GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Security Evaluation and Management for the SAP R/3 Environment

GSEC Certification Practical
Option 2 – Submitted 3/16/2004
Eric Goodman

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Table Of Contents:

INTRODUCTION 3

THE SAP SECURITY TASK: 3

THE SIX (6) FUNDAMENTALS OF SECURING AN SAP ENVIRONMENT. 4

1. THINK LIKE A CRIMINAL 4

2. UNDERSTAND YOUR SAP R/3 ENVIRONMENT 4

3. REVIEW OR DEFINE YOUR SAP SECURITY POLICIES AND PROCEDURES 6

4. USE A LAYERED APPROACH TO SAP SECURITY 7

5. DO NOT FORGET PHYSICAL SECURITY 10

6. DEFINE METHODS FOR MAINTAINING A SECURE ENVIRONMENT 11

CONCLUSION 11

REFERENCES: 13

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Introduction

Many myths about SAP Security start with the concept that SAP is too large for any small security team to understand and maintain, or that SAP is a monster that cannot be tamed without hiring SAP experienced consultants whose cost range from the hundreds of thousands to well into the millions of dollars. This belief is far from true. It is true that an ERP package can overwhelm even the largest team with time and expansion; however, evaluating the current state of an SAP environment and managing the security of the system can be conducted efficiently and with little effort. Often, security management is compromised due to lack of focus. This paper will help management focus on the six (6) fundamental principles that solidify the basic security of an SAP environment.

1. Think Like a Criminal.
2. Understand your Environment.
3. Define your Policies and Procedures.
4. Use a Layered Approach for IT Security.
5. Do not forget Physical Security.
6. Define Methods for Maintaining a Secure Environment.

Based on experiences and observations that I had while being tasked to evaluate the current security in an SAP environment I developed a straightforward approach. The emphasis of this paper is SAP R/3; however, I have found that the technique can be applied to other SAP environments and other systems in the landscape.

The SAP Security Task:

Whether during an SAP implementation, an SAP audit by the External Financial Auditor, or an annual review of internal controls from inside the company by the Internal Audit Function, the development of security in and around SAP is tasked to the chosen few who admit to understanding the word “security”.

Realizing that you are the sole manger in a room of many highly educated information technology personnel to state this fact, ultimately means that you have added a seemingly daunting task to your already overwhelming list of yearly projects and a measurement on your yearly goals and objectives. Now, not only are you responsible for evaluating the technical aspects of security, but you also have to explain it in terms of cost, return on investment (ROI), and any business impacts.

Do not worry if you find yourself in a similar situation when tasked by your superior to analyze the security and internal controls of your SAP infrastructure. While in this situation myself, I structured a simple method for evaluating and eventually securing an SAP environment. It all begins with what I call The Six Fundamentals of Securing an SAP Environment. Once you have the simple principals down you can apply them to each segment of your infrastructure and internal to them.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The Six (6) Fundamentals of Securing an SAP Environment.

1. Think Like a Criminal

What do I mean by "Think like a Criminal"? The first thing a manager should do is follow the same steps as any hacker, cracker, or script kiddy that will eventually try to compromise your SAP security.

Information security attacks are usually planned and orchestrated by following four basic steps: Profiling, Architecting, Attacking/Testing, and Implementing. I will define these terms relevant to the SAP environment in the following paragraphs.

- Profiling or Architecting the network and/or environment: Criminals do this by trying to "perform a footprint analysis" to "enumerate information" about the systems. This allows them to know your hardware and software versions. Script Kiddies will try to exploit publicly distributed vulnerabilities of operating systems, databases, applications and network appliances with tools they haven't developed but downloaded from the Internet. (Schultze p.13)

- Attacking and testing: Criminals try to obtain access through "user manipulation", while trying to "escalate privileges, gather additional passwords and secrets, and install backdoors or key recorders". They attack and test security whenever and wherever possible. (Schultze p.13)

- Implement the exploits or "leverage the compromised system": Criminals try to disrupt backups, financial data, or manufacturing data. Review and test critical data and recovery steps to verify normal operation. A true criminal will disrupt passively rather then actively. Slowly changing financial data to produce incorrect reporting, or disrupting backup routines and files to prevent a clean restoration are far more devastating for a company over time. (Schultze p.13)

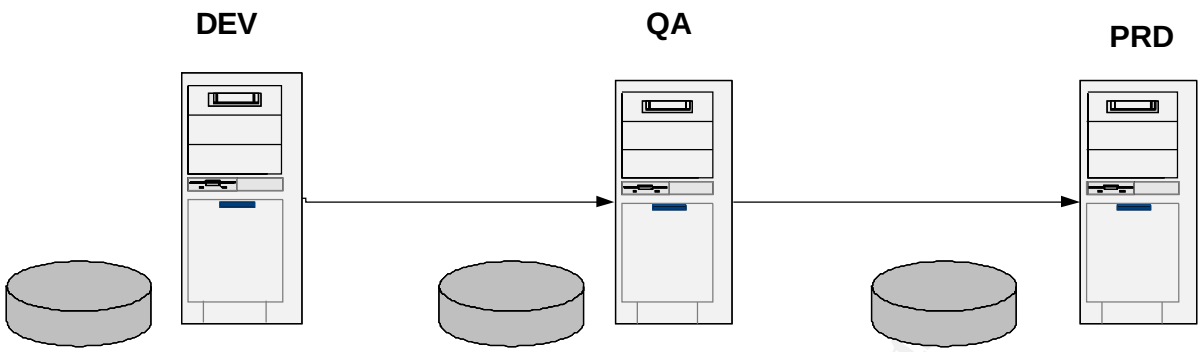
By following the same principals that a criminal would use you can begin to understand where vulnerabilities exist in your environment.

2. Understand Your SAP R/3 Environment

To understand your SAP environment it is crucial to start by learning the basic structure of SAP. The SAP R/3 (Client server) differs from the SAP R/2 (Mainframe) system configuration. To better understand the task exemplified here, I will briefly explain the SAP R/3 three-tier landscape.

The SAP three-tier landscape is basically a set of servers differentiated as Development, Quality Assurance (Consolidation), and Production. These can be on separate systems or have multiple instances installed on one server. The preferred install is on separate servers. (Figure 1)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



Once you have the basic concept of the landscape, start developing a spreadsheet of the systems that send data to each SAP server or receive data from each SAP server. A simple example is shown below.

SAP Server and data transfer:										
	Sales System		**Mfg System**		**HR System**		**Web Server 1**		**Web Server 2**	
	Data to	Data from	Data to	Data from	Data to	Data from	Data to	Data from	Data to	Data from
SAPDEV	N	Y	Y	Y	Y	N	Y	N	Y	N
SAPQA	N	Y	Y	Y	Y	N	Y	N	Y	N
SAPPRD	Y	Y	Y	Y	Y	N	Y	N	Y	N

Even a simple table will allow you to identify what other systems are connected to each SAP server. This then allows you to develop the listing of what operating systems are on each system, if a database is on these systems or not, what applications are installed on each system connected to SAP, who the system administrator(s) and application administrator(s) are on each system, and then follow-up with these administrators on how the systems connect to SAP.

Many network tools are available to automatically perform a passive scan on the systems in the network to discover all of these facts. I was fortunate enough to work with the network architecture team in order to list every fact I needed for each server connected to my SAP environment. All that was required then was to verify the scan results and update my spreadsheet of systems and security settings to include software versions and the connectivity stream to or from SAP.

After completing a review of the landscape of the SAP environment, you can start to identify the areas of vulnerability and work your way toward the Layered Approach to SAP Security. Prior to this point, you must first review any of the current security policies that are in place. Policies and Procedures explain how, when, who, and where these security settings or mitigating controls apply.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

3. Review or Define your SAP Security Policies and Procedures

The next step in my process allows for a quick reference of the current security "supposedly" applied in each system within your corporation. If a policy exists for a system, it becomes a benchmark to compare the system to when you actually log into it and review the security setup. The security setting in the policy may or may not be true for the systems it is written. What you should find are at least a basic set of three security policies or many security policies that should role up into these three categories: the IT Security policy, the Development Standards policy, and the System(s) Maintenance policy.

The IT Security Policy may be a detailed security policy that applies standards for each and every system and application within the corporation. Or, you may find the IT Security policy to be a very lengthy, confusing, and general definition of access, authentication, and usage policies in the employee manual of your company. Either way, you will locate simple security settings to build a security tracking spreadsheet that can be continuously used for each system. A security database can be more comprehensive, but for consistency and complexity I'll continue to speak concerning a security spreadsheet. A very simple example is shown below.

System	Standard User ID?	Time to User Lock?	Time to Session End?
SAPDEV	N	6	3
SAPQA	N	6	3
SAPPRD	Y	6	3
Sales	Y	6	3
Manufacturing	Y	6	3
HR	N	6	3

The Development Policy helps add to your spreadsheet by defining items such as interfaces, database connections, programming languages used (such as XML or JAVA), and any custom development for each system. Although the policy itself may not state these exactly they will focus you on items to look for within your system(s). These should be added to your security tracking spreadsheet as points of potential vulnerabilities. An updated example is shown below.

System	Standard User ID?	Time to User Lock?	Time to Session End?	Interfaces
SAPDEV	N	6	3	NFS to SAPPRD
SAPQA	N	6	3	NA
SAPPRD	Y	6	3	NFS to SAPDEV, DB connection to SALES
Sales	Y	6	3	DB connection to SAPPRD
Manufacturing	Y	6	3	XML to SAPPRD
HR	N	6	3	3

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The System Management Policy will cover items such as database, spool, fax, tablespace, and user management settings and procedures. There should also be a set of steps for backup and recovery that can help you identify when they happen, where they happen, and to what media they reside.

If standards and policies are not formally documented and version controlled then it is like they never existed. I say this because tracking or identifying the areas of risk and control of a system will be a moving target depending on which IT person you ask. I was fortunate enough to have many documented policies and procedures that allowed me to build a spreadsheet with relationships for application to security settings that could be queried against the other systems to check for standardization of settings, mitigating controls, and whether the security fix is even applicable to a particular server. For example, you cannot apply a database security rule on a server that does not have a database on it. That is why after understanding your landscape and reviewing your current policies, you need to develop a matrix of vulnerabilities based on layers of your SAP environment. Update your security tracking spreadsheet with items found within the policies.

4. Use a Layered Approach to SAP Security

The simple fact about security is that many areas and techniques specific to each area for securing the SAP environment exist. Without listing each of the systems identified in your review, assigning each current security or control to each, and then identifying high level layers that apply to each, you will either miss holes that criminals can exploit or an entire avenue of information flow that can be compromised.

Here is a simple table to get you started in setting up areas of focus to develop a risk matrix for the areas of your SAP environment. Obviously it is not all-inclusive, but it should spark ideas of your own on how to layer your approach to securing SAP. (Morris p.13)

Layer	Environment Components	Security Aspects	Security Responsibilities
1. **Presentation**	GUI, browser, PC/Desktop	Access Control, Authentication, virus scanners, encryption	▪ IT Security ▪ SAP Security ▪ End-user policies
2. **Communication**	SAProuter, network, SNC, SSL, HTTPS, SSH	Access control, Authentication, Packet filtering, Encryption	▪ IT Security ▪ SAP Security ▪ Vendor Security
3. **Web link**	ITS, WAS, BC, XI	Access Control, Encryption, Certificates, Single sign-on	▪ IT Security ▪ SAP Security
4. **Application**	Application Modules, Work processes, interfaces with external systems	SAP user access, password rules, authorizations, transaction controls, data access controls	▪ SAP Security, ▪ End-user policies ▪ Business Owners ▪ SAP Functional Team

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

			▪ Internal Audit
5. **Database**	Oracle, SQL Server	Access to tables, backup consistency	▪ IT Security ▪ SAP Security
6. **Operating System**	UNIX WIN2000	Access to SAP files, OS services	▪ IT Security ▪ SAP Security

4.1. Securing the Presentation layer is started by restricting user access, and limited server authentication to the SAP graphical user interface (SAPGUI). Although the transmission of the SAPGUI packets cannot be secured directly, many environments use a CITRIX application to lock access to the SAPGUI software that also limits access to sniffing the packets on a local desktop. Also, limiting access to the SAPGUI saplogon.ini file can help segregate access for persons to certain SAP systems by not listing them. Begin at a high level and determine the front-end application is used to access the SAP system, where it is located in the network, and how can it be secured.

4.2. Securing the Communication Layer (Network) is concerned with access to information transmitted within your SAP environment. It should cover the areas of communication used between servers connected to your SAP systems. These may include the wide area network, the local area network, a virtual area network or even a storage area network. The system settings and security controls can be the most technical in nature for these areas. Enlisting the help of your network administrators in the beginning stages of the six fundamentals will help greatly when reviewing and implementing these controls. Many tools and utilities exist for network security but are usually focused on certain areas of the WAN, LAN, or SAN and are easily accessed by entering standard searches for LAN security or Network Security on www.google.com or www.yahoo.com. You and your team will need to use many tools for areas of your network. Which utility is best for you is dependent on your network structure; hence, the need for an understanding and mapping of the network layer. (Quinn p.13)

4.3. The Web Link layer secures interfaces and language translators for external systems and databases. SAP has two standard connectors: Business Connector (BC) and Exchange Interface (XI). Both may be used for communication between systems in networks, to and from a DMZ, and are possible points of vulnerability. SAP also has to standard web publishers: Internet Transaction Server (ITS) and Web Application Server (WAS). Understanding the connectors and publishers and increase your understanding of the SAP environment and update your security tracking spreadsheet.

4.4. Securing the SAP Application is where you may find a lack of information. SAP distributes the “SAP Security Guide 3.0” for the basic areas of security of the environment, and sells books such as the so called “Authorization Made Easy” guides for user access control, but these are very limited in description and lacking in a concise plan for designing, developing, implementing, and reviewing SAP security.

Data Classification should be the first step in defining security for SAP. Classifying data in to categories of Highly restricted, Confidential, Internal, and Public data access will

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

help you segregate duties with in SAP roles and other access points. Define a corporate data classification to categorize the critical master data or table access, configuration, custom programming, and change processes within SAP. Then, build a matrix of business data owners mapped to these elements for approval and independent review.

Reviewing segregation of duties within roles is impossible if you cannot establish a consistent list of organizational restrictions based on the data classification that can be applied across roles. The organizational restrictions can be units such as plant (WERKS), company code (BUKRS), and cost center (KOSTL). Once this list is complete, understanding the SAP authorization security design is the next step. To review this, simply match the data within the SAP role and user tables of AGR_DEFINE, AGR_PROF, AGR_TCODES, AGR_1251, AGR_1252, AGR_USERS, UST12, USR02, and UST04 to the list of restrictors to see if they are in conflict. Using MS Access and mapping the appropriate fields can give a complete company listing of security within SAP roles. When you build the database do the following:

- Link the PARENT_AGR field in the AGR_DEFINE table to the AGR_NAME in the AGR_TCODES tables then.
- Map AGR_NAME in the AGR_PROF table to the AGR_NAME field in the AGR_DEFINE table.
- Map the PROFILE field in the AGR_PROF table to the AUTH field in the UST12 table after deleting the right two characters in the AUTH field.
- Then map AGR_NAME field in the AGR_USERS table to AGR_NAME in AGR_DEFINE table.

This will give you the listing of *Users to Roles to Transactions to Authorizations* in SAP. Build a table with this query and name it representative of the contents (tblUserAccess). So now you have the organizational restriction base, and a listing from SAP of the assignment of all fields. Now, setup a query in MS Access to find the relationships of the organizational restrictions in the user roles and find the duplicates. Since SAP authorization security is based on “or” logic the overlaps or multiple value assignments to users for organizational restrictions are the areas of concern that can open security for users in SAP. An example: If you want to restrict by PLANT and you only want to give user X access to PLANT ABCD and you discover in this MS Access search that user X has a value for PLANT ABCD in one role and a PLANT value of ABDC in another assigned to X, then X has access to BOTH plants and is a security issue. (Morris p.13)

After you review access vulnerabilities you need to review segregation of duties (SOD). Using the same MS Access tables you can identify which users have access to transactions that are in conflict. An example is that a user should not be able to order, approve, pay, and receive. Each of these processes has an SAP transaction or transactions for them. Working with the Internal Audit function, the External Auditors, and files that you can find freely on the web for SOD conflicts you can build a listing of transactions that should not be assigned to the same user (tblConflicts). Setup a query

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

in MS Access to find these conflicts with in the table tblUserAccess above for *Users to Transactions* and resolve the conflicts with the business owners of the roles.

The next step in the SOD review is what most persons miss. To do a review at the security object field level rather then just at the transaction level. Using the tblUserAccess above you have the listing of users to transactions to objects, but require understanding of the *object field* conflicts. If you did a good job at defining the organizational restriction base then you have the listing of object fields to compare to the SAP table USOBT_C. This table lists the relationship of security objects to SAP transactions. You now map the tblConflicts and the tblUserAccess tables to the USOBT_C for overlap or conflicts. Not a simple task but very possible and won't cost you a hundred thousand dollars initial with twenty thousand dollar a year maintenance fees for an external software tool. But if you feel it's easier to buy the tool there are several good ones on the market now that Sarbanes-Oxley was passed and companies are forced to do these reviews every ninety days. Examples would be VRAT by VirsaSystems at www.virsasystems.com or SECURINFO for SAP at http://www.securinfo.com/securinfo_for_sap.asp. (SAP p.13)

4.5. When Reviewing and securing the database apply the same areas of concern: data classification, access, and authentication. "Database security is concerned with a level of granularity, such as table, row, or cell. In database systems objects can be complex logical structures, a number of which might map to the same physical data objects. In database views users have access to a specific schema object and the specific types of actions allowed for each user on the object (a user can issue SELECT and INSERT statements but not DELETE statements on the EMPLOYEE table). Each database user has access to objects in the corresponding schema. Additionally a database can be restricted by roles, a job or access privileges, profiles (like roles except they deal with resources like CPU_PER_SESSION." By default, SAP mounts on the database and limits access to these objects for database users except the ora<SID> and $OPS users. As an example access privileges of other users within the database should not equal these users or the DBA and SYS users for Oracle. (Swenson p.13)

4.6. Securing the Operating system is the next level of complexity and depth of controls. Mainly identifying the data classification, user or system access rights, system services and processes required for proper performance, and process for authentication can cover many of the areas and help you identify areas that have tight controls or need to be improved.

The Layered Approach can be expanded as your knowledge of the landscape, systems, components, and data increases. After a few months of listing these elements in my security spreadsheet it has grown to be quite extensive. This task was by far the most exhausting, involved the collaboration of many teams, and was very time consuming. But I was not finished yet.

5. Do not forget Physical Security

Apply the set of controls of data classification, access, and location to the data center, the corporate office, and the personal computers. This can help prevent costly

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

downtime of critical systems that can be caused by something as simple as the cleaning person turning off a PC that was running a program would run overnight, to someone driving a car into the wall of the building because they know which side the data center is located.

The building should have security procedures that limit access for non-employee to areas of the company to restrict knowledge of the location of the data center and the network cabling and telephone closets.

In the data center, systems should be categorized into critical and non-critical application based on business input for data and process that keep the company generating revenues. The critical systems have more limited access then the non-critical; they will have redundant power, fire suppression, and possibly redundant servers in other locations in case of disasters.

6. Define Methods for Maintaining a Secure Environment

Maintaining a secure environment is as important as initially securing it. If you constantly are fixing the same security opportunities because you fail to maintain them you will never achieve a higher level of security.

A good plan is to start with defining roles and responsibilities for security administration. If you followed my steps you will have already defined the administrators of each system and application. All you need is to distinguish between the security designers and developers, the security administrators, the security reviewers, and the security approvers. Then, assign tasks to each person for maintaining the security settings of certain components. These persons should notify the team when changes occur that can compromise any area of the SAP environment listed in your security setting spreadsheet, or a change that may require you to add a potential vulnerability and solution to it. This separation of duties will keep an objective level of control, monitoring and review when implementing and approving all external system and internal system changes.

Change management of the network, servers, system patches and upgrades, programs, users, and access/role changes should be measured against the security listing that you developed in the security spreadsheet of controls for each system. This ensures that a consistent security posture is maintained in the SAP environment.

Conclusion

Following these six fundamentals enabled me to clearly outline the state of the SAP environment based on criteria: data classification, access, and authentication. It further allowed me to periodically review, and report to management on the state of the environment. By having a detailed listing of data and systems mapped to vulnerabilities and controls I was able to develop a matrix of cost analysis based on availability and replacement of these elements. Reporting to management the potential cost of losing, restoring, or replacing any element allows them to measure risk and assign budgets.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

While completing my task many areas had good controls for user and system authentication: the presentation, operating system, database, and application layers. It unveiled areas where further evaluation was needed due to lack of current information or my control understanding: communication, web link.

Armed with the knowledge from the SANS security essentials class I have a greater understanding of the potential areas of risk and have started a procedure that will only get more detailed and complex with the growing SAP landscape. I have mitigated some risk but have opened my eyes to others with my understanding the areas of security.

The environment is ever changing with new applications requirements, systems upgrades, and requests for external and internal connections to SAP for data transfer leads to an ever-present state of vulnerability. The risk of attack and penetration of the environment from external and internal persons has been limited but not eliminated. Remember the basic formula R + C = r where R = big risk, C= big controls and r = little risk. You can never get rid of risk.

© SANS Institute 2004, Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

References:

1. Schultze, Eric "Thinking like a hacker"
   URL: http://security.shavlik.com/Whitepapers/Thinking%20like%20a%20hacker.doc.pdf
   March 7 2002.

2. SAP AG: http://www.sap.com

3. SANS Institute: http://www.sans.org/

4. Quinn, Steven "UNIX Host and Network Security Tools" May 16 1996.
   URL: http://csrc.nist.gov/tools/tools.htm#audit

5. McLean, Ian Windows 2000 Security Scottsdale: The Coriolis Group, 2000.

6. Theriault, Marlene Oracle Security Handbook Berkeley: The McGraw-Hill Companies, 2001.

7. Brenton, Chris Mastering Network Security Alameda: SYBEX, Inc. 1999.

8. Swenson, Scottie Introduction to Oracle Database Security
   URL: http://www.seattle-sage.org/1999/03/199905_ora_sec_talk.pdf

9. Morris, Gary
   URL: http://www.sapbasis.org/securitydocs;
   URL: http://users.ev1.net/~gmorris/securitydocs/sapsecurityguidever3.pdf
   URL: http://sapbasis.msspro.com/AMEZ_46_all.pdf

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Last Updated: October 24th, 2017

Upcoming Training

San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Cyber Defense Initiative 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Dec 14, 2017 - Dec 19, 2017	vLive
Community SANS Nashville SEC401^	Nashville, TN	Jan 08, 2018 - Jan 13, 2018	Community SANS
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Community SANS Hawaii SEC401	Honolulu, HI	Jan 08, 2018 - Jan 13, 2018	Community SANS
Mentor Session - SEC401	Memphis, TN	Jan 09, 2018 - Mar 13, 2018	Mentor
Northern VA Winter - Reston 2018	Reston, VA	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, Netherlands	Jan 15, 2018 - Jan 20, 2018	Live Event
Mentor Session - SEC401	Minneapolis, MN	Jan 16, 2018 - Feb 27, 2018	Mentor
Las Vegas 2018 - SEC401: Security Essentials Bootcamp Style	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	vLive
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
SANS Miami 2018	Miami, FL	Jan 29, 2018 - Feb 03, 2018	Live Event