Interested in learning more about security?

SANS Institute InfoSec Reading Room

Identity Management

Six months ago you hardly heard of "Identity Management" - but today you hear about it and see it nearly everywhere. Information security magazines of all nature are publishing more and more articles about identity management and improved access control measures. Hardware manufacturers are adding new and improved smart cards, USB authentication keys, and biometric input devices to their line of products. Software developers are scrambling to promote new and improved access control applications and improved authenticati...

Kevin Kaufman
GIAC Security Essentials Certification (GSEC) Practical Assignment
Version 1.4b - Option 1

IDENTITY MANAGEMENT

Table of Contents **Page**

Abstract

Six months ago you hardly heard of "Identity Management" – but today you hear about it and see it nearly everywhere. Information security magazines of all nature are publishing more and more articles about identity management and improved access control measures. Hardware manufacturers are adding new and improved smart cards, USB authentication keys, and biometric input devices to their line of products. Software developers are scrambling to promote new and improved access control applications and improved authentication utilities. Is "Identity Management" a new buzzword in the Information Security arena or is it an important security principle just now coming of age?

With all the hype going on about biometrics, smart cards, and other "failsafe" access control measures, how do you know what to evaluate, test, and implement? How do you know what system is right for your organization? Before can you answer that, you have to determine whether or not your organization has an Identity Management Policy. If you do, is it sufficient? Is it accurate? Is it Feasible? Is it realistic? And best of all, has it been fully tested? If you do not have an Identity Management Policy, than how do you create one? Where do you start?

Why do you need Identity Management?

As organizations grow and add services such as e-commerce and global remote access, and integrate new business functions such as joint ventures and multiple span projects, controlling who is accessing company information resources is becoming an even more difficult task. Information and Network Security Specialists need to be able to control who is accessing sensitive and proprietary information, when they are accessing it, and from where they are accessing it. Access could include but is not

limited to: web-based access, remote dial-in access, access via VPN, or direct access via the organization's intranet. As the scope of access control continues to grow and span across multiple systems and multiple applications, each system could be using a different method of access control and user authentication.

Web-based access control can be achieved by using Microsoft Internet Information Server, Coldfusion, or Apache services to authenticate user logons. Users could be using standard FTP or Telnet sessions to access information or they may be dialing in directly to a Remote Access Server (RAS) or they could be creating a Virtual Private Network (VPN) connection via the Internet or other network connection. Joint ventures with other organizations may require configuring VPN tunnels between network firewalls to allow the interchange of information. The possibilities are nearly unlimited.

So how does an organization manage multiple facets of access control?
Answer: With a comprehensive Identity Management Policy and with the help of a comprehensive Identity Management application.

It may sound simple, but it is not necessarily all that simple. Identity Management Policies should focus more on what the organization would "like to do" as opposed to what it "currently does." You then have to evaluate current procedures against desired procedures, research and select the correct access control solution(s) that meet your organization's needs, and finally develop a plan for implementing those solutions. These solutions can be implemented throughout the entire organization or just in those areas where they are needed most. Identity Management can encompass multiple facets of access and authentication.

In his article "What is Identity Management," Rutrell Yasin lists the following building blocks to an Identity Management System:

1) Password Reset
2) Password Synchronization
3) Single Sign-On
4) Access Management Software

A complete identity management solution should allow users to reset their own passwords or unlock their accounts. This can be accomplished using client software or an interactive voice or touch-tone response system, but the most practical method is using a web-based interface. The web-based interface can be accessed via any internet browser. This solution would provide open access while on the company intranet and you can use SSL secure authentication when accessing the utility externally. In any event, the solution has to provide a reasonable series of challenges or questions to which only the prescribed user would have all the answers. I have seen such solutions which ask the user for their social security number, the date they were hired, and their birthday as challenges to positively identify themselves before allowing them to change their password or unlock their accounts.

Such a web-based solution would greatly reduce the number of help desk calls for password resets. In 2001, Nancy Tripp, the manager of the Sun Trust Bank's Solution Center, calculated that 27-35% of all help desk calls are password related. To counter this, Sun Trust installed Courion's PasswordCourier password management software solution. The solution allowed employees to reset their Windows NT, Netware, and IBM Mainframe passwords and then synchronized all three to use the same password – which leads us into the next building block.

Products which provide password synchronization across multiple systems also reduce help desk administrative requirements, but more than that, they reduce the frustration level many users reach by having to go to each separate system they access to change passwords so they do not have to remember different passwords for each system. This can be quite advantageous in enterprise environments that use separate systems such as Windows NT domains, Lotus Domino web-based resources, IBM mainframe accounts, SAP client accounts, etc. etc. The list could go on and on, depending on the size of enterprise environment. When users have to maintain more than one password, the chances that they will lock one account or another by using the right password on the wrong system or the wrong password on the right system. The user then becomes even more frustrated when multiple accounts are locked and they have a deadline to meet. Password synchronization solutions are easier to implement than the next building block item (single-sign on solutions) because they use existing API calls to access multiple password database records and security modules.

The next building block, single sign-on solutions (SSO) are a little more resource demanding to implement, usually requiring separate authentication servers and the installation of single sign-on agent on each workstation. The SSO agent stores the user's logon information and passes it to all applications that require separate authentication. Some of the most popular SSO solutions available are:

1) Computer Associates' eTrust Single Sign-on
(http://www3.ca.com/Solutions/Product.asp?ID=166)
2) Passlogix's V-Go Single Sign-On
(http://www.passlogix.com/sso/marketing/overview.asp)
3) Blockade System's ES Access Single Sign-On
(http://www.blockade.com/products/esaccess.html)

The last of the primary building blocks is the use of access management software to allow the right people into the right places at the right time. Complete access management solutions use multiple methods of verifying identity depending on the type of access. Access could be authenticated with standard usernames and passwords, digital certificates, or by using hardware or software tokens. Great access management solutions are provided by following vendors:

1) IBM Tivoli Access Manager for e-business.
http://www-3.ibm.com/software/tivoli/products/access-mgr-e-bus/
2) IBM Tivoli Access Manager for Operating Systems

http://www-3.ibm.com/software/tivoli/products/access-mgr-operating-sys/
3) Netegrity's SiteMinder
http://www.netegrity.com/products/index.cfm?leveltwo=SiteMinder
4) Entegrity's AssureAccess
http://www.entegrity.com/products/aa/aa.shtml
5) RSA Security's ClearTrust
http://www.rsasecurity.com/products/cleartrust/datasheets/dscleartrust.html
6) Oblix's NetPoint
http://www.oblix.com/products/netpoint/index.html
7) Baltimore Technologies's SelectAccess
http://www.baltimoretechnologies.com/selectaccess/index.asp
8) Entrust's Authority solution packages
http://www.entrust.com/authority/index.htm
9) Waveset's Lighthouse Password Manager
http://www.waveset.com/Solutions/Lighthouse/Password_Manager/

Personally, I am quite familiar with and fond of RSA's wide range of access management solutions to include hardware solutions mentioned earlier. RSA's Secure ID Tokens can be used to authenticate users via remote dial-up access or through VPN Access Clients.

Many vendors have even formed alliances and joint ventures to develop better access management solutions. Entrust and Waveset formed an alliance that will enable them to deliver identity management solutions for government and business use which easily deploys into enterprise and web-based applications and can handle highly secure identity management solutions for sensitive environment. The alliance was formed based on government and enterprise business needs to implement complete identity management solutions, which incorporate the best of multiple vendors in one packaged solution. The two companies plan to use bi-directional technology sharing to improve efficient and cost-effective identity management solutions which can be deployed across diverse applications and environments while maintaining accountability of functions and privacy for stored identification credentials.

A final building block that should not be forgotten is password policy enforcement. This could be seen as a component of the password reset procedures, but it is important enough that organizations should address it explicitly. I am sure we have all encountered password policies which require eight characters or less, at least one alphabetic character and at least one numeric character, or even a special character or at least one capital letter, and of course the system keeps a history of the last ten passwords used. All of these topics should be part of the organization's access management procedures and identity management policy.

Putting It All Together

So, now that we have the building blocks for a good identify management policy, how do you put it all together?

Remember, you have to develop your policy first – based on what the organization "wants to have," then compare that to what you "currently have" and make improvements where needed. Of course the best process would be to gradually implement your solutions, one area at a time, until the complete Identity Management solution is in place.

A simple password management process may look like the following:

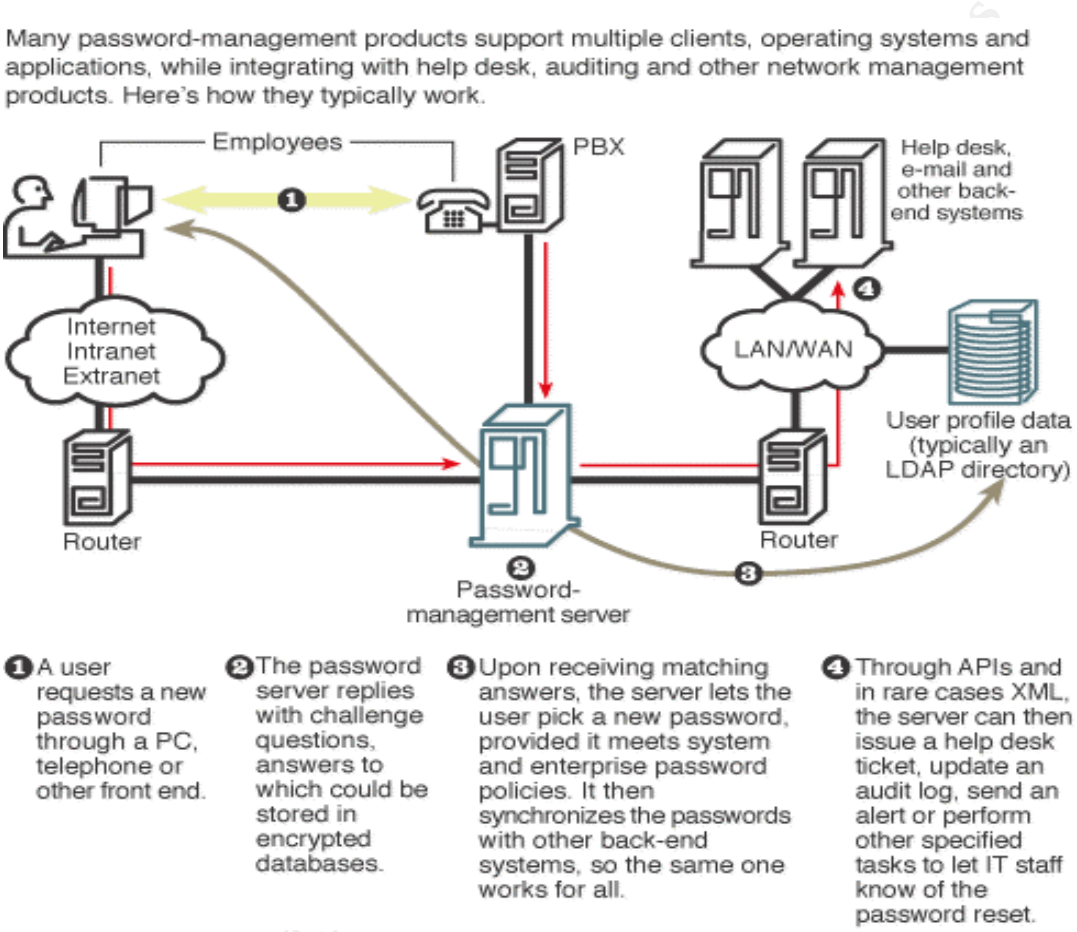

Diagram courtesy of Network World Fusion

There are many companies that provide complete identity management solutions and would even assist in creating your Identity Management Policy.

IBM's complete Identity management solution addresses the following four key areas of identity management and includes seven separate products in one scalable open source solution:

1) Identity lifecycle management (user self-care, enrollment and provisioning).
2) Identity control (access and privacy control, single sign-on and auditing).
3) Identity federation (sharing user authentication and attribute information between trusted Web services applications).

4) Identity foundation (directory, directory integration and workflow).

As with other complete Identity Management solutions the benefits can be dazzling. A complete system should:

1) reduce operating costs by integrating identity management into centralized operations such as Help Desk support
2) it should increase productivity by limiting the amount of time users spend changing and managing their own authentication credentials
3) allow the organization to perform timely security audits to uncover vulnerabilities
4) provide a direct realized return on investment by being able to integrate users, systems, and applications faster and with less downtime

Security Assertion Markup Language (SAML) and WS-Security

Recent developments have lead to the establishment of the Security Assertion Markup Language (SAML) - an emerging XML-based standard for exchanging authentication and authorization information between systems and applications.

Multiple vendors to include RSA Security, Netegrity, Oblix, Baltimore Technologies, Crosslogix, Sun, IBM-Tivoli, and Novell, are supporting and implementing this standard that will allow multiple products from multiple vendors to interact as organizations need them to. This allows organizations to pick and choose the solutions they want for their specific areas and integrate them into one complete customized Identity Management package.

One development problem is that Microsoft has chosen to use Kerberos as its protocol for passing authentication information. However, Microsoft has committed itself to integrating a set of proposed standards developed in conjunction with IBM and VeriSign known as WS-Security. Both standards are under review by the Organization for the Advancement of Structured Information Standards (OASIS) Security Services Technical Committee (SSTC).

The main debate is that SAML uses HTTPS encryption while WS-Security uses true XML encryption. WS-Security better protects individual transactions while the complexity of SAML supports single sing-on solutions. So there is a trade-off, better security or better functionality? Each organization has to decide for themselves.

Multiple top-notch vendors joined in arms to form the Liberty Alliance, aimed at producing a global network identity solution to be used on the Internet to support single sign-on support. The goal of this single sign-on solution is to allow individuals and businesses to conduct on-line transaction more efficiently and with the peace of mind that security is being maintained. Profile information is supposed to be managed by the individual to which it pertains but is securely stored by and shared between companies of choice. The intent is to stimulate and simplify the use of e-commerce while adding

security by supporting a wide range of identity-based products and services and placing the control of personal information in the hands of the owner.

The Liberty Alliance's Liberty 1.0 authentication solution is based on SAML, while Microsoft's competing .NET Passport technology uses WS-Security. Both standards are running neck-to-neck in the race to the finish line. It would be a good thing if the two were to converge and develop one global standard, but don't hold your breath on that one. Whatever does happen, it looks like the future of e-business and e-commerce is dependant on these standards.

The Liberty Alliance is currently composed of over 150 member companies supporting over one billion customers. Popular names like Verisign, RSA, Entrust, Intuit, register.com, Netegrity, PingID, Visa, Mastercard, Nextel, Vodafone, Novell, and Cisco are all involved.

E-Business and e-commerce rely heavily on extranet access to a wide range of services, be it business-to-business, business-to-consumer, Internet based applications and portals, or remote access to company proprietary information. Most organizations are desperate to find a solution to these needs that meets their budget and stays within their security concerns. The path continues to lead back to OASIS' approval of proposed standards and the Liberty Alliance and Microsoft's acceptance and compliance to these standards. Together with IBM, Microsoft developed a Simple Object Access Protocol (SOAP) which is claimed to be an extension of WS-Security that supports SAML and Kerbos forms of identity management but has as yet not produced any detailed plans of integrating SAML into its .NET Passport technology. The Liberty Alliance in-turn stated that it would support WS-Security with the release of Liberty 2.0 in the near future.

The Gartner group reported that financial institutions would more than likely be the first to adopt the federated global identity management solutions offered by Liberty or Passport, but showed no near term intentions of adopting either one. Emphasis is developing however from business-to-business providers for these financial institutions to adopt one or the other to reduce their cost of operating and increase their return on investments. More than likely, the emphasis will be on integrating security interfaces to Active-Directory since most enterprise organizations are operating in a Windows based environment. Gartner predicts that the main emphasis will be on providing user management across multiple applications via extranet access clients. Gartner developed the following Extranet Access Management magic Quadrant to display the Leaders and Niche Players involved in this development:

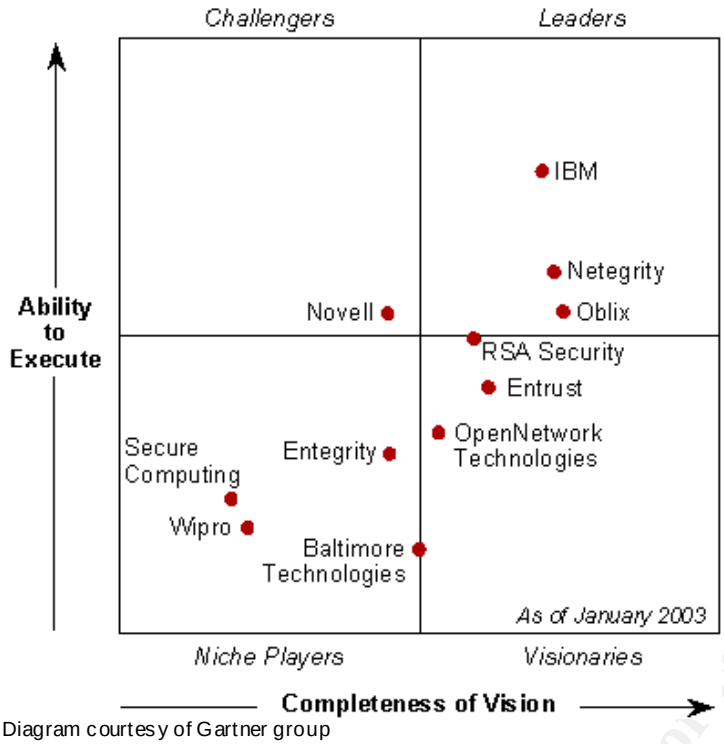

Diagram courtesy of Gartner group

You will notice that Microsoft is not displayed in all of the four quadrants. This is because Microsoft currently offers no supporting products but has announced that TrustBridge technology will be shipped as a component of .NET Server. Combined with Commerce Server.NET, the two could provide an extranet access management solution which uses Active Directory and could interface with a complete Identity Management solutions.

Identity Management Return on Investment

By far an organization's major concern is return on investment. Securing proprietary information and personal data is no longer just an IT concern, but a concern for the Board of Directors and external investors alike. In most cases, a company's most precious asset is the information stored on its IT systems. Customer lists, proposals, and financial information are the true credentials for every organization. Compromising these credentials would mean compromising the organization's existence.

In the past, budgeting for IT security was always a sore subject for the financial analysts - but times are changing. More and more organizations are realizing that a true return on investment comes from efficiently and effectively security its credentials. By implementing identity management solutions, not only does the organization benefit from improved security and access control, it benefits from lower operating costs in the form of more efficient operations and reduced manual effort.

Identity management allows users to manage their own access control (to an extent). Yeah, yeah – there will always be those in management that fell as though this is purely

an IT function and that Help Desk Support technicians need to be available 24/7 to manage user accounts - and in instances like this it is meaningful to demonstrate to those members of management the benefits from lowered IT costs or outsourcing expenses for such IT support. Demonstrate the by-call expenses accrued each time a user has to call the Help Desk to unlock or reset an account password. Demonstrate that it would take at least 5 minutes on the phone to do so as opposed to 1 minute via an automated web-based identity management system where the employee can validate their own identity and synchronize all system passwords at one time. It is this increase in productivity time that will catches most managers' attention.

Case Study

Burlington Northern Santa Fe has to maintain over 45,000 users-identification profiles, 38,000 for employees and an additional 7,000 for external users and staff access rights.

For Rick Perry, the director of security, managing these profiles is not easy tasks. Through the continuous merger of seven major railroads, BNSF has acquired employees from other regions who now need access to computer mainframe to input scheduling and availability information. Oh and by the way, most of these employees do not have offices with desks and computer connected directly to the organization's intranet – they input data remotely from home or on the road.

But Rick overcame all of this and integrated a near complete identity management solution that helps him manage these accounts while providing security and increasing employee productivity.

Rick was faced with users in all experience levels.
Locomotive engineer used to input their timecard information using a voice response or touch-tone activated telephone system (faux IVR).

Rather than using the current system of inputting Social Security Numbers and dates of birth, Rick wanted to protect this personal information and developed a PIN-based system where every employee created their own PIN and had to change in every calendar quarter. Rich also wanted to allow employees to change their passwords remotely rather than having to contact the company's Help Desk to do so. And if that weren't enough, accounts payable needed to allow extranet access to customers for bill paying and shipment tracking.

Rick searched and searched, and evaluated and evaluated, multiple products from multiple vendors and finally decided on Waveset's Lighthouse Software as an identity management solution.

Rick quoted it as: "Some of the other products we looked at [from bigger companies] were very costly and unwieldy. A lot of them required that we conform to their processes. Lighthouse has a feeling of being more flexible, and easier to adapt to our environment. It was lightweight, but not in a bad way."

The Waveset Lighthouse solution could be integrated into BNSF's web-based systems and back-end servers made up of mainframes, Windows NT servers, and AIX servers.

The lighthouse solution starts at around $250,000 but allows the organization to quickly realize a return on investment.

It took BNSF 3-4 months to completely integrate the Identity Management solution throughout internal systems. The major challenge was integrating the system used the most such as email and the mainframe databases.

Another challenge for BNSF was to implementing standard policies on all systems.

The security department is eagerly awaiting integration of external users and has already reduced turn-around time for internal account requests from 48 hours down to 24.

It may take some time to work out all the "bugs," but Rick sees the solution as a way of achieving company goals of increasing productivity and improving service.

SUMMARY

I think you can now see the importance of Identity Management. Standardizing and integrating identity management across all systems and platforms helps reduce an organization's operating costs and increases productivity, as well as improves access control and security overall. It is not an easy task and in some cases it is not an inexpensive one either, but the benefits speak for themselves. It is within every organization's interest to create a strict Identity Management Policy and to integrate an automated Identity Management solution that helps achieve company goals.

References:

"19th Annual Tech Ex Awards – Protocols, Winners: SAML and WS-Security." PC Magazine. November 19, 2002
URL: http://www.pcmag.com/article2/0,4149,715069,00.asp (29 April 2003).

Baldwin, Howard. "Identity management software helps railroad connect with far-flung employees." Waveset Tech Republic, Sep 23, 2002
URL: http://www.waveset.com/News/features/TechRepublic/092302/index.html (30 April 2003).

Bort, Julie "Identity Management Begins with the Humble Password." Network World, 21 October 2002. URL: http://www.nwfusion.com/supp/security2/password.html (29 April 2003).

"Entrust and Waveset Announce Strategic Alliance To Deliver Secure Identity Management Solutions." Dallas, TX. 07 Apr 2003
URL: http://www.entrust.com/news/files/04_07_03.htm?entsrc=transform_theme (29 April 2003).

Fontana, John. "Accent on access control - Conference to highlight SAML, an emerging standard for identity management." Network World. 15 July 2002. URL: http://www.nwfusion.com/news/2002/0715saml.html

"IBM Tivoli Identity Manager." IBM. Updated 24 April 2003.
URL: http://www-3.ibm.com/software/tivoli/products/identity-mgr/ (29 April 2003).

"Identity Management." IBM. Updated 11 April 2003.
URL: http://www-3.ibm.com/software/tivoli/solutions/security/id/ (29 April 2003).

"Identity Management." The National Electronic Commerce Coordinating Council. A White Paper Presented at the NECCC Annual Conference, December 4-6, 2002, New York. URL: http://www.ec3.org/Downloads/2002/id_management.pdf (29 April 2003).

"Integration of Provisioning, Password Management, Audit, Event Management and Administration Solutions To Benefit Joint Customers." Consol Enterprise Security. December 2, 2002. URL: http://www.consul.com/index.php3?cid=501 (29 April 2003)

McClain, Mark (President and Founder, Waveset Technologies). "Identity Management – Tangible ROI For Enterprises." SC Magazine, November 2002
URL: http://www.waveset.com/News/features/scmagazine/112002/index.html (30 April 2003).

Pescatore , J., Wagner, R. "Extranet Access Management 2H02 Magic Quadrant." Gartner Research Notes. 08 January 2003.
URL: http://www.gartner.com/reprints/ibm/112404.html (30 April 2003).

Rutrell Yasin. "What is Identify Management." Information Security Magazine April 2002.
URL: http://www.infosecuritymag.com/2002/apr/cover_casestudy.shtml (29 April 2003).

"Security Assertion Markup Language (SAML) - Technology Reports Overview." Cover Pages hosted by OASIS
URL: http://xml.coverpages.org/saml.html (29 April 2003).

"The Liberty Alliance Project."
URL: http://www.projectliberty.org/ (30 April 2003).

Last Updated: October 22nd, 2017

Upcoming SANS Training

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

SANS San Diego 2017	San Diego, CAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Seattle 2017	Seattle, WAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, AE	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Milan November 2017	Milan, IT	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Amsterdam 2017	Amsterdam, NL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Miami 2017	Miami, FLUS	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Paris November 2017	Paris, FR	Nov 13, 2017 - Nov 18, 2017	Live Event
Pen Test Hackfest Summit & Training 2017	Bethesda, MDUS	Nov 13, 2017 - Nov 20, 2017	Live Event
SANS Sydney 2017	Sydney, AU	Nov 13, 2017 - Nov 25, 2017	Live Event
GridEx IV 2017	Online,	Nov 15, 2017 - Nov 16, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CAUS	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, GB	Nov 27, 2017 - Dec 02, 2017	Live Event
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZUS	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Khobar 2017	Khobar, SA	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Austin Winter 2017	Austin, TXUS	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Munich December 2017	Munich, DE	Dec 04, 2017 - Dec 09, 2017	Live Event
European Security Awareness Summit & Training 2017	London, GB	Dec 04, 2017 - Dec 07, 2017	Live Event
SANS Bangalore 2017	Bangalore, IN	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Frankfurt 2017	Frankfurt, DE	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DCUS	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS SEC460: Enterprise Threat Beta	San Diego, CAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, NL	Jan 15, 2018 - Jan 20, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SEC599: Defeat Advanced Adversaries	San Francisco, CAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Berlin 2017	OnlineDE	Oct 23, 2017 - Oct 28, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced