Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

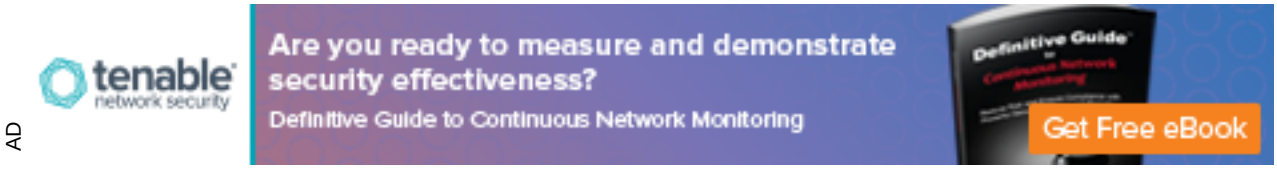
This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Mainframe Security featuring CA - Top Secret

This document will provide an overview of the current (2002) status of mainframe security and a detailed understanding of the CA-Top Secret mainframe security product. It will also provide an overview for using Top Secret and an in-depth guide for auditing and reviewing Top Secret security.

Copyright SANS Institute
Author Retains Full Rights

AD



Mainframe Security featuring CA-Top Secret
by Chad Barker
February, 2002 version 1.3

Introduction

This document will provide an overview of the current status of mainframe security and a detailed understanding of the CA-Top Secret mainframe security product. It will also provide an overview for using Top Secret and an in-depth guide for auditing and reviewing Top Secret security.

Mainframes Today

With the surge in technological advances and the big push for distributed systems one would assume that mainframes are dying a quick death. Technology leaders seem to be pushing to move legacy applications off the mainframe to midrange systems. However this is not necessarily the case. Many companies are still using mainframes today and many of them are looking for ways to integrate the mainframe with their client-server networks. [11]

Many of the legacy mainframe applications are still an integral part of company's revenue stream or back-office systems. The cost and difficulty of re-engineering these applications is forcing company's to keep the mainframes around. And because system integration is often critical to a company's success it is becoming more important to integrate the mainframe and midrange applications.

IBM has added significant functionality to their mainframe. Mainframes can now serve as a firewall, run e-commerce systems, support TCP/IP, use LDAP to secure access to directory information, and run UNIX.

While mainframe security is generally considered more secure than other platforms, this new mainframe functionality has introduced greater security risks. Luckily there are several security packages specifically developed for mainframe security. The three main products are:

IBM's Resource Access Control Facility (RACF)
Computer Associates' Access Control Facility 2 (ACF2)
Computer Associates' Top Secret

Each of these software packages has been around for many years and have been effectively implemented and tested over time. Each of these packages will allow a secure mainframe environment if implemented and maintained appropriately. This paper will focus exclusively on the Top Secret product.

[11] Korzeniowski

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

Top Secret Overview

As stated in the previous section, mainframes have continued to receive less focus in most IT organizations. And mainframe security is usually assigned a lower priority than midrange platforms. This is primarily because mainframes are not known to be associated with significant hacking attempts, viruses, or other security breaches. What these organizations tend to forget is that most security breaches (and usually the largest in terms of financial losses) are internal breaches. So while organizations focus on firewalls, intrusion detection systems, virus prevention, and VPNs, they are not spending their time and resources on the biggest risk…..internal security. The mainframe is still a core system for many institutions and its role is increasing to act as a file, web and application server. This creates additional emphasis on mainframe security. A secure perimeter doesn't add much value if the interior is insecure!!

The focus of the remainder of this paper will be utilizing Top Secret to improve internal mainframe security. It will attempt to provide an overview of how Top Secret works, some important commands (for Security Administrators), and a brief audit guide (for Security Auditors). It will not get into the details of the newer features of Top Secret (i.e. LDAP, UNIX, firewall capabilities, etc.) but will focus on the more traditional mainframe security controls.

Top Secret Administration

Top Secret provides many functions including: system entry validation, individual accountability, auditing, resource access control, and security administrator control. It is hierarchical in nature allowing a great deal of flexibility for the organization. Each user has a unique user ID called an ACID (Accessor ID). User access can be restricted to allow access only to certain facilities or recources. Each ACID is assigned certain access privileges that are maintained in the user's Security Record. All of the security records are maintained in the overall Top Secret Security File. The Security File is an encrypted database that contains all user access permissions.

Top Secret allows control over user password attributes. Top Secret can control expiration intervals, syntax restrictions, violation thresholds, and password history. Top Secret also controls the syntax and length of the ACID and allows user access to be restricted to specific terminals, facilities or to a particular time of day or day of the week. ACIDs are not only user IDs they can also be zones, divisions, departments, groups, and profiles. This can make auditing Top Secret confusing. The zone, division and department ACIDs are the foundation for the hierarchical Top Secret setup. The groups, profiles and users are the foundation for the functional setup. Understanding this is critical as it is the underlying structure of Top Secret.

Zone ACID – the highest level within Top Secret. It allows the organization to be split into several subsections. All other ACIDs and resources are defined to a zone.
Division ACID – allows definition of subsections within each zone. Departments, profiles, groups, and users are defined to each division.

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

Department ACID – allows for logical separation of users based on job functions (i.e. Accounts Payable, Programming, Finance, etc.). Users and groups are defined to their respective departments.
Group ACID – allows grouping of users that share similar access requirements. Groups and profiles are very similar.
Profile ACID – allows grouping of common resource access requirements. Then users can be defined to profiles rather than creating separate access permissions for every individual user ACID.
User ACID – designates a specific user and must be associated with a single department.

With all of these layers it can become a daunting task to perform security administration. Top Secret addresses this by having multiple layers of security administrator functions. This helps facilitate layered security as well as separation of duties for Security Administration. The Security Administrators can be restricted to only allow access to certain zones, divisions, and departments. This feature is particularly nice in larger organizations to help control the access privileges granted to the security administration staff. To accommodate the segregation of duties for Security Administrators, there are several types of security administration ID's. There are six types of security administrator ID's:

MSCA (Master Security Control ACID) – there is only one MSCA and it is established at installation. This ID has unlimited administration authority and is usually given to the Security Officer.
SCA (Central Security Control ACID) – has unlimited scope and is not associated with a specific division or department. There should only be a select few SCA's and mostly to function as a backup for the MSCA.
LSCA (Limited Central Security Control ACID) – similar to and SCA but the authority can be limited to certain zones.
ZCA (Zone Control ACID) – is limited to a specific zone but can control the divisions, departments, profiles and users within that zone.
VCA (Divisional Control ACID) – is limited to a specific division within a zone but can control the departments, profiles and users within that division.
DCA (Departmental Control ACID) – is limited to a specific department and can control profiles and users within that department.

Top Secret has four MODES that it can operate under: **DORMANT**, **WARN**, **FAIL**, and **IMPL**. DORMANT mode means that Top Secret is installed but is NOT validating any rules that have been defined. WARN mode means that Top Secret is functioning but it will only present a warning when a violation occurs but will still allow the event to happen. FAIL mode is when Top Secret will not allow violations to occur. IMPL means Top Secret is active and will fail for violations but users not defined to Top Secret can still function but can't access protected resources. So it is critical to understand these MODES because a company can have excellent security in place but if Top Secret is not in FAIL mode then there is a false sense of protection.

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

Top Secret has several other key areas that are important to know if you are a Security Administrator or Auditor.
ALL record – this lists resources that are globally accessible to all mainframe users.
AUDIT record – stores the resources that are to be audited.
Facility Matrix Table – stores all the facilities (TSO, ROSCOE, etc.) defined to Top Secret.
Started Task Table (STC) – stores all the started task procedures and the associated ACIDs.
Resource Descriptor Table (RDT) – stores the predefined resource classes. The RDT is also where you can specify default protection rules for all resources.

Top Secret allows tracking of security violations and many other activities. Events can be sent directly to SMF, to the Top Secret Audit/Tracking File, or both. There are advantages using the Top Secret file. It reduces overhead to SMF, can't be suppressed like SMF, and can be viewed immediately without waiting for SMF to generate the reports. Top Secret has several batch programs that help monitor security. **TSSAUDIT** monitors changes to the Top Secret Security file and other sensitive areas. **TSSUTIL** allows customized reporting based on various criteria and **TSSTRACK** can be used for real-time monitoring of security events.

This is far from an all-inclusive overview of Top Secret. However, those are the primary areas that a Security Administrator or Auditor should know before evaluating a Top Secret implementation. Next we will walk through some steps to evaluate specific controls within Top Secret.

Assessing and Auditing Top Secret

Auditing Top Secret security is relatively easy if you know what you are looking for and how the software works. If you don't at least understand the basic layout and structure of Top Secret (as described above) then it will be extremely difficult to perform an effective review. This section will provide an overview of the major Top Secret reports and commands required to audit Top Secret. It will also walk through several steps showing how to use these reports and key areas to look for.

The first step is to ensure Top Secret is properly installed at Initial Program Load (IPL). The following steps apply to an MVS environment using Top Secret.

a. Review the IEASYSxx parameter in SYS1.PARMLIB to ensure that the operator cannot override the startup parameters.
b. Review COMMNDxx in SYS1.PARMLIB to ensure that Top Secret is initialized immediately following initialization of JES.
c. Review the SYSLOG to ensure the verification of sequence of IPL events.
d. Determine whether the TSS started task is password protected.
e. Identify the library from which the TSS started task is being run by reviewing the JES2 proc in SYS1.PROCLIB for a concatenated TSS PROCLIB (This is sometimes used to provide tighter security over the Top Secret started task),

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

STEPLIB, JOBLIB, and SYS1.PARMLIB(LNKLST). Unless the PROCLIB is concatenated in the JES2 proc, MVS will search STEPLIB, then JOBLIB, and then the libraries listed in LNKLST (in the order listed).

Once this has been verified the next step should be to either request or obtain some of the standard Top Secret security reports. Obtaining these reports at the start of the audit will allow for greater efficiency throughout the review. This lists a few key reports to obtain (this is the actual Top Secret command used to run the report) with a brief description of each:

a. TSS MODIFY (STATUS) – this helps ensure that the appropriate facilities have been defined to Top Secret.
b. TSS LIST(ALL) DATA (ALL) – this lists everything defined within Top Secret and could be a very large report.
c. TSSAUDIT PRIVILEGES – this report lists all user ID's (ACID's) with special bypass privileges.
d. TSS LIST(STC) DATA(ALL) – this report lists all started tasks defined to Top Secret and the security for each.
e. TSS LIST(AUDIT) DATA(ALL) – lists all resources and ACIDs that are currently being audited.
f. TSS WHOHAS DSN (TSS) and (SYS) and (PROD.*) – displays who has access to the Top Secret utilities, System libraries and Production datasets.
g. TSS WHOHAS VOL(*ALL*(G)) – shows who has access to all volumes defined to Top Secret.
h. TSS WHOOWNS DSN(**) – displays the owners of all datasets defined to Top Secret.
i. TSS WHOHAS MODE(DORMANT) and (WARN) and (IMPLEMENT) – lists the resources and ACIDS that are not in FAIL mode. Fail mode means if someone attempts to access a resource where they don't have access then they will be denied access.
j. TSS LIST(ACIDs) TYPE(SCA) and (VCA) and (DCA) DATA(ALL) – lists all ACIDs with Administrator privileges.
k. TSS LIST(ACIDs) DATA(ADMIN) – lists any users with special Administrator privileges.
l. TSS MODIFY (SYSOUT) and (FAC(ALL)) – look for deviations from the expected control options for all facilities.
m. TSS CHART – this shows all ACIDs and resources defined to Top Secret in the form of an organization chart. This allows an auditor to ensure the Top Secret security database structure has been designed effectively. [3]

There are many other commands and reports necessary for an audit of Top Secret but these basic reports are a good start. The first step is to ensure the Top Secret global parameters are appropriately established. The TSS-O MODIFY command will generate a listing of the installed Top Secret options. The auditor should then follow these steps:

[3] CA-Top Secret User Guide

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

a. Review the Global System MODE to ensure that Top Secret is implemented in FAIL mode to prevent access to resources unless access is specifically granted.
b. Review the AUTH control option to determine the method used by the Top Secret algorithm to grant access to a resource.
c. Review the following parameters in the Top Secret parameter file to ensure they are implemented in a manner that is appropriate.
    i. AUTOERASE - indicates whether or not to erase all residual information on the DASD volume (should be YES).
    ii. BACKUP – YES allows for automatic backup of the Security File (must also have the BACKUP DD statement in the TSS started task procedure).
    iii. BYPASS - allows jobs/users to bypass security and should only be used in an emergency.
    iv. DOWN - determines the security if the system goes down and should FAIL all access attempts.
    v. EXIT(OFF) - deactivates installation exit. If EXIT(ON), review exit coding to ensure that no bypassing of TSS security controls occurs.
    vi. FACILITY - controls facilities and display status.
    vii. HPBPW - allows expired/changed passwords to be used for limited time in batch.
    viii. INACTIVE – specifies how long an ACID with an expired password can be used before it is suspended.
    ix. JES - indicates whether the JES early password verification feature is in effect. If early password verification is not in effect then the user and password are required on the job card.
    x. LOCKTIME – 0 deactivates terminal locking.
    xi. LOG - indicates options for additional SMF and Audit/Tracking File logging. NONE deactivates logging while FAIL always logs violations.
    xii. MSUSPEND – NO allows unlimited attempts to guess the MSCA's (master security account) password.
    xiii. NEWPW - indicates new password rules in effect.
    xiv. NOAUDIT – deactivates facility-wide auditing.
    xv. NPWRTHRESH - sets maximum threshold for new passwords to be verified before complete logon sequence needs restarting.
    xvi. PTHRESH – 0 allows unlimited attempts at guessing user passwords.
    xvii. PWEXP - frequency of forced password changes.
    xviii. PWHIST - number of previous passwords that cannot be used.
    xix. PWVIEW - controls display of passwords by administrators.
    xx. RECOVER - indicates if the system is recording changes to the Recovery File.
    xxi. RPW - restricted password list.
    xxii. SECTRACE - diagnostic security trace.
    xxiii. SHRFILE - security file shared by multiple machines.
    xxiv. SIGN – M allows multiple logons with the same ACID to the specified facility.
    xxv. SUSPEND - allows operators with the CONSOLE attribute to suspend users.

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

xxvi. TAPE - external control of tapes. OFF deactivates built-in tape security.
xxvii. TMPDS – NO indicates that temporary data sets are not protected and can not be audited.
xxviii. VTHRESH - resource violations thresholds should be limited and should Suspend the ACID when the threshold is exceeded. [3]

d. Review the Top Secret resource defaults in the Resource Descriptor Table (RDT).

The next step is to ensure ACIDs and passwords are appropriately restricted. The following is a list of steps to help accomplish this objective.

a. Determine if any ACIDs have password attributes that differ from the defaults reviewed above.
b. Identify any ACIDs that have never been used or have not been used in a long time.
c. Obtain a listing of recently terminated/transferred employees. Verify that these employees' access privileges have been suspended, canceled, or modified to match their new job responsibilities.
d. Review the listing of all users, groups, facilities, and resources that are in DORMANT, IMPL, or WARN mode. Obtain justification for any exceptions.

Once this is complete it is important to ensure special TSS privileges are appropriately assigned and monitored. There are key attributes and authorizations that can be defined to specific ACIDs that grant that user special privileges.

a. Review the Privileges and Attributes Report (TSSAUDIT PRIVILEGES) to determine which users are assigned special privileges.
   i. ADSP – NO means new datasets are unsecured in a non-Alwayscall environment.
   ii. CONSOLE – allows the operator to issue MVS console commands from any workstation and change control options.
   iii. NOVOLCHK - allows access or use of any volume (without logging).
   iv. NODSNCHK - allows access or use of any dataset (without logging).
   v. NORESCHK - allows use of any terminal, program, CICS, or user resource (without logging).
   vi. NOLCFCHK - allows use of any command, program, or transaction (without logging).
   vii. NOSUBCHK - allows jobs to be submitted with any ACID (without logging).
   viii. VOL(x) ACCESS(BLP,UPDATE) - allows update access to the specified volume without verifying access.
   ix. VOL(*ALL*) ACCESS(ALL) - allows ALL access to any volume.
   x. DSN(*****) ACCESS(ALL) - allows ALL access to any dataset. [3]
b. Obtain justification for these authorities.
c. Ensure activity for these ACIDs are logged to SMF or the Top Secret Audit File.

[3] CA-Top Secret User Guide
[3] CA-Top Secret User Guide

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

It is important for the auditor to review access to the security administration IDs and to ensure they are appropriately distributed. The following steps should be followed to review access to security administrator privileges within Top Secret.

a. Generate a list of all security administration IDs and review to ensure that users with administrative authorities are appropriate. The command to generate the list is TSS-O LIST(ACIDS) TYPE(SCA, DCA, etc.).
b. Review the organization of the security administration function to ensure that functions are appropriately segregated (if any de-centralization exists).
c. Review user administration authorities over datasets, programs, volumes, resources, ACIDs, facilities, and special functions.

Next the auditor should review security over started tasks and subsystems.

a. Review controls over started tasks (STCs) to ensure they are appropriately protected.
b. Identify programs defined in the MVS Program Properties Table (PPT). Ensure these programs can't bypass password protection.
c. Use the TSS MODIFY(STATUS) command to ensure the appropriate facilities have been defined in the Facility Matrix Table. [2]

The auditor should ensure the AUDIT function is appropriately used to monitor ACIDs with particularly high risk.

a. Generate a Top Secret Audit report (PRIVILEGES[SHORT]) to determine the current usage of the AUDIT attribute and review to ensure this is appropriate.
b. Review the AUDIT record to identify additional logged instances.

It is critical to ensure access to the Top Secret and other critical datasets and libraries are appropriately restricted.

a. Determine the names of the following Top Secret files and libraries and review access privileges to them:
    i. Loadlib
    ii. Parmlib
    iii. Proclib
    iv. Secfile
    v. Recfile
    vi. Auditxx (2 audit files similar to SMF files)
    vii. Backup
    viii. CPFfile (Command Propagation Facility)
b. To ensure that MVS system libraries are appropriately secured by Top Secret, review access permissions to SYS1.** libraries. A sample of libraries should be reviewed to ensure access permissions are appropriate.
c. Determine other critical production libraries and review access controls for an appropriate sample.

[2] AuditNet

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

While backup and recovery is not necessarily a security control, it is also important to ensure critical Top Secret datasets and libraries are appropriately backed up and rotated off-site. It is particularly important because in the event of a disaster it is critical that Top Secret be restored with the rest of the system. If not this puts an organization at risk. Recovery of Top Secret should be included in every disaster recovery test. At a minimum the Auditor should perform the following steps to ensure Top Secret is backed up.

a. Determine current backup procedures. Ensure that the following files and libraries are being backed up:
   i. Security File
   ii. Recovery file
   iii. Audit file
   iv. Backup file
   v. Top Secret load library
   vi. Top Secret procedure library
   vii. Top Secret parameter library
b. Determine if the Recovery File is active and use the TSSAUDIT utility to determine changes made to the TSS control options during the period under review. Determine whether changes are monitored and independently reviewed.
c. Determine the TSS data set names for all primary and backup data sets. Establish who has ownership of these data sets (TSS WHOOWNS) and whether appropriate. Ensure that primary and backup data sets are located on different volumes. [2]

Those are the specific Top Secret security audit steps. Of course there are several other basic audit steps when evaluating security for any organization. No organization can completely rely on the Top Secret software without fundamental security controls such as security policies, regular review of violation reports, etc. The following section briefly reviews some of those key steps.

Security policies and procedures must be in place to provide effective and consistent control over data security administration.

a. Obtain a copy of the Data Security Administration policies and procedures. Review to determine whether or not they are adequate.
   i. Review procedures for adding/modifying/deleting user access authorities.
   ii. Review procedures for updating employee access upon transfer within the company, and termination.
   iii. Select 20 users and verify authorization of access and ensure that access granted is consistent with access authorized.
b. Review security awareness and education procedures.
c. Review the Data Classification Policy.

[2] AuditNet

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

d. Review the User Classification Policy (i.e. users are defined within a logical structure of profiles, with appropriate owners, and profiles are assigned access).

Ensure appropriate review of Top Secret audit reports is performed to respond to security violations.

a. Document the process for reviewing Top Secret audit reports, including who receives the reports, who reviews the reports, what actions are to be taken, retention of reports, etc.
b. Select a sample of reported incidents and ensure that appropriate review and response was taken by management.

Summary

Top Secret is an extremely powerful tool for securing the mainframe environment. There are many additional features that are not included in this documentation. The goal of this paper was to provide an overview of the Top Secret software and to document an approach to evaluate and audit an organization using Top Secret. These audit steps were originally for an MVS environment but were modified to be more generic. So it is critical to understand that these audit steps should be tailored to fit your specific mainframe environment.

RESOURCES

[1] Abramson, Christopher. "A Return to Legacy Security." July 27, 2001. URL: http://rr.sans.org/main/legacy.php

[2] AuditNet. "Review checklist for CA-Top Secret data security review." URL: http://www.auditnet.org/docs/TOPSECRT.txt

[3] CA-Top Secret User Guide.

[4] Computer Associates "CA-Top Secret for OS/390" white paper.

[5] Computer Associates web-site. "eTrust CA-Top Secret Security for z/OS & OS/390." URL: http://www3.ca.com/Solutions/Product.asp?ID=180

[6] Discussions with Computer Associates support staff.

[7] Encyclopedia of Computer Security. "CA Enhances eBusiness Security Across Mainframe and Distributed Platforms" URL: http://www.itsecurity.com/tecsnews/jun2001/jun26.htm

[8] IBM. "z/OS and OS/390 Security." URL: http://www-1.ibm.com/servers/eserver/zseries/zos/security/

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

[9] IBM. “CA-Top Secret Overview.”
URL: http://www.redbooks.ibm.com/redbooks/SG245677/css/SG245677_49.html

[10] IsecurePrivacy. “OS/390 Security.” URL:
http://www.isecureprivacy.com/whitepapers/iSP%20OS-390%20Security.pdf

[11] Korzeniowski, Paul. “Ironclad Security.” Information Security. August 2000. URL:
http://www.infosecuritymag.com/articles/august00/columns6.shtml

[12] RSA Security. “RSA Security Announces Support for IBM's OS/390 Mainframe Environment.”
URL: http://www.rsasecurity.com/news/pr/011113.html

© SANS Institute 2002, Author retains full rights.

Last Updated: September 1st, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced