Global Information Assurance Certification Paper

Identity Management: (An overview on securely managing users, throughout the corporate environment)

By David D. Cahoon
Version 1.4b, Option 1 for GSEC
June 2003

Abstract

As corporate businesses globally expand their e-business through growth, acquisitions, and mergers, consolidating user information across multi platforms add to the propensity for unauthorized access that can be magnified exponentially by the number of identifiers that must be maintained. Added to this complexity is the demand from Corporate Business to provide increased security over their growing user base and productivity of their security staffs, leveraging lower cost models and integrating most if not all of their core business processes.

To better understand how to achieve these goals on managing user information a top-down hierarchical view is presented on Identity Management. This top-down view will start with the Corporate "Buy In", the establishment of policies and procedures, defining the Authoritative Source (Data Owners) which will feed The Identity Source (Data Custodians) which in turn supplies the necessary information needed for the User Management (Data Users). Finally we will look at how Identity Tools could be utilized in this type of environment.

Introduction

What is Identity Management?

Identity management is a term used to identify individuals in a system. Most recently this term has become the buzzword for many IT organizations in defining roles and access rights by controlling their access to resources within that system by associating user rights and restrictions within the established identity. It is driven primarily to provide better security throughout the organization. It can also manifest itself by improving service levels and reduced administrative costs. If we look at our Social Security number as an example of identity management, we see how quickly this can become a very complex environment. It can be used to identify you in many different ways. It is used in conjunction with identifying you as a taxpayer, used as your driver license number, bank accounts, and even as your library card. Managing access to all of these accounts, and who has access to these accounts, as well as auditing and reporting becomes a daunting task for even the most seasoned IT professional. As we will soon see, setting up controls, policies and procedures, and structure to the Identity Management process will be key in a successful implementation. Before any serious IT architecture review for implementation of Identity Management takes place,

getting corporate “Buy In” is essential, and not just for approval of corporate dollars. Yes, you will have to explain Return on Investment to your corporate brethren, but there are other requirements that must not be overlooked.

Corporate “Buy In”

The first thing to understand in this journey of establishing Identity Management is to know that upper management must fully endorse this strategy. As I mentioned above they’re probably will be a significant spend on infrastructure support, key components being data storage, enterprise directory, authentication and authorization systems, but more importantly they must invest and endorse in a strategic security policy and procedure program. This will be the foundation for all other processes concerning the Identity Management initiative. This will determine the data owners, who are authorized to grant access, which is responsible for the data, it begins the mechanism for ensuring authentication and authorization, and ultimately who will maintain these functions. Corporate security policy and procedure will directly influence the implementation of identity management. Unfortunately, there is no one policy or procedure that will fit all corporations. It will have to be tailored to each business requirement. Some basic guidelines are listed below.

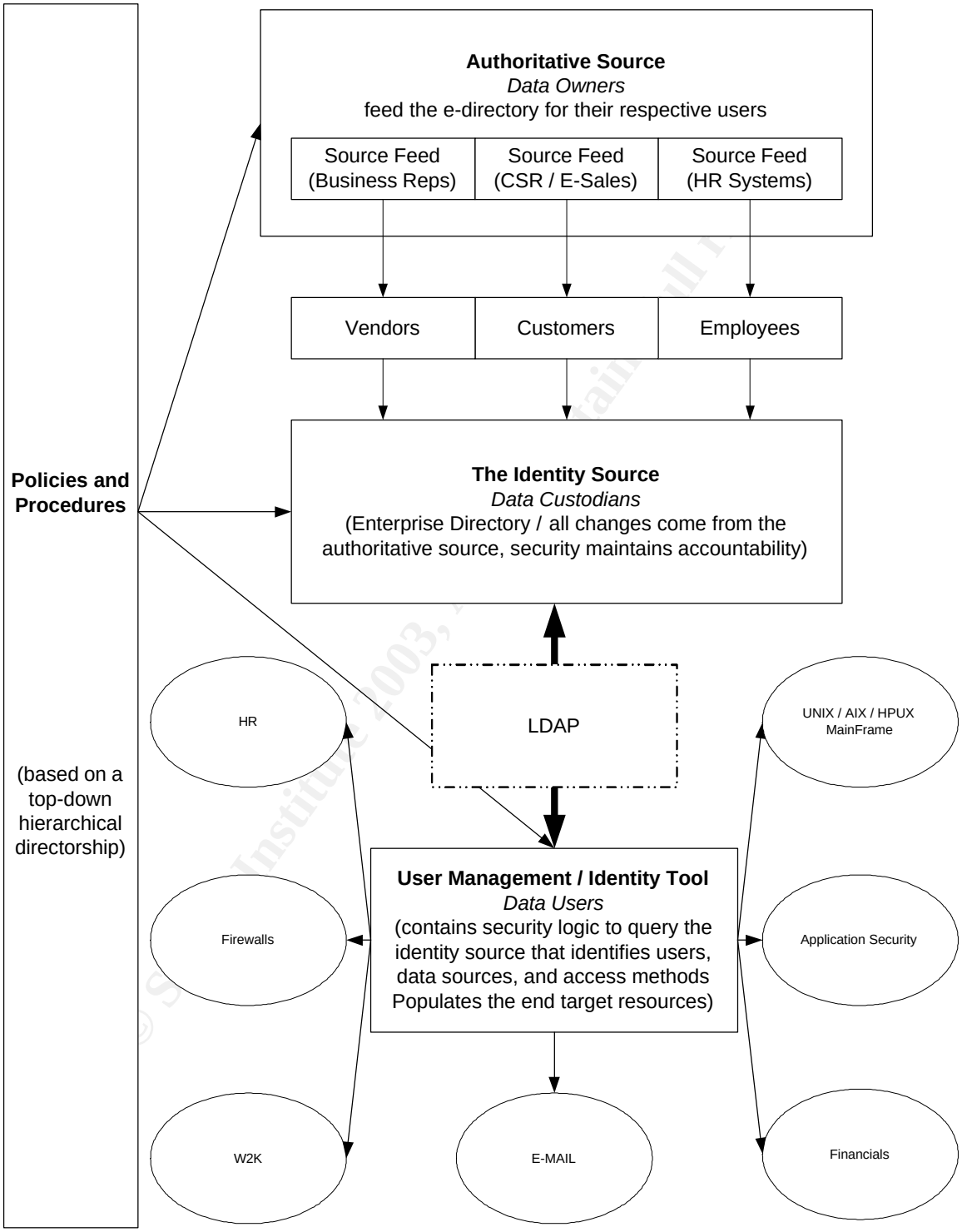
“The Security Policy needs to

1. Be implementable and enforceable
2. Be concise and easy to read
3. Be protective yet be productive
4. Be regularly updated
5. State the reasons why it is in force
6. Define responsibility
7. Follow regulatory guidelines”

(Crabb-Guel http://www.sans.org/resources/policies/bssi3/)

Security procedures will define how you protect the company resources and how to enforce the policies. It will describe the mechanism necessary to build, use, and enter information needed for Identity Management.

Finally, the key reason you will need corporate “Buy In” is they will play the key role in User Administration. Please note that the IT Organization is responsible for maintaining hardware and software that delivers user credentials, but it is the Corporate Management role to decide who, what, and how user information is going to be managed. Depending on the clarity of these documents and procedures will directly affect how well your Identity Management solution will be. A haphazard plan with no business direction is doomed from the start. To better understand this relationship the following diagram will show how significant the corporate role is. It shows how their decisions affect all parts of the Identity Management structure. Notice that it touches all aspect of Identity Management.



The Authoritative Source

The next logical step in the Identity Management flow is defining the Authoritative Source. This is the first place that the policy and procedure decisions made by the corporate management will determine who controls what data. How they perform their duties will be dictated in those procedures. This is also the first step in how you will identify your users. Lets step through this process in more detail

What is an Authoritative Source?

This is the area I refer to as the *Data Owners.* I will also refer to them as the Corporate Data Stewards (CDS). By looking at the diagram I have broken this area into three distinct sections. The CDS directly control which users have access to their respective data. This information ultimately feeds the enterprise directory structure. The sections contained in this area are:

Business Representatives
Customer Service Representatives or Electronic Sales
Human Resources and Payroll Systems

Please note that your organization may have many buckets within these three major ones, but this architecture leads to the primary focus of the Corporation to provide increased security, leverage lower cost models, and integrate core business processes. As previously mentioned, there should be a policy which dictates that within the company can request or directly enter in information about a user. They will be directly responsible for their data and who has access to it. This structure also lends itself in defining your directory structure. Some fore thought should be considered when granting access to your data. Logically storing your data and creating a standard set of user access has two major advantages

1. Security
   - Definition of Role Based Security Models
   - Safely integrate vendors, customers, employees
   - Helps define access to applications
   - Begins the mapping of how Authentication & Authorization takes place
   - Provides the framework for Identity Management needs

2. Revenue
   - Improvement in revenue yields and business cycles
   - Improve efficiencies of security department
   - Faster integration of applications
   - Provide accurate accounting of information
   - Reducing overall expenditures in IT operations

By setting up your source feeds in a logical and streamline manner can pay huge dividends at the end of the tunnel involving Identity Management. To recap, you need to establish solid policies and procedures and has those living documents dictate how you set up your authoritative source. Those individuals must be responsible for who has access to your data. We next move into the Identity Source Area, where we will look at how we maintain the information, control access to the information, and maintain accountability.

The Identity Source

The Identity source area performs three major functions. Lets look at how each one these critical functions work within the framework of Identity Management.

Maintain Information

This is where you store and hold your protected resources. But what exactly does that mean. I must go back to the corporate "Buy In" section that stated, "It is the Corporate Management role to decide who, what, and how user information is going to be managed". I cannot state how important this is. These policies will dictate how user information will be stored, such as will it be encrypted or not, is it accessible from the Intranet or extranet, how long will the data be stored and ultimately who has access. Certain data may be used for several applications or transactions, and who has access is directly attributed to the security policies. How you set up this data is very critical in a successful implementation. Will you use an LDAP directory structure, or some relational database structure, or even using DSML developed by OASIS. It is noted, most tool selections, which will help administrate identity management, is based on an LDAP compliant format. How you set your data stores and raw data should have a direct relation to your business requirements. Keeping this data updated is absolutely necessary. Ensuring that the data steward's are correctly identifying the classifications of their data and delegating who has access will be instrumental in maintaining your information. Through consolidation and structuring like tables and groups together thus in tun help leverage return on investment. Preplanning and stating hard business requirements is key to properly maintaining your information, how this is set it up will determine ease of use and return on capital.

Controlling Access

Again, the business policies and procedures will directly affect how access is controlled. Based on these structures will impact how the security administrator will control access. This is not to be confused with the user authentication, which is a different mechanism to properly authenticate a user. This is where they validate their identity. Once they have validated their identity, they are given access to certain resources; this is the control I'm speaking of, one, which controls access to the data stores, whether that is in a directory style format, or

relational database. Other key issues that need to be evaluated are what level of control will we place on this data. Some insight should be fed from the corporate data stewards. Ultimately they are responsible for who has access to data or application information. Will it be course medium or fine grain access? Will they have read write or execute rights. Can they control other users, groups, or realms? What applications will they be able to launch? How will that control be fed or utilized? Are the decisions you are deciding making sense and meet business objectives? Obviously, this is a lot of decisions to make, but are critically important if you want your implementation to be successful. Spending the time in pre-work will save huge amounts of rework and effort in the long run. The last section of the Identity Source deals with accountability, several items are necessary in maintaining accountability.

Maintaining Accountability

Before anyone can account what has taken place in your identity source one needs to know what was there in the beginning and what has taken place afterwards. You must also be able to account for these transactions. Let's examine a bank vault for an example. Most people are familiar with a bank vault, the governing bank body oversees what can and cannot be done in their vault, and they dictate when it opens and closes. They're guards that monitor who can enter and exit. There is video circuit that's monitoring the systems to oversee what is transpiring. Certain people can enter and either deposit or withdraw items from the vault and the accountants are responsible for ensuring that any transactions inside the vault is properly accounted for each day starting from day one! If we examine this from a data store view, we can relate the previous example into the reality of maintaining accountability in the Identity Source. As usual, you will need specific policies and procedures to define that can access your data stores, directed by the governing body (corporate). Within these guidelines, rules, and policies will dictate when individuals have access to it. As with the bank example someone will need to oversee the transactions. Decisions such as, will this be a manual process, or an automated process, need to be decided. What type of technologies will you put in place to watch these transactions? What type of historical reporting tool or log files will be kept on these systems? Some external monitoring such as Intrusion Detection Systems (IDS) or Host based IDS, might be required as the bank's video monitoring systems are. You will need to account and in some cases report on what was entered into your data stores. The key component of this area is to maintain control on what is in your data a store at all times. If you cannot keep track of what goes in or what goes out, you cannot properly maintain who has access to your information, due to the fact you do not know what information you are protecting! This is a critical piece of your architecture. You will absolutely need this if you ever decide to take legal action against someone in the case of improper usage of your systems.

The IT security department should spend a considerable amount of time and effort in this space. Setting up proper containers, sub containers and structures within your data store will reduce administration dramatically. Ensuring proper rights and controls are in place will help in increased efficiencies, and maintaining accountability will decrease the frustration of what has transpired on the system.

User Management

For most people this is what is thought of when you mention Identity Management. It is the security administrator, delegated administrator, or even the individual, maintaining information on the user. Five major subsets are featured in managing the user, which include user provisioning, delegated administration, password resets/synchronization, self-service, and integrated workflow. Although this portion of identity management is the most recognizable, all of the previous sections are just as important when thinking about identity management. Let's discuss the major subsets of user management.

User Provisioning

This is the process we use to manage the user. It is the lifecycle of the user. It starts when you grant access, modify; term or delete accesses when it is no longer needed. Corporations are finding this task is consuming a tremendous amount of time and efforts from not only their administrators, but from help desks and user alike. Reducing this complexity and streamlining these processes could pay huge dividends to the corporate bottom line as well as freeing up precious time for their administrators to perform other duties. This is one area where return on investment could be realized almost immediately. By having a tool perform the user provisioning process, literally hours per user could be shaved from the user provisioning process. More importantly it could help track and disseminate multi-user profiles and help manage those identities. This could also help in creating role based security system. New mining tools for user grouping could help in building a role-based model, and getting rid of the dreaded copy person for rights generation. How we manage the life cycle of user's access will become more critical as access points and the multitude of rights ever increases.

Delegated Administration

This is an area that could have huge dividends if properly implemented. By giving other administrators or designated users the ability to provide user provisioning, it will free up time and increase productivity by decreasing the turn around time to perform user administration. Some examples where delegated administration makes sense are in business-to-business transactions. This could be where you give access to web applications. They could then enter their own user information to access this web data. There would have to be predefined business rules, but you could offload that administration to the end user. This makes sense

due to the fact that the distant company would know when additional access needed to be granted as well as terming ended user accounts. This is just one example how delegated administration could help streamline the process of identity management.

Password resets/synchronization

One of the largest headaches for any large organization is the amount oft time spent performing password resets. The help desk or support center can easily spend up to 50 percent of their day resetting passwords. The other time is spent synchronizing password to rest of their accounts. This has traditionally been a huge manual process. If you could just save 30 percent of your help desks time in performing password resets, the saving could be phenomenal. This is where a properly setup identity management structure could reap large gains in productivity. First of all it could gives the advantage of having the user perform their own password reset. Having a backend process that would synchronize the password to other systems could also be developed and utilized. This is where proper tool selection makes sense, which I'll go over in more detail later in the paper. Some suggestions of how this is to be accomplished are through an online web process, or a front-end GUI, or a phone system that directly interfaces to your systems. By knowing where your users are located and how they are identified gives you the leverage to use this technology. Obviously, by saving time and lowering FTE count, corporate will love the return on investment. The other benefit is you're freeing up time of your administrators to perform true administration of your systems and not just data entry.

Self service

Knowing what information you are going to store on your infrastructure will increase the likely hood of being able to perform self-service. This would be the ultimate goal of all security administrators. Pre-canning your identity solution in a self-service walk-up, web, GUI, or phone system is the ultimate in streamlining your processes. So much time is spent manually entering the same information over and over again in your systems. By creating silos of security domains can makes sense in some architectures, simplifying these structures cannot be overlooked. Having a good identity management structure could give you tremendous leverage in having a self-service front end. An example of this would be access to company literature that you want control of who accesses your systems. Manually entering this data does not make sense, but having the user enter the data does. You could also direct them to a use policy statement before logging in. Streamlining this process is another way of leveraging you identity management.

Integrated workflow

This is the final area concerning user management. Having your business rules seamlessly integrated with your identity management process makes perfect sense. Having the ability to generate request, fulfilling transactions, and monitoring it through the system based on business rules helps on better flow, tracking of work request and reporting. Hopefully it will also streamline the process. This is where corporation with development staffs needs to be engaged early in the identity management process. Having a list of upcoming projects that need user information would be critical in the development stage. It also could help in speeding up the development effort. Knowing what user's rights, privileges, and access are will save huge amounts of time and effort in the development process. Integration will be key in user consolidations.

Tool Selection

In this section I will not be evaluating any particular vendor, but describe some of the tool offerings and capabilities of the tools on the market today. The first aspect of any tool selection will be based how you authenticate and authorize your users. Most tools perform this category but some things to remember. Make sure that the tool you choose meets your environment, not only from an Operating Systems standpoint but also, from a Policy and Procedure one. You will need to compliment and enforce your company security policies. Another piece to this puzzle is where will your users perform authentication, will it be only on your intranet, do you have a web presence, with web enabled user authentication, what external entities will be accessing your data. Depending on these answers will greatly affect your decision on the tool you bring in. Beware of vendors that only perform a narrow piece of the authentication and authorization model. Some vendors are just using the buzzword "Identity Management" to have you look at their tool. Speaking of web-enabled systems, look for products that can securely maintain your data infrastructure, is Single Sign On (SSO) a big initiative or not. Administration, functionality and ease of use will also play a big role in your selection. Get the biggest bang for your buck. Lastly, look for tools that have extensive logging and historical reporting. Having this data will be invaluable to your Security Team. Hopefully, these criteria's will help you in your selection.

Summary

Hopefully you will have a better understanding of what Identity Management is. Having Corporate "Buy In" and upper management support are critical for a successful implementation. Having written and defined policies that are enforceable are also critical. Ensuring that your procedures make sense and are followed is key. Assigning the corporate data stewards will ensure that only the authorized individuals are accessing those resources. Having a solid architecture when establishing your identity source will streamline efficiencies and simplify

administration. Properly utilizing authentication and authorization mechanisms as well as administration of user accounts will also increase productivity and streamline processes. This paper was meant as on overview of the identity management process and how to securely manage users, hopefully this has stimulated additional thought processes when taking on the task of setting up identity management.

References

Perkins, Earl "Securing Identity: Part 3 - Infrastructure Versus Management" Security & Risk Strategies Global Networking Strategies 13 March 2003 URL: http://www.metagroup.com (15 May 2003)

King, Chris "Focusing Identity and Permissions Management: Introducing User Life-Cycle Management" Security & Risk Strategies Global Networking Strategies 28 August 2002 URL: http://www.metagroup.com (21 March 2003)

Microsoft TechNet "Identity Management" URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/ittasks/architect/idman.asp (24 April 2003)

Crabb-Guel, Michelle "Section Three: Policies and Procedures" URL: http://www.sans.org/resources/policies/bssi3/

Aberdeen Group. "Identity Management Systems: A Core Business Competence" September 2002 URL: http://www.aberdeen.com/ab_abstracts/2002/09/09022806.htm (20 May 2003)

Reed, Archie "The Definitive Guide to Identity Management" URL: http://www.rainbow.com/IDebook/

Hunt, Michael, "Provisioning: The Key to Identity Management" 8 March 2003 URL: http://www.itsecurity.com/papers/waveset1.htm (16 April 2003)

Muchimilli, Raj "Identity Management - A Security Framework for the Enterprise" URL: http://www.nymissa.org/documents/EYIMpesentation.ppt (03 June 2003)

The National Electronic Commerce Coordinating Council, "Identity Management" 4 December 2002 URL: http://www.ec3.org/Downloads/2002/id_management.pdf (6 Jun 2003)

Infosecurity, "Identity Management" URL: http://www.infosecurityworldonline.com/identity_management.aspx (20 June 2003)

Last Updated: July 22nd, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor