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.

Exploring Identity Management

Identity management is the concept of centralizing the control of resource provisioning and system access. Leveraging human resources software, corporate directories, and centralized servers, it provides large enterprises with the means to initiate workflow for automatically allocating and de-allocating physical and computing resources to users. Poor or no identity management can open many security holes and this class of software, combined with effective policy, promises to counter these vulnerabilities. Some software...

Copyright SANS Institute
Author Retains Full Rights

AD

Exploring Identity Management
SANS Security Essentials
GSEC Practical (ver. 1.4b option 1)
Paul Pannell
4 December 2002

Abstract

Identity management is the concept of centralizing the control of resource provisioning and system access. Leveraging human resources software, corporate directories, and centralized servers, it provides large enterprises with the means to initiate workflow for automatically allocating and de-allocating physical and computing resources to users. Poor or no identity management can open many security holes and this class of software, combined with effective policy, promises to counter these vulnerabilities.

Some software solutions cover all areas of identity management while others only address a specific concern. This document aims to provide a guide to the various ways it can be implemented and show how identity management can lead to improved security.

Introduction

In the corporate computing environment of today information security is a high priority. This is for good reason. According to a CSI/FBI study, an identified breach of corporate computer resources costs an average of $943,000. And this figure only accounts for directly accountable costs related to the incident [1]. There are many other losses involved that are much harder to account for. Companies also suffer from lost productivity and downtime, lost revenue due to customers not having access to sales material, and a decline in consumer confidence in the organization. Corporations must strive to mitigate the costs associated with lapses in information security and many are turning to identity management to accomplish this task.

The goal of identity management is to provide large entities with the ability to use a centralized database of user identities to streamline workflow and automate tasks dealing with user authentication, access rights, policy enforcement, and provisioning of both physical and electronic resources. A white paper published by PricewaterhouseCoopers and Gartner stated that "[Identity management] is a convergence of technologies and business process [2]." This implies there is no one product that will address all points of pain for a company. There exists a wide range of offerings that solve different aspects of the identity management problem, but even the products that attempt to encompass all the issues involved will be ineffective with out properly defined policies. Moreover, identity

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

management must be incorporated into the company culture enterprise wide in order to enjoy the full benefits the concept can offer.

There is a very real return on investment associated with proper identity management. Aside from a reduction in security related costs, the automation of tasks decreases the expenditures necessary for system administrators. In some cases, allowing users to perform self-maintenance of their resources can also minimize the cost of help desk personnel.

In some industries identity management can be a necessary component in an enterprise strategy due to emerging laws and regulations. In the United States, the Health Insurance Portability and Accountability Act and the Gramm-Leach-Bliley are inciting changes in the health care and financial services industries, respectively. These acts place requirements on the level of information security that will be hard to meet in a cost effective manner with out utilizing identity management.

Description of Solutions

All identity management solutions evolved from the concept of having a single, centralized repository of user information that, when updated, can initiate company wide all desired actions related to the change. Some systems use a proprietary centralized server, but the more robust systems work by utilizing 'hooks' or 'connectors' that tie-in to preexisting corporate human resource software such as PeopleSoft's HRMS, SAP's HCM, Active Directory, and even simple LDAP directories. A change in the human resource software is recognized by the identity management software and then, depending on rules or predefined user roles, the software connects to all other necessary systems to automatically handle things such as smart card maintenance, account creation, password setup, or access rights modification. Task that have physical components are addressed as well. For example, a change could initiate an email to a building proctor for the issuance of a door access card.

All identity management products are designed to manage resources for the full lifecycle of an employee. This means that resource allocation is only the first step. All subsequent changes in the status of the employee will also be managed by the system. These systems make the enforcement of corporate policy much more simple because the actions are carried out based on set rules and there is little opportunity for human indiscretion. The ability of identity management systems to bridge many different platforms is why they are so powerful and offer much in the way of centralization and simplification.

While some products focus on a single aspect of identity management others span all of the concepts involved. The following products have been divided into three categories: secure authentication, authentication synchronization, and full

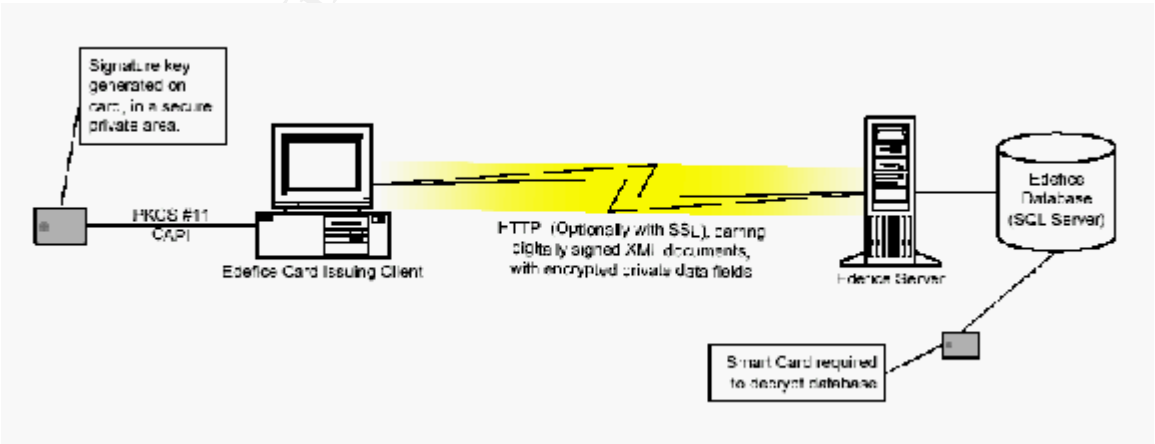
© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

provisioning. This is certainly not an exhaustive list of solutions available, but is intended give the reader an overview of the types of identity management solutions available by illustrating one of the software solutions for each type.

Secure Authentication

Smart cards are the most readily available form of secure authentication today. A smart card is a plastic card the size of a credit card with an embedded integrated circuit. The exact specifications of the cards and the devices used to read the cards will vary by manufacture, but most cards contain an EEPROM memory and some also have a microprocessor that can be programmed [3]. In order to prevent the card itself from being the weakest link in the security chain, the cards are designed to be very secure. Physically, smart cards are tamper resistant to prevent access to the information they contain by probing techniques and reverse engineering. Electronically, the cards are programmed with logic that enforces rules for access to the data by the card reading device.

The use of a smart card is inherently more secure than password only authentication because it requires a two point authentication. It requires something you have (the card itself), and something you know (the password associated with the identity on the card). The benefits of using smart cards do not end with account logon. Most implementations also allow the cards to also be used to gain physical access to restricted areas and the cards can function as a corporate badge. Intercede, a UK company offers Edefice as one such solution. Their Edefice Security Manager acts as the central server to store user digital identity information in a SQL database. The system is fully accessible through a XML based web interface. Some of the security highlights of the system are the ability to connect to the web services using SSL and encryption of the SQL database that requires the use of a card to decrypt. Card account provisioning can be achieved automatically through the use of meta-directories and a LDAP directory import mechanism.



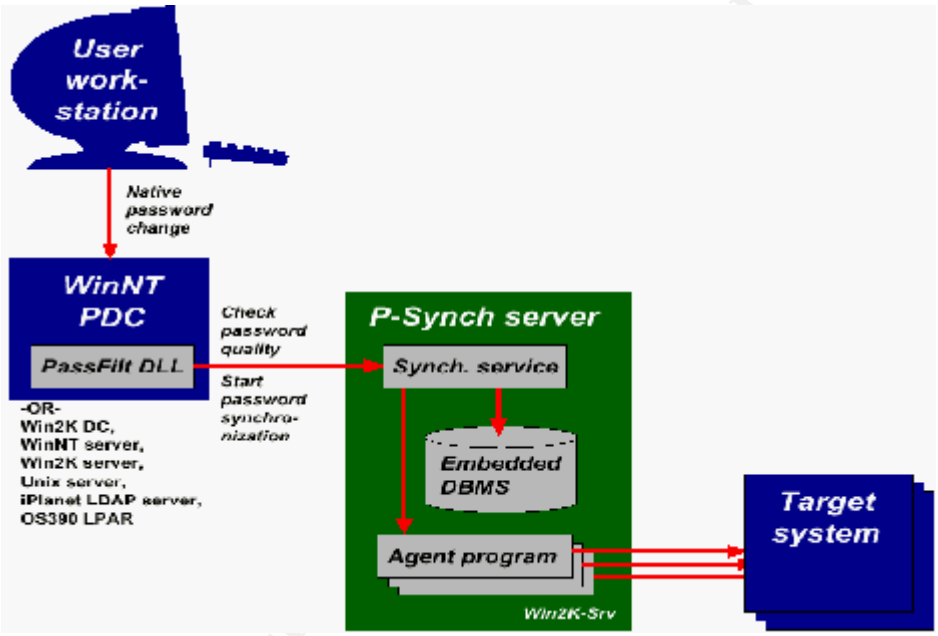
[Figure 1]

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Full lifecycle management of the solution provides for card issuance, modification of the contents, and cancellation. Provisioning of temporary cards is also supported [4].

Authentication Synchronization

Authentication synchronization systems, also referred to as password synchronization systems, tackle the problem of users having many different passwords for many different accounts. With this kind of identity management software, when a user needs to change a password, it can be done in one place and the change will propagate to all accounts the user has. P-Synch, provided by M-Tech, is one solution of this type.



[Figure 2]

"P-Synch can automatically trigger password synchronization when users change their passwords on LDAP directories, MVS or OS390 mainframes, Windows NT servers and domains, Unix servers or Windows 2000 servers and active directory [5]." In addition to the ability of a user to change their password on one of the above systems, there is also a web interface for initiating the update. Systems such as this are aware of the different password rules on all the platforms they interact with and will require the user's password to be valid on all systems. Also, the password will be checked to ensure it is strong against dictionary and other common attacks.

Much of the buzz about identity management concerns automation of tasks, and P-Synch offers this as well. In the event of a disabled or forgotten password, users have the ability to reset passwords themselves. For security, users must first authenticate themselves with a secure token or by answering a series of predetermined personal questions. As with all components of a security system, intersystem communication must be secure. P-Synch achieves this by using

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

128-bit IDEA for communication between the synchronization server and the various platforms. This encryption scheme is utilizes both a shared secret key and random session keys.

Full Provisioning

Full provisioning software combines the elements of authentication synchronization and secure authentication and provides for the provisioning of user accounts and physical resources. Business Layers, one of the early developers of provisioning software defines this as 'eProvision' and offers a product of the same name. Their software has the ability to provision users with "e-mail and network accounts, databases, groupware, productivity applications, VPNs, firewalls, telephone lines, ASP-based services, PCs, notebooks, cellular phones and more [6]." The process for implementing full provisioning is not as simple as with more single focus products for identity management. eProvision communicates with the existing human resources software in use by a company to create a digital profile for each user. The rules configured for the system are then applied to this profile to create what Business Layers calls an Active Digital Profile (ADPr). The ADPr is what is then used to initiate the necessary workflows for the provisioning of resources. The communication between the eProvision components is secured with 128-bit Secure Socket Layer encryption [6]. An example of the far reach of this provisioning system is its ability to interface with the DeXa.Badge solution from Schlumberger. DeXa.Badge is a secure authentication solution that can be fully provisioned by the eProvision software [7].

Full provisioning products promise to be even more robust in the future. One reason for this is that Business Layers has offered its ADPr as an open specification for the exchange of information between provisioning systems [8]. The standard specifies XML for communication between systems so it is highly customizable and any software developer can incorporate it into their products for easy integration into an existing provisioning system.

The varying levels of service of these identity management solutions make it easier to initially buy into the idea. An organization that does not have the resources or need for a full provisioning system could begin with one of the more specific solutions to take care of their greatest need. Given the way identity management systems are designed to work with disparate systems, it is easy to see that an investment in a smaller system will not be wasted because the system can be incorporated with provisioning systems added in the future. This allows a somewhat ad-hoc approach to implementing identity management solutions.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Security Benefits of Identity Management

Identity management promises to counter the following security vulnerabilities:

Mismanaged permissions and accounts
In organizations where there is no central management of account creation, accounts may be created by many different people and may or may not be properly documented. The biggest security threat in this situation is when a user changes roles or, in the most extreme case, is terminated. According to recent FBI reports, more than 80 percent of today's enterprise security violations are internal [9]. In order to combat this, if an employee receives a promotion or is transferred to another department they should no longer have any permissions not associated with their new role. Obviously, In the case of termination, all the access rights of the employee must be removed in a timely fashion.

Multiple accounts on the same system for a single user is also a security risk and increases time requirements on system administrators. If a user requires the access privileges of a group they are not currently in, they may simply be given a second account. This can lead to duplicate accounts for each function the user must perform. If a user's access rights are to be removed, the administrator may remove one account that is no longer used and assume their task is complete. Other duplicate accounts may remain and leave a point of entry for would-be intruders. Through automatic provisioning of accounts, identity management can automatically add or remove users from groups and avoid duplicate accounts. This will be time saving and help ensure that there will be no unauthorized access to systems.

Human error
When accounts are provisioned and user information is changed manually, there is always the possibility of human error. This may not be likely in a small environment, but in companies with thousands of users and multiple interface points, mistakes will be made. These errors are not only time consuming to repair, but also increase the risk unauthorized access to resources.

Authorized requests
Identity management provides a structured process for requesting resources. This avoids the situation where someone might ask for an account as a personal favor and protects against social engineering. If all requests must be granted at a single entry point (the human resource software or centralized directory) then the administrator of a specific system will not need to create individual accounts and doesn't have the responsibility of making sure that account request are authorized.

Reclamation of physical resources
The benefits of a strict workflow also benefit de-provisioning. If a change in an employees' status dictates that they are no longer authorized to have a physical

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

resource (such as a laptop or PDA) then someone will be explicitly given the task of reclaiming that device and the provisioning system will document their responsibility in order to hold them accountable. There is an obvious cost incentive to this, but there is also an increase in security because valuable information may remain on the device or the device may be able to access other systems within the company.

Authentication

Some software implementations of identity management offer a single sign on ability. This is the concept of having one password that grants access across multiple systems. Against policy or not, if user has many passwords they are likely to write them down. If a user only has one password to remember they are much less likely to keep their password in obvious places around their workstation and thus improve security. Generating passwords in a centralized location also makes it simpler to utilize software that checks passwords and requires the password to conform to strong standards. Passwords themselves are not entirely safe. Passwords transmitted over networks in clear text, or sometimes even when encrypted, could possibly be intercepted. Also, there is no way to be sure an uninformed or careless employee will not share a password. Authentication will be further secured by incorporating smart cards into the identity management scheme. This way, if a user gives out their password or it is otherwise compromised it will not immediately grant outsiders access to secured systems. Cards also allow for non-repudiation. In other words, if personnel must use a smart card to access systems, it is much more difficult for them to deny any actions that were taken while their card was in use.

Policy enforcement

Policies are an integral part of any it security plan but, even the best policies must be religiously enforced to be effective. It is not uncommon for policies to be side stepped as a matter of convenience or when time is short. When implementing an identity management solution, corporate policy is intergraded into the rules the system uses for provisioning. This takes much of the responsibility for conforming to policy off humans. If all requests for resources must be made through the identity management system then policies will be followed by default.

The above situations illustrate how identity management can provide large increases in security for organizations that employ it. Also, the examples show how administrative and support overhead can be minimized in many cases. For both these reasons, it is easy to justify investing in these systems. Furthermore, as employees increase their use of multiple devices and mobile devices become ubiquitous the need for identity management will be amplified.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Case Studies

Widener University in Pennsylvania saw a great opportunity for an Identity management system. Every year, the school has around 2,000 new students that must have accounts provisioned and then, at the end of the school year, resources must be de-allocated for students that are not returning. Widener chose Business Layer's software to reduce the huge amount of time and overhead required to setup new accounts on several different systems and, with the ability to quickly remove accounts at the end of the year, minimized the security risks associated with many unused accounts [10].

Intercede's Edefice was chosen by a "major UK Government department" to handle the problem of secure authentication. The smart card solution provided allows government employees to securely log on to multiple platforms as well as connect securely from remote locations. Changing requirements, such as network resource access and physical building access can be addressed by the full life cycle management system as the needs of the department shift over time [11].

As a large software company, Sybase employees had many different passwords for the systems they used. Management wanted to increase network security and give users the ability to resolve some password related issues themselves. M-Tech software is used to fulfill these requirements and Sybase reports that calls to the help desk have been reduced by more than 85 percent [12].

Creating policy

The information presented on identity management thus far has illustrated many security benefits. However, all of the decisions made by the different software implementations are based on rules defined in the provisioning systems. It is natural for these rules to follow from an enterprise security policy. If the policy itself is faulty, many of the advantages of using identity management software will vanish. This section will address issues that must be considered when determining a security policy so that the full return of identity management systems will be realized.

As with any project, one of the first steps should be the definition of goals. What resources the policy will cover and exactly which parts of the enterprise will be regulated by the policy are questions that should be answered early on. For a security policy, it is probably best to take a two level approach. On the first level, the general regulations of what is and what is not permissible should be addressed with out focusing too much on system specific decisions. This can then be used as a guide for creating a more detailed policy that can be readily integrated into the rule set for a provisioning system. As an example, the first

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

level could define what resources a certain class of employees should be allowed to access. Then the second level would clearly state how (group permissions, access lists, etc.) the policy will be implemented on each system in use by the organization. A policy that is adaptable is desired, but this conflicts with the goal of a clearly detailed policy. You want a policy to be general enough that it does not have to be rewritten every time there is a slight change in how a certain software handles security however, too ambiguous of a policy will allow for wide interpretation and possibly permit practices that are not secure.

If one is available, it is a good idea to use a previous policy as a guide for a new policy. This will ensure that problems encountered in the past are not overlooked and issues that are no longer important can always be removed. For this reason, it is always best to document why decisions were made within a security policy. The developers of the next iteration of the policy can then understand the rationale behind each part of the policy and fully understand if the problem previously addressed remains an issue.

It is important that a policy be developed based on input from all personnel that will be affected by the policy. In most cases, there will exist business needs that conflict with having systems that are as secure as possible. All users need to be given the resources that they require to perform their job function effectively. To accomplish this, the creators of the security policy must identify the owners of systems enterprise wide. Since the identity management system will allocate resources on these systems, the owner of the system should approve the policy regarding the creation of rules governing who will have access to the system and what level of access this will be.

In an identity management system that uses role based provisioning it is important for policy to clearly state what type of users will be placed in each role. A sufficient number of roles must be created so that administrators are not forced to place a user in a role that has greater privileges than what is specifically required.

When using a centralized system like identity management software there is one main point of entry, which must remain secure. This entry point is the directory or human resources software used to initiate the provisioning workflow. The security policy should explicitly define who has the authority to access this system and what functions they may perform. Even if the provisioning is secure after a change is made in the human resources software, if the policy allows for unregulated access to this software, it would not be difficult to grant unauthorized access to resources across the enterprise.

Finally, the security policy should be subjected to both internal and external audits. Auditing should be a process, not just an event. By constantly reviewing their policy, corporations have the opportunity to address vulnerabilities that may not have existed when the original policy was documented. Identity management

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

systems facilitate the changing of rules company wide so an updated policy can be easily implemented.

Conclusion

Although identity management is a relative new idea, it is certainly a proven concept. Whether a corporation has had previous security incidents or just wants to prepare for the future, the solutions currently available can help to secure their resources. The preceding should serve as an aid to identifying security risks and provide an understanding of how an identity management solution can be implemented to counter these risks.

© SANS Institute 2003, Author retains full rights.

References

1.
Armstrong, Illena. "Access Management Part One: Sound ROI With Security Benefits." URL:
http://www.scmagazine.com/scmagazine/2002_10/cover/index.html
(4 Dec. 2002).

2.
"Identity Management. The Business Context of Security: a White Paper." URL:
http://www.pwcglobal.com/extweb/newcoatwork.nsf/0cc1191c627d157d8525650600609c03/9fba7a678f38f43885256b12007d5ea9/$FILE/Security%20White%20Paper.pdf (4 Dec. 2002).

3.
Lewis, Brett. "Making Smart Cards Work In the Enterprise." 4 April 2002. URL:
http://rr.sans.org/authentic/smart_work.php (4 Dec. 2002).

4.
"Edefice Product Overview." URL:
http://www.peapod.co.uk/products/intercede/edefice.pdf (4 Dec. 2002).

5.
"Transparent Syncronozation." URL:
http://www.psynch.com/about/trans-synch.html (4 Dec. 2002).

6.
"Business Layers: eProvision Software." URL:
http://www.businesslayers.com/dayone.asp (4 Dec. 2002).

7.
"Schlumberger Integrates eProvisioning Software into DeXa.Badge Solution." 9 Oct. 2002. URL:
http://www.slb.com/press/newsroom/index.cfm?PRID=13301&ThisSectionID=112 (4 Dec. 2002).

8.
"ADPr | Frequently Asked Questions." URL:
http://www.adpr-spec.com/profile/faq.htm (4 Dec. 2002).

9.
Somayaji, Nanjunda. "Implementing Java applications security." May 2002. URL:
http://www.serverworldmagazine.com/monthly/2002/05/java.shtml (4 Dec. 2002).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

10.
"Business Layers: Success Stories." URL:
http://www.businesslayers.com/success_stories.asp (4 Dec. 2002).

11.
"Intercede - Solutions - Government - Case Study." URL:
http://www.intercede.co.uk/Solutions-government-success1.htm (4 Dec. 2002).

12.
"Case Study: Reducing Help Desk Password Calls: Self-service and Problem Elimination." URL: http://www.dci.com/brochure/hdbos/schedule.asp
(4 Dec. 2002).

Yasin, Rutrell. "What is Identity Management?" April 2002. URL:
http://www.infosecuritymag.com/2002/apr/cover_casestudy.shtml (4 Dec. 2002).

Figure 1.
"Edefice Product Overview." URL:
http://www.peapod.co.uk/products/intercede/edefice.pdf (4 Dec. 2002).

Figure 2.
"Transparent Synchronization architecture." URL:
http://www.psynch.com/technology/arch-ts.html (4 Dec. 2002).

© SANS Institute 2003, Author retains full rights

Last Updated: September 3rd, 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