Global Information Assurance Certification Paper

GSEC Practical Assignment Version 1.2d

Jack L. Strauss, CISSP 20350

The Use of Intrusion Detection Technologies in Corporate Information Security Policy Implementation and Enforcement

Abstract: The implementation and use of information security technologies are having a significant impact on corporate information security trends. For the first time in many years, those reporting information security incidents are reporting more outside attacks than inside attacks on corporate information. Security awareness, management attention, and enforcement are among the likely reasons for this long-standing trend to change. In this paper, the author presents a practical use for intrusion detection technologies as a technical control for corporate information security policy implementation and enforcement. The definition, purpose, and structure of corporate information security policy are presented for context. A taxonomy for IT centric information security is offered to frame the discussion of intrusion detection technologies. A specific example of current intrusion detection software enforcing information security policy is presented. The impact this technology has on corporate information Due Care is touched on. And, finally, this paper closes with some ideas and considerations for ongoing research in this area.

Introduction: Information security is not new. In fact, formal methods for "keeping a secret" can be traced back to Julius Caesar. As Phil Zimmerman lyrically notes in his text *An Introduction To Cryptography* [1], "when Julius Caesar sent messages to his generals, he didn't trust his messengers. So he replaced every A in his messages with a D, every B with an E, and so on through the alphabet. Only someone who knew the "shift by 3" rule could decipher his messages….and so we begin." From those early times until now, the importance of information security has remained vital. To operate effectively and to protect the value of the corporation, businesses must understand the role of information security and information security technologies. In fact, the *2001 CSI/FBI Computer Crime and Security Survey* [2] suggests, among other things, that the long-standing trend of the overwhelming incidents of insider attacks, as opposed to attacks from outside, to corporate information *may* be changing. It further points out that unfortunately, the deployment of information security technologies alone is not stemming the general increase in reported incidents of attack and further, the survival of business organizations will require an approach to information security the embraces both the human and technical dimensions of the problem.

Information security and information security technologies are different. Information security is defined here as the totality of policies, procedures, controls and practices to ensure that the right people get the right information, and only those people. Information security is a matter of corporate posture. Every aspect of the corporation's operations impacts its corporate posture. Personnel matters, facility operation, product development, services, project management, sales, mergers and acquisitions, and many more, all require careful consideration and management as all of these areas effect the conditions under which information security is achieved, or not. At the highest level, information security is part of overall corporate risk management. Information

security technologies are (usually) automated methods by which information security policies, procedures, and practices are implemented and enforced.

Corporate posture is a matter of leadership and management. Before procedures, practices, controls or implementing technologies can be developed, put into use or acquired respectively; the corporation's leadership and management must define, document, approve, and disseminate "what" is to be done. This is the role of policy.

Therefore, we suggest a fundamental premise for sound information security is - information security policy comes first, then information security technology. This relationship may sound ridiculously simple at first. Consider, however, that most companies do not have a comprehensive cross-functionally integrated corporate set of information security policies while at the same time they have extraordinary investments in information technologies, and in some cases information security technologies. The reasons for this situation include the rate at which IT has grown, both in its own complexity, as well as the growth in the complex interrelationships of IT and corporate activities that we have come to know as E-Commerce and E-Business.

Following our fundamental premise - information security policy comes first, then information security technology – we present below the definition, purpose, and structure of corporate information security policy. A taxonomy for IT centric information security is offered to frame the discussion of intrusion detection technologies. Next we present a discussion on intrusion detection technologies and provide a sample of current commercial intrusion detection software and then an example of a specific information security policy that the software may implement and enforce. We next discuss, at a high level, the impact this technology has on corporate information Due Care requirements. And, finally, this paper closes with some ideas and considerations for ongoing research in this area.

Information Security Policy: Comprehensive information security policies are part of an overall corporate risk management strategy. The information security policy documents, in plain English, the business processes and information contents and flows that require security and/or integrity measures. They are documented references to management decisions and commitment to Due Care.

Development of information security policy becomes confusing when policy writers attempt to imbed an inappropriate level of detail. Charles Cresson Wood, in his work *Information Security Policies Made Easy* [3] writes, "Policies are mandatory and can also be thought of as the equivalent of an organization-specific law. Policies are distinct from, but similar to "guidelines," which are optional and recommended. Policies are higher-level requirement statements than "standards," although both types of management instructions require compliance. Policies are distinct from and considerably higher-level than "procedures", which are specific operational steps or methods that workers must employ to achieve a certain goal. Policies are also different from "controls" (also known as "countermeasures," "security measures," and "safeguards"), which is a device or a mechanism used to regulate or guide the operation of a machine, apparatus, or system."

Organizing, managing, and disseminating information security policies in a cross-functional environment becomes difficult when there is no, or weak, structure to the policy set. The

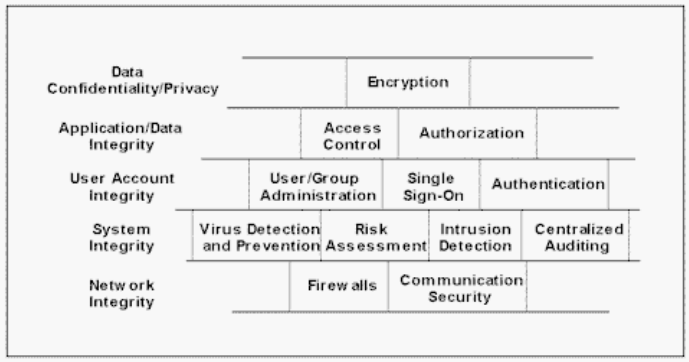
SafeCorp℠ *Information Security Policy Development Process* [4] utilizes a straightforward organization to what otherwise would result in an ad hoc collection of policy statements:

General Policies
Data Handling Policies
Physical Security Policies
Human Resource Policies
Information Systems/Technology Policies
Product Development Policies
Special Operations Policies

The General Policies section is intended to document executive management concerns. This is the section that establishes and charters the company's information security team as well as establishing management's intent and commitment to "Due Care". The other sections provide policy related to specific functional areas within the company. Note that within this structure, the policy document will provide high-level guidance for the more detailed areas such as Information Systems/Technology and Product Development. Each of those areas have specific detailed policies, procedures and controls that will be coordinated with and through the information security team.

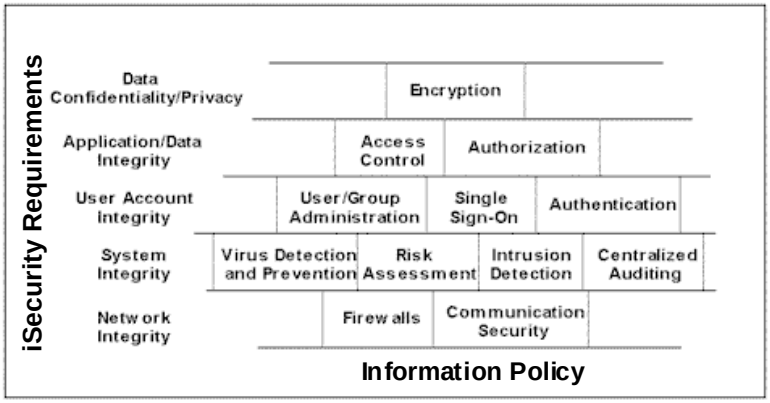
These more detailed policies, procedures and controls provide a separate challenge. The products, operation and language of information technology are complex. It is necessary to define terms and provide organizational structure to this area. To that end we provide the Information Technology (IT) Security Taxonomy in the next section of this paper.

IT Security Taxonomy: In order to provide clarity in the computer security product marketplace, The Hurwitz Group, in the paper *The Market Taxonomy for Distributed Security Management* [5], have developed and published a useful taxonomy for organizing the discussion of IT product application. Motivated by the fragmented and application specific solution space, The Hurwitz Group presents the IT security product space as shown below:



This taxonomy attempts to group IT solutions into the five areas of Network Integrity, System Integrity, User Account Integrity, Application Integrity, and Data Confidentiality/Privacy. Where: Data Confidentiality/Privacy focuses on creating a persistent and portable security perimeter around data; comprised mainly of encryption technologies. Application/Data Integrity focuses on the corporate data assets and the applications that access them; comprised of access control and authorization. User Account Integrity focuses on management of access points; comprised of user/group administration, single sign-on, and authentication. System Integrity focuses on security of individual systems, databases, and applications; comprised of virus detection and prevention, risk assessment, intrusion detection, and centralized auditing. And Network Integrity focuses on the integrity of the external security perimeter and is comprised of firewalls and communications security.

This is as good an IT product organizational device as any in the literature and we will adopt it for the IT focused portion of this discussion. To extend this taxonomy into an Enterprise-level solution space, we add the foundational layer of the Information Policy and *i*Security Requirements as shown below. As described in the section above, the Information Policy documents, in plain English, the business processes and information contents and flows that require security and/or integrity measures. The *i*Security Requirements facilitates a systems engineering approach to requirements compliance and traceability.



Intrusion Detection: As depicted above, Network Integrity focuses on the integrity of the external security perimeter and is comprised of firewalls and communications security. This can be thought of as the first line of defense. System Integrity focuses on security of individual systems, databases, and applications. Comprised of virus detection and prevention, risk assessment, intrusion detection, and centralized auditing, this area provides the second line of defense.

Specifically, Intrusion Detection (ID) technology attempts to monitor, assess, and determine "unauthorized" behavior within the system. Once the unauthorized behavior is detected, ID technology logs the behavior (using internal functionality or working with other auditing technologies), then the ID system "may" cause action to take place to stop the unauthorized behavior. This latter functionality is sometimes referred to as Intrusion Prevention, depending on the action taken.

Unauthorized behavior within a system is essentially anything you don't want the system to do. It usually takes the form of repeated attempts at passwords, attempting to gain certain system privileges, executing arbitrary commands, running specific software, and consuming computing resources leading to denial of service. The logging feature is required for post event analysis and possible evidence gathering in case of a malicious attack.

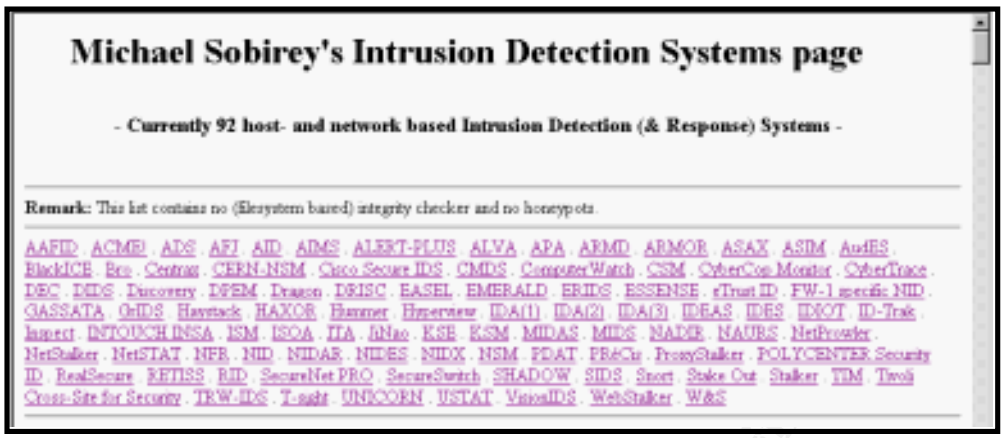
ID technologies have been developed to monitor the host computer on which they run (Host-Based ID Systems) while other systems have been developed to monitor network traffic between host computers (Network-Based ID Systems). Host-Based systems often are tightly coupled to the operating systems of their hosts and attempt to detect malicious behavior directly. Network-Based ID systems attempt to deduce behavior based on the content and format of the data on the network.

Further, certain ID systems are adaptive, while others are signature-based. Adaptive ID systems (A-IDS) attempt to monitor the system or network and given certain heuristics or expert input, identify or learn what "normal" traffic is and then "alert" on abnormal traffic. Signature based ID systems (S-IDS) are designed to compare traffic and/or "state" data against predetermined patterns or "signatures" and then "alert" on those conditions. There are relative advantages and disadvantages to both approaches.

A-IDS promise self-learning and complete customization. In practice, however, A-IDS require great expertise in the installation and running of these systems. In fact, these systems form the foundation of most of the advanced research into ID Technologies in general. This research is primarily government funded. Robert Durst, et al, in their paper titled *Testing and Evaluating Computer Intrusion Detection Systems* [6], present current, ongoing research efforts hosted by the U.S. Air Force.

S-IDS are generally simpler and are the current focus of most commercial product developments. These systems work very much like virus scanner and detection systems. They use predetermined patterns and sequences, which have come to be known as exploits. These systems are generally faster and don't generate as many false positives because they know exactly they are looking for, the predetermined patterns. However, like virus scanners and detectors, they can't detect something they don't know about and require constant update of the signature database to remain effective or even useful. Advanced products using stateful technologies, that is, understanding content flow and not just isolated patterns are continuing to emerge and provide a more sophisticated approach. They too required updates and maintenance of the signature databases to remain effective.

There are a growing number of ID systems available. Below is a sample of a website that tracks ID development projects and ID Products (http://www-rnks.informatik.tu-cottbus.de/~sobirey/ids.html) [7].



Michael Sobirey's Intrusion Detection Systems page

- Currently 92 host- and network based Intrusion Detection (& Response) Systems -

Remark: This list contains no (filesystem based) integrity checker and no honeypots.

AAFID . ACME! . ADS . AFI . AID . AIMS . ALERT-PLUS . ALVA . APA . ARMD . ARMOR . ASAX . ASIM . AutoIS . BlackICE . Bro . Centax . CERN-NSM . Cisco Secure IDS . CMDS . ComputerWatch . CSM . CyberCop Monitor . CyberTrace . DEC . DIDS . Discovery . DPEM . Dragon . DRISC . EASEL . EMERALD . ERIDS . ESSENSE . eTrust ID . FW-1 specific NID . GASSATA . GriDS . Haystack . HAXOR . Hummer . Hyperview . IDA(1) . IDA(2) . IDA(3) . IDEAS . IDES . IDIOT . ID-Trak . Inspect . INTOUCH INSA . ISM . ISOA . ITA . JiNao . KSE . KSM . MIDAS . MIDS . NADIR . NAURS . NetProwler . NetStalker . NetSTAT . NFR . NID . NIDAS . NIDES . NIDX . NSM . PDAT . PR4Cs . ProxyStalker . POLYCENTER Security ID . RealSecure . RETISS . RID . SecureNet PRO . SecureSwitch . SHADOW . SIDS . Snort . Stake Out . Stalker . TIM . Tivoli Cross-Site for Security . TRW-IDS . T-sight . UNICORN . USTAT . VisualIDS . WebStalker . W&S

ID technologies do not assume an outside attack. In fact, unless the ID system is built into a router or firewall, the operational assumption is that the Firewall perimeter has already been breached, or, that the attack is from the inside. This is a fundamental and an important feature as the system privileges granted to legitimate users generally provide direct access to sensitive information or critical system resources. Further, users of corporate assets may configure or change configurations of systems and unknowingly violate corporate policy or create system vulnerabilities.

A closer look at two commercial offerings provided some interesting examples of the general technology. Note, the author does not intend this paper to be a formal product evaluation. *NetProwler* [8] from Axent (now merged with Symantec) is a Network-based S-IDS utilizing a novel (patent-pending) Stateful Dynamic Signature Inspection technology to enable users to design unique attack definitions. NetProwler agents dynamically accept only those attack signatures associated with the OS and applications that are being defended. A Host-Based S-IDS, *entercept* [9] from entercept, Inc. (formerly ClickNet) provides unique, kernel coupled, agent based detection and control features capable of preventing unwanted actions rather than reacting to events that have already occurred, like many products on the market. Further, and most important to this discussion, is the ability to administer the product using a security policy paradigm that makes the relationship to corporate information security policies very straightforward. This feature is key as most of these products will stay abreast of attack methods and signatures as a normal course of business, or they will go out of business. The security policy paradigm used to administer *entercept*, facilitates the implementation of higher-level policies and not just focus on the attack detection and related activities.

The relationship between information security technologies to policy enforcement can be confusing because information systems administrators use the word policy at a lower level of abstraction, the control level, than do corporate information security policy writers. The information systems administrator needs to configure systems, in this case ID systems to react to each separate signature in the database (or accept a default). The activity usually requires the choice to do nothing, log the event, alert someone, and/or take some drastic action such as terminate the offending process. Each of these is called a policy by the SYSADMIN. Whereas the corporate information security policy writer may simply state, “All internet users must run their internet browser software with Java Script disabled.”

Understanding the role of intrusion detection technologies in corporate information security policy implementation and enforcement requires:

1. Understanding the purpose and structure of corporate information security policy
2. Understanding the hierarchy of information systems and some form of information security taxonomy
3. A fundamental understanding of intrusion detection technology and products
4. The desire and ability to bridge the language gap, and sometimes the technical gap between corporate information security policy writers and information systems administrators

If we understand each of the above requirements, we can then say with assurance, "intrusion detection technologies are automated methods by which information security policies, procedures, and controls are implemented and enforced. They are part of the second line of defense once and if the primary security perimeter has been breached. ID systems do not assume the attack or misuse comes from outside the company allowing for control implementation regardless of the origin of the attack or misuse. I can use ID technology to enforce *corporate* information security policy."

Policy and Implementation/Enforcement Example: As discussed above, there are at least conceptual differences in what the corporate information security policy writer and the information systems administrator mean when each uses the word "policy". To illustrate how to bridge the gap, we present the example below:

Consider the corporate information security policy, "All internet users must run their internet browser software with Java Script disabled."

The implementation of this policy can take the form of periodic security policy requirements meetings with staff and repeated requests from the systems security administrators, physical inspection and identification leading to individual default setting, and, if indicated, disciplinary action. The problem with this approach is obvious for facilities of any significant size. The period between meetings and inspections may be too long to be effective. The ability to individually spot and change browser settings is problematic since they are easy to change back. And, the manpower requirement is costly. This approach is less and less effective in relation to the size and growth of an organization.

Using ID technology, in this example a Host-Based S-IDS like *entercept*, as mentioned above, to implement and enforce this policy, the administrator, from the control console sets each host (by the use of an agent) to terminate the launch of the browser (Netscape or Internet Explorer, etc.) upon reading default settings and finding Java Script enabled. This prevents a browser that is in violation from even running. The policy is implemented, and more importantly, enforced directly.

This approach eliminates several of the problems with the physical inspection approach. The period of inspection is irrelevant as each machine implements the policy directly every time the browser in launched. The user can't change the default, and if they do, it won't run. Other than periodic policy administration updates, the manpower necessary is minimal. And, the solution naturally scales with the size or growth of the organization.

Impact on Due Care: Due Care can by thought of as a functional opposite of Negligence. Actually, Due Care is a legal term of art and has many subtle meanings that continue to be interpreted in the Courts. To demonstrate Due Care in an Information Security discussion, means to have the Policies, Procedures, and Controls that clearly show management direction and commitment as well as operational activities that are, at a minimum, considered "standard" in one's industry. Demonstrating Due Care is both a competitive advantage (when your competitors are lagging behind your processes) as well as a legal risk mitigation strategy.

Intrusion Detection Technologies are becoming more robust, easier to deploy, less prone to false alarms and resource consumption, more readily available for all computing platforms and networks, and less expensive day by day. It is simply a matter of time, and probably a short time before ID is considered a "standard" control technology in a Due Care sense. In fact, citing the *2001 CSI/FBI Computer Crime and Security Survey* [2] again, 61% of respondents have installed ID systems. If you are not using some form of ID soon, you had better have a real good reason why.

Further Research: Significant research in this area continues. Both government and commercial sectors have a vested interest in the improvement of intrusion detection technologies. We offer two thoughts below:

First, integration of intrusion detection technology into commercial operating environments would be made easier if ID product companies would consider, develop, and offer setup scripts that would allow the type of policy implementation and enforcement that was discussed in the example above. Windows 2000 for example has security administration features similar to this suggestion. There is great complexity, and possible liability issues for product companies to solve this problem, but the issue is so important that it should be considered.

Second, for large systems or installations a 1% false alarm (false positive) rate can generate too much data for analysts to handle. Any research leading to new techniques or refinements of existing techniques that reduce false positives will advance the ID state of the art. It is interesting to consider at what point does the ID system itself become a participant in a Denial of Service attack (as the ID system itself consumes system resources). This is something to consider when installing ID software on a host system.

About the Author: Jack L. Strauss is the President and CEO of SafeCorp, Inc. a professional information security consulting firm. Jack Strauss is an information security expert and business executive with more than two decades of experience in the design, development, re-engineering and management of complex military and commercial computer and communications systems.

Jack has a B.S. degree in electrical engineering from Loyola Marymount University and a M.S. degree in electrical engineering from the Air Force Institute of Technology. He has been designated a Certified Information Systems Security Professional (CISSP) by the Information Systems Security Certification Consortium and is expert in all ten domains of concentration. Jack is certified by the Project Management Institute as a Project Management Professional, and has extensive additional professional education in areas such as quality and productivity, communication systems development and software development. He is also the author of numerous technical publications.

Notice: All trademarks are the properties of their respective holders

References:

1. *An Introduction to Cryptography*, Phil Zimmerman, Network Associates 1990-1999; {www.networkassociates.com URL Checked 5/15/01}

2. Computer Security Issues and Trends VOL. VII, No.1, Spring 2001; *2001 CSI/FBI Computer Crime and Security Survey*, Richard Power, Editorial Director, Computer Security Institute 2001. {www.gocsi.com URL Checked 5/15/01}

3. *Information Security Policies Made Easy* version 7, ISBN #1-881585-06-9, Charles Cresson Wood, CISA, CISSP, Baseline Software, Inc. Oct. 1999. {www.pentasafe.com URL Checked 5/15/01}

4. SafeCorp℠ *Information Security Policy Development Process*, Jack L. Strauss, CISSP, PMP, SafeCorp, Inc. 1999-2001. {www.safecorp.com URL Checked 5/15/01}

5. *The Market Taxonomy for Distributed Security Management*, Hurwitz Group, Inc. 2000 {www.hurwitz.com URL Checked 5/15/01}

6. *Testing and Evaluating Computer Intrusion Detection Systems*, Robert Durst, et al, Communications of the ACM, July 1999, Vol.42, No. 7

7. http://www-mks.informatik.tu-cottbus.de/~sobirey/ids.html URL Checked 5/15/01

8. http://www.symantec.com (Product formerly from AXENT), URL Checked 5/15/01

9. http://www.entercept.com (Company formerly ClickNet) URL Checked 5/15/01

Last Updated: July 25th, 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
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
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event