practice information on designing and implementing secure networks in an Internet Data Center. I will focus on the expected threats and their methods of mitigation, rather than on "Put the firewall here, put the intrusion detection system there." I will begin this document with an overview of the architecture, then details the specific modules that make up the actual network design. The first three sections of each module describe the traffic flows, key devices, and expected threats with basic mitigation diagrams. Detailed technical analysis of the design follows, along with more detailed threat mitigation techniques and migration strategies.

Architectural Components of an IDC Service Provider

The question is "What is an IDC"? An IDC is generally as a Data Center with facilities that provide hosting capabilities to any organizations who would like to host their servers, applications in the data center. The data center is equipped with video surveillance camera, on-site security officers, backup generators, biometrics sensors, fire suppression system and on-site management. Typically, an Internet Data Center provides the following services:

i) Shared Web Hosting – In this service, the customer typically uses a portion of a server
ii) Dedicated Server hosting – the customer uses the whole server and is normally a fully functional e-commerce software.
iii) Co-location hosting – The customer has dedicated racking space to house their servers
iv) Application hosting – The customer application is hosted at the IDC

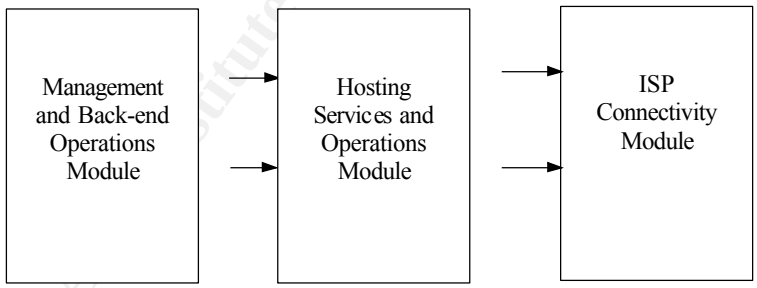
The IDC architecture depicted below is pretty much based on Cisco's recommendation in terms of building a scalable, robust and a secure network infrastructure:



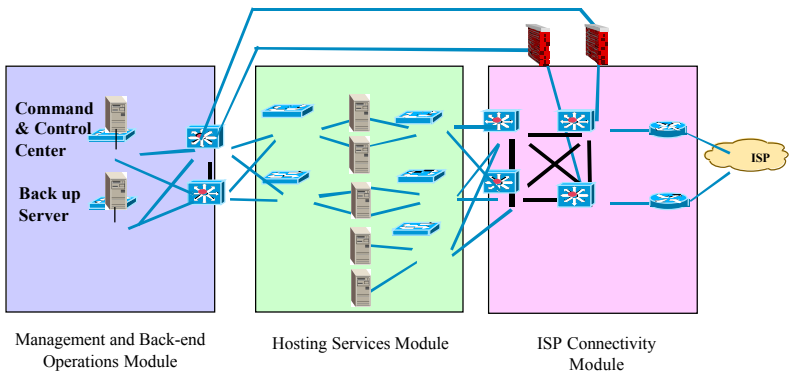
Modular Approach

I would like to address the concept of an IDC center in a modular approach. Each of this module is essentially a functional module with application, network and security relationships between all the functional modules. With this approach, it allows an IDC to evaluate and implement security on a module by module basis, instead of attempting the complete the architecture in a single phase.

The figure below represents each of the functional modules. This high level overview shows the flow and functional relationship between the modules.



The diagram below represents a view of the modules within each functional block. Each of the modules will perform specific functions and will require specific security measures in conjunction with its functions. The diagram also represents an architectural view of a typical IDC network layout.



1) Management and Back-end Operations module

Essentially, the objective of having a management module is to ensure the management of all network and host devices within the IDC are being managed securely. Typically, these are the key devices in a Management module:

- Firewall Management console – this console is used to manage it's own firewall as well as customer's firewall
- Intrusion Detection System Console – the console is used to manage the network-based IDS and host-based IDS. It also serves as the central point for alert notification as well as management and configuration of all the IDS throughout the network. When firewalls are properly configured, they keep out most of the undesired traffic. However, in order to provide some level of access, firewalls have some tunnels left open that can be exploited by hackers. Packets that pass through these tunnels are typically not analysed by the firewall and allowed to pass through unexamined. This means that the internal devices have to be relied upon to protect the network for the allowed data streams. This is where intrusion detection systems (IDS) come into play, to compensate the above-mentioned weaknesses of firewalls. A complete IDS has two components. The first is a network-based system that monitors network traffic and detects attacks such as Distributed Denial of Service (DDoS) attacks based on recognised traffic signatures. The remaining component is a host-based system that monitors activities and events (execution of critical files, log-ons etc.) occurring within a host.

- Firewall – the function of this firewall is to control all incoming and outgoing traffic to/from the management network via specific ports.
- Network-based IDS – provides detection of attack that may successfully pass through the firewall and capture suspicious traffic within the module itself. The IDS is deployed in *Stealth Mode*. Most IDS allows the configuration to monitor network traffic on one stealth interface and communicates with the IDS management network on another. This is called 'stealth mode' because the monitoring NIC does not have an IP address and is therefore invisible on the network. This configuration will further enhance the security of the IDS and the network.
- Syslog Server – this can be the central location for all the network devices as well as the host to send their respective logs to.
- Network management system – this server serves as the central SNMP monitoring for all devices.
- RADIUS/TACACS Server – it provides password management to network devices. Thus eliminating the need to store username and passwords on the device itself. It can also integrate with a Two-Factor authentication server to provide one-time password.
- Terminal Server – this server will be used to provide any configuration changes to devices
- Layer 2 switch – used to link up all the management module devices and preferably supports Private VLAN for added protection.

One of the most important tasks in the Management module is having proper logging and reporting capabilities for devices throughout the network. However, the challenge is always to read and maintain logs from all the devices in the network. Therefore, this management module can also be known as an out-of-band network. An OOB network is essentially a network where there is no production traffic. All the network devices will then send data and logs to the OOB network via direct connection. By having this network, managing logs and reporting becomes easier and more straightforward. All the logs can be directed to the Syslog server and in the event of any network related problems or security breach, the data and logs collected would be extremely useful for troubleshooting and analysis. The logs gathered from the syslog server can always complement the logs gathered from the IDS as well as the firewall for a more complete analysis

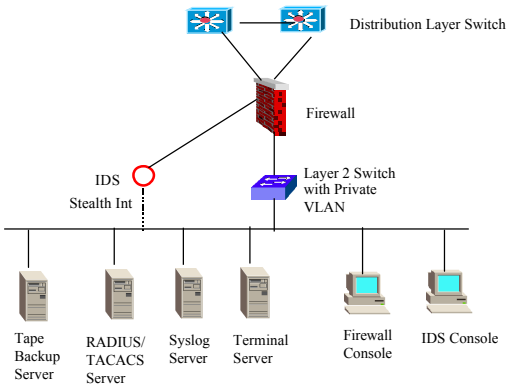
Another important area to look at is the alerting function. When an attack do occur, administrators will need to be notify and alerted. Thus, by utilizing in-built alerting plug-ins within the firewall/IDS or third party alert notification system such as Alarm Point, all appropriate alarms and alerts will be sent to the administrators via email, paging, SNMP traps and etc.

When all the alarms and alerts are gathered from multiple different sources, it is very important that the time of events are consistent and synchronized with each other. Thus, in order to synchronized the time, each of the network and host devices needs to be configured to point to a Network Time Protocol (NTP) server that will provide clocking to all the devices. This will ensure accurate and synchronized time among all devices.

Another important task is the segregation of duties and rights of operators and root administrators. It is always vital that to assign different privileges to different users. An operator will normally be assigned read-only rights and will not be allowed to do any configuration changes to a system. Daily tasks such as back-ups, monitoring and alerting are

among the routines of an operator. Root administrators will have the administrative rights to the system. However, when an attack do happen, it is critical to know when is the last changes that took place. Therefore, proper Change Management Control will need to be in place to ensure that all system and configuration changes are properly documented.

Wherever possible, communication between all devices to the management module should be encrypted such as through the use of IPSEC, SSH or SSL encryption. The figure below shows a physical layout connectivity in the Management Module. Private VLAN is configured on the layer 2 switch to prevent hosts on the same subnet from communicating unless necessary.



2) Hosting Services Module

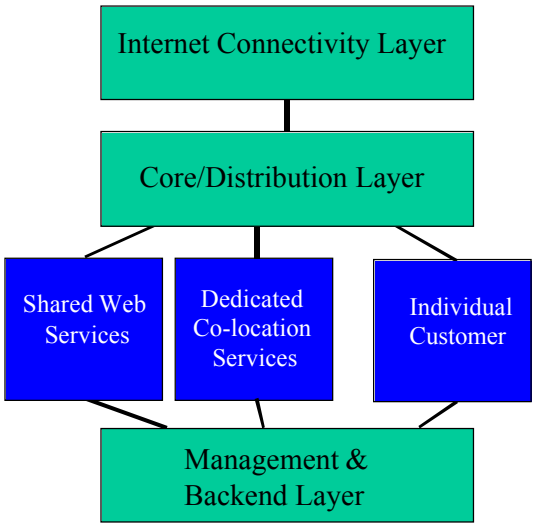
In this module, each IDC may deploy different ways in designing the architecture for the hosting network based on specific customer's requirement. In this paper, I will categorize the deployment into three categories:

1) Sharing of a single firewall amongst multiple different customers
   In this scenario, the IDC will basically host a single firewall to protect multiple customers. However, this solution will only cater for a few basic services that will be allowed through the firewall itself. There are two ways to deploy this as well. The first will be connecting each customer to a different firewall subnet. In this case, the firewall will have multiple network interface cards to cater for each of the customers network. The second option is to connect the customer's network to a Layer 3 switch and assign individual VLAN to each of the customer. The switch will then be connected to the external firewall. Proper access control list will be implemented on the switch to prevent hosts within the switch to communicate with each other.

2) Customer having their own dedicated firewall and IDS
   This is especially true for co-location customers whereby the customer will host their

servers in a dedicated rack. In a single rack, all the servers are protected by a dedicated firewall and IDS is also deployed to provide better security.

3) No added security devices
The customer will host their servers without any security devices like firewall or IDS.



In this module, there are a host of threats and risks that the IDC will have to undertake. Among the threats are:

- Operating system and application layer attacks
  This attack can range from attack on the OS itself to attack to the application layer of the system. This is done by exploiting vulnerabilities and loopholes in the server itself. Apart from this, another form of common attack are virus attacks. The IDC or the customer themselves can deployed gateway anti-virus that intercepts HTTP, SMTP and FTP traffic traversing to and from the servers. By keeping up to date with the latest OS patches and fixes, the risk of getting compromised can be minimized. Host-based IDS can also be deployed to ensure that attacks to the host itself can be immediately detected and notified for immediate actions.

- Unauthorized intrusion
  This is by far the most common attack ranging from network probing to unauthorized port scanning. This threat can be very much mitigated to the use of proper access control and IDS. The network-based IDS deployed should have the capability to capture huge amount of traffic and be able to capture traffic across multiple VLANs. Generally, the types of traffic traversing in this module are WWW, FTP, SMTP and probably some Telnet traffic.

- Packets sniffing
  This can be easily limited through the use of switching technology.

- Exploitation of trust relationship between hosts
  The compromised of a server in the same subnet can lead to the exploitation of other servers within the subnet. Normally, in order to mitigate the threat of a compromised device, proper filtering is implemented at the firewall, router or Layer 3 switches to prevent exploitation from a compromised server. However, in a network within the same subnet, any host within the subnet can communicate with the rest of the hosts in the subnet. Thus, Private VLAN is implemented on the Layer 2 switch in order to prevent a compromised device from communicating with other hosts on the same subnet.

- IP spoofing
  This can be stopped on the firewall itself. If it is a locally initiated spoofed attack, RFC 2827 filtering on the switch can also help to limit the threat.

All servers within this Hosting Module are generally overlooked in terms of security. Thus, in summary, deployment of network-based and host-based IDS, access control at different levels, private VLANs, strong passwords and up-to-date system administration will be able to prove a better countermeasure and response against external as well as internal attack.
.

3) ISP Connectivity Module

This module will consist of the distribution and core layer switches as well as the border routers connecting to the Internet. The threats in this module typically targets the border router, core switches as well as the network itself. Among the threats are:

1) Router exploit
   Routers by itself can be exploited in many ways. Like servers, they too are vulnerable. In the Internet, the customer's edge router is probably the first visible object. It is the device that provides access to and from every network and if the router itself is not secure, it can easily be compromised. There are standard ways to harden and secure a router and in summary, these are the basic necessary steps in hardening a router:
   - Password management
     The best way to handle passwords is to store them on a TACACS+ or RADIUS authentication server. However, almost every router will still have a locally configured password for privileged access. Simple steps like having multi-tier passwords and encrypting the passwords will reduce the likelihood of the password being compromised
   - Controlling access to the router. Cisco router for example may support access and connections via Telnet, rlogin, console port and others. Thus, controlling access to the router via these means will ensure that only authorized administrator is allowed to login to the router. Access to the router can also be enhanced through the use of two-factor authentication together with Terminal Access Controller Access Control System Plus (TACACS+) or RADIUS server.
   - Locking down Simple Network Management Protocol (SNMP) access to a router
   - Turning off unnecessary services if not required such as HTTP, TCP and UDP small services, Finger, CDP and NTP
   - Proper logging of router events will facilitate troubleshooting and analysis in the event

of network problem or security breach. This can be achieved by sending the router logs to a syslog server in the Management Module. Also, in order to ensure that the routers time are synchronized, all the routers in the network can be configured to point to a NTP server

- Configure anti-spoofing on the router will minimize the risk of a spoofed attack. Configuring anti-spoofing is normally done on the border router to prevent external spoofing attack.
- If the routing protocol used in the router supports authentication, it is best enable that as well. This can help in some of the attack based on routing information.
- Basic filtering and access control list can also be configured to limit only legitimate traffic through the router. The router can therefore act as the first layer of access control for traffic coming into the network.

2) Switches

As for switches, most of the methods in securing a router apply to switches as well. However, there are not as much of information available in a switch as compared to a router. Other than the above, there are a couple steps that can be taken in further securing a switch:

- Trunk settings on a port should turned off if the port is not used as a trunk port. This will prevent a host receiving all traffic on a trunk port if the port is configured with trunk settings.
- Disable all unused ports to prevent any unauthorized used of the ports to gain access to the network resources
- VLAN number on a trunk port should not be use anywhere else in the switch. This will prevent packets tagged with the same VLAN as the trunk port from reaching another VLAN without crossing a Layer 3 device
- Configuring Private VLAN on a switch will provide added protection to the hosts residing on the switch. Once deployed, if there is a compromised host in the network, it will not be able to communicate with other systems

3) Network Exploit

This exploit normally targets to bring down a network by flooding the network with enormous amount of traffic, so much traffic that the entire network becomes congested and simply stop receiving anymore traffic. This causes a Denial of Service to the network, as legitimate traffic is now unable to access the network. Distributed Denial of Service attack is such an attack and when it is executed successfully, it cannot be stopped. Such an attack can only be mitigated through cooperation with the ISP. The ISP can limit the amount of traffic flooding the customer's network by enabling rate-limiting feature on its router. Once the traffic exceeds a certain threshold, the traffic will be dropped.

At the customer border router, this rate-limiting feature can also be enabled to provide additional layer of control against the Ddos attack

Sample Router Configurations

Here are the basic configuration options present on nearly all routers in the SAFE lab:

```
! turn off unnecessary services
!
no ip domain-lookup
no cdp run
no ip http server
no ip source-route
no service finger
no ip bootp server
no service udp-small-s
no service tcp-small-s
!
!turn on logging and snmp
!
service timestamp log datetime localtime
logging 192.168.253.56
logging 192.168.253.51
snmp-server community Txo~QbW3XM ro 98
!
!set passwords and access restrictions
!
service password-encryption
enable secret %Z<)|z9~zq
no enable password
no access-list 99
access-list 99 permit 192.168.253.0 0.0.0.255
access-list 99 deny any log
no access-list 98
access-list 98 permit host 192.168.253.51
access-list 98 deny any log
line vty 0 4
access-class 99 in
login
password 0 X)[^j+#T98
exec-timeout 2 0
line con 0
login
password 0 X)[^j+#T98
exec-timeout 2 0
line aux 0
transport input none
password 0 X)[^j+#T98
no exec
exit
banner motd #
This is a private system operated for and by Cisco VSEC BU.
Authorization from Cisco VSEC management is required to use this system.
Use by unauthorized persons is prohibited.
#
```

```
!
!Turn on NTP
!
clock timezone PST -8
clock summer-time PST recurring
ntp authenticate
ntp authentication-key 1 md5 -UN&/6[oh6
ntp trusted-key 1
ntp access-group peer 96
ntp server 192.168.254.57 key 1
access-l 96 permit host 192.168.254.57
access-l 96 deny any log
!
!Turn on AAA
!
aaa new-model
aaa authentication login default tacacs+
aaa authentication login no_tacacs line
aaa authorization exec tacacs+
aaa authorization network tacacs+
aaa accounting network start-stop tacacs+
aaa accounting exec start-stop tacacs+
tacacs-server host 192.168.253.54 single
tacacs-server key SJj)j~t]6-
line con 0
login authentication no_tacacs
```

Sample Switches Configuration

Here is the base security configuration present on nearly all CAT OS switches in the SAFE lab. IOS switches use a configuration nearly identical to the router configuration.

```
!
!Turn on NTP
!
set timezone PST -8
set summertime PST
set summertime recurring
set ntp authentication enable
set ntp key 1 trusted md5 -UN&/6[oh6
set ntp server 192.168.254.57 key 1
set ntp client enable
!
! turn off un-needed services
!
set cdp disable
set ip http server disable
```

```
!
!turn on logging and snmp
!
set logging server 192.168.253.56
set logging server 192.168.253.51
set logging timestamp enable
set snmp community read-only Txo~QbW3XM
set ip permit enable snmp
set ip permit 192.168.253.51 snmp
!
!Turn on AAA
!
set tacacs server 192.168.253.54 primary
set tacacs key SJj)j~t]6-
set authentication login tacacs enable telnet
set authentication login local disable telnet
set authorization exec enable tacacs+ deny telnet
set accounting exec enable start-stop tacacs+
set accounting connect enable start-stop tacacs+
!
!set passwords and access restrictions
!
set banner motd <c>
This is a private system operated for and by Cisco VSEC BU.
Authorization from Cisco VSEC management is required to use this system.
Use by unauthorized persons is prohibited.
<c>
!console password is set by 'set password'
!enter old password followed by new password
!console password = X)[^j+#T98
!
!enable password is set by 'set enable'
!enter old password followed by new password
!enable password = %Z<)|z9~zq
!
!the following password configuration only works the first time
!
set password
X)[^j+#T98
X)[^j+#T98
set enable
cisco
%Z<)|z9~zq
%Z<)|z9~zq
!
!the above password configuration only works the first time
!
set logout 2
```

set ip permit enable telnet
set ip permit 192.168.253.0 255.255.255.0 telnet

Catalyst 3500XL Private VLANs

This configuration snapshot details the configuration for private VLANs on the public services segment:
interface FastEthernet0/1
port protected
!
interface FastEthernet0/2
port protected

References

Cisco System. “Improving Security on Cisco Routers” Date Unknown URL: http://www.cisco.com/warp/public/707/21.html

Convery, Sean and Bernie Trudel. "Cisco SAFE": A Security Blueprint for Enterprise Networks. Internet. Monday June 25, 2001. http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safe_wp.htm

Ferguson, Paul. "Request for Comments: 2827". Network Ingress Filtering: Defeating Denial of Service Attacks, which employ IP Source Address Spoofing. Internet. May 2000. http://rfc.net/rfc2827.html

Andrew L. Briney, "Zen and the Art of Intrusion Detection" ComputerWorld, Mar/12/2001 (2001) URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO58458,00.html

SANS Institute. "How To Eliminate The Ten Most Critical Internet Security Threats ver 1.33" 25 June 2001. http://www.sans.org/topten.htm

Cisco Systems. Defining Strategies to Protect Against TCP SYN Denial of Service Attacks http://www.cisco.com/warp/public/707/4.html , Cisco Systems

Last Updated: July 25th, 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
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
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event