Global Information Assurance Certification Paper

Internal Security in a Engineering Development Environment

GIAC Security Essentials
Certification (GSEC)
Practical Assignment
Version 1.4b

Option 1 - Research on Topics
in Information Security

Submitted by: Art M. Homs
Location: Boca Raton, Florida

September, 2004

Organizations that design, develop, test, and support IP based products present unique security challenges in a converged services network. In an ideal scenario, engineering labs where these activities take place are insulated from the corporate environment to prevent interactions that can compromise corporate network confidentiality, integrity, and availability. From a business point of view it is often difficult, if not impractical, to maintain the level of isolation that will ensure secure and reliable operation while mitigating risks. This paper examines some of the critical security issues and some of the tradeoffs associated with securing corporate network resources in engineering organizations while following practices that enable the efficient pursuit of business objectives.

Table of Contents

List of Figures

1 Abstract/Summary

Organizations that design, develop, test, and support IP based products present unique security challenges in a converged services network. In an ideal scenario, engineering labs where these activities take place are insulated from the corporate environment to prevent interactions that can compromise corporate network confidentiality, integrity, and availability. From a business point of view it is often difficult, if not impractical, to maintain the level of isolation that will ensure secure and reliable operation while mitigating risks. This paper examines some of the critical security issues and some of the tradeoffs associated with securing corporate network resources in engineering organizations while following practices that enable the efficient pursuit of business objectives.

2 Introduction

Developing and/or test IP based products as part of the corporate business model creates internal security risks that are distinct from those prevalent in other industry sectors that do not have engineers creating IP based products that are typically vulnerable and could potentially be exploited in their early developmental stages.

The need to test and interwork these products with external vendors and business partners (BP) over the internet creates the requirement of providing network connectivity to the external world (Internet) while protecting the confidentiality, integrity, and availability of other corporate resources.

In organizations that develop and test IP based products, internal networks are used not only for basic corporate access and communications functions such as file and printer services, workflow processes, database access, voice over IP, and email, but also as a vehicle to engineer, test, support, for their products. In many cases, engineering labs have the need to integrate third party products and to access vendors or external business partners, introducing concerns with maintaining the confidentiality of proprietary intellectual information.

This situation has become more prevalent as more products become IP based, and as more companies identify the need to integrate their IP products with third party vendors or partners who sometimes are competitors in other market sectors, or that compete with other product lines.

In addition, these products might inadvertently (due to initial design or implementation shortcomings) create large amounts of IP traffic that can essentially create the equivalent to a Denial of Service (DOS) attack that could adversely affect resource availability outside the engineering development zone.

Engineering lab computer systems require development and test applications normally not found on the corporate network side. The traditional method to secure the corporate network from the engineering development and lab networks has been to strictly isolate network traffic between the each other.

This paper examines the subtle (and sometimes not subtle) conflicts between security policies, business goals, engineering technical requirements, and the tradeoffs associated with securing corporate information resources while mitigating risks and the tradeoffs that are available to security professionals.

It focuses on identifying the major topology and process issues associated with networks that must support engineering development activities as well as providing suggestions on how to best secure this type of networks.

A topology that balances these concerns is suggested, and several recommendations are provided that highlight some of the major process issues associated with implementing the suggested solution.

3 IT Network Infrastructure

3.1 The Corporate Environment

In most organizations there is staff who due to the nature of their responsibilities have limited information technology needs, which are typically limited to using the network as a mechanism for information transfer such as e-mail, for database access and for documentation sharing.

From a security viewpoint, the corporate environment is characterized by the following characteristics which allow:

1. Minimal conflict between business goals and security policies.
2. Standard client OS and application templates.
3. Consistent client policies.
4. Uniform IP and subnet asignments (DHCP/fixed)
5. Controlled external business partners access (if at all)

In the corporate network environment, information security lends itself to the classical firewall model (see reference 2) which insulates the corporate network from the outside world (that is, the Internet) while controlling internal information resources via some type of role based access control (RBAC) mechanism. This holds true in converged network scenarios (see reference 1).

Typical organizational areas that exclusively require corporate network include, Human Resources, Finance, Accounting, Sales, and Marketing. The latter two organizations will have occasional special network needs for product

demonstrations and to validate interworking with customer systems when required by potential customers.

There are, of course, industry sectors such as retail, banking, and financial institutions, that have network usage requirements which are limited to the those described above since they are not directly involved in developing, supporting, and selling IP based products.

In these types of institutions, system security is more controllable and manageable not only because of the standardized , more readily characterized nature of the network traffic but also because of the consistent type of client systems, usually consisting of a standard template providing a browser, email client, and a document client suite such as Microsoft Office.

3.2 The Engineering Environment

In contrast to the corporate environment, engineers who actively develop IP based products have information technology requirements that include those identified for the corporate network zone as identified above, but that go well beyond in terms of desktop applications and network traffic demands, not only in terms of traffic but also in the types of services and ports that must be available in their network zone.

3.3 The Test and Support Environment

This zone is needed for those who require direct, remote customer support as well as having the need to test and integrate IP products with external vendors and partners.

As opposed to the widely available and open Internet, the corporate network is by definition limited to internal information and communication purposes. Most of the information, applications, and services are intended exclusively for internal use, and can therefore provide outsiders with a significant competitive advantage if they could achieve unrestricted access. Increasingly, access by external business partners (BP) to the information, services and applications is required due to the multi- vendor nature of contemporary technical projects that aim for the growing web based and/or IP based market. A particularly high risk is associated with connections to business partners who are or might possibly be in the immediate future in competition with other corporate units, or where it is impossible to rule out the possibility of the business partner entering into further cooperative deals with direct competitors, thereby allowing information from the corporate network to fall into the hands of unauthorized third parties.

In order to minimize information security risks, it is necessary to keep the number of business partner (BP) connections down to the minimum necessary, and to

employ technical solutions in line with defined security standards when setting up and operating these connections.

The Test and Support Zone is a network that is co-located but that it is physically isolated from the corporate network via a managed firewall.

In this scenario, the organization needs to, either directly or indirectly, make available resources to the business partner. Provision of these resources takes place via appropriate services that are enabled via the Engineering and test external firewall.

The task at hand is to use topological means (firewall) to satisfy the requirements on the business partner connection and also abide by existing security protection measures in such a way that prevents unauthorized access, either intentional or unintentional by either of the partners. This implies that the firewall rules and access rights given to business partners be controlled (reviewed and approved) a which in turn places the burden on the engineering groups for early identification and approval of the specific BP and of their specific access requirements.

In so doing, the relationship between expenses and potential benefits must be considered. Which characteristics of the business partner and the required resources need to be considered to minimize expenses?

They are:

1. Trustworthiness of the business partner
2. Level of required protection for the access to be provided
3. Ability to restrict services/accesa to the minimum required.

A critical component of the trustworthiness of a BP connection is the validity with which it can be authenticated. This ranges from "unknown" to "strongly authenticated". The latter means that the identity of the source can be proved using cryptographic methods and/or multiple factor authentication.

This kind of business partner can more readily be allowed access to specific resources, for instance, in the Test and Support zone environment via firewall rules or access control lists as opposed to an anonymous user which should never be allowed.

Note that a growing number of organizations that may not even develop any IP products might have the need to integrate and test a variety of IP based products as a service provider. Since this zone allows direct external access it must be considered as a security high risk and must be isolated from the corporate zone. In figure 1, access from the Testing and Customer Support zone must be blocked to the Corporate network zone. However, limited access is allowed from the Engineering zone to both the Corporate and Testing/Customer Support zones.

4 Secure Solutions and Alternatives

4.1 Network Topology

Although there exists substantial experience on how to implement secure firewall measures (see references 2, 6, 8, and 9) that protect the enterprise from external threats, documented practices for internal protection are not as prevalent.

The “Corporate Firewall” topology includes a firewall, inner and outer screening routers, VLAN switch, a proxy Internet access server, and inner, outer, and DMZ IDS sensors. Associated with this topology is a VPN switch in front of the firewall to support encrypted and authenticated external Internet access to corporate resources.

Each of the firewalls separating the corporate, engineering, and testing/support zones require:

1. Physical Security and Restricted Physical Access (NIST, reference 2).

2. The ability to respond and react to external threats 24x7 under the direction of IT and Infosec.

3. Infosec approval process for any topological or logical changes, including identifying specific protocols, ports, and specific systems.

4. Support of external auditing:
   Logging and history of configuration changes.
   Periodic audit of firewall rules.
   Reporting capabilities for the above.

5. Inclusion of IDS sensors operated by Infosec.

6. The InfoSec approval and registration of Business Partners

7. Obtaining and recording written acceptance of corporate rules for Business Partners by each BP.

8. A proxy filter to prevent inappropriate Internet web access.

9. To be included as part of the Business Continuity/Disaster Recovery plan.

10. Registration and implementation of secure web certificates for web services.

Management of the corporate network and external interfaces as well as between zones must be consistent, preferably through the services provided by one IT organization. This ensures common processes, and simplifies the operation and coordination of peripheral defenses in case of attacks, in auditing, logging, and in following secure maintenance processes.

Note that there will be a concern by the engineering groups that implementing the above processes might impact their ability to quickly react to customer demands. It would not be realistic to compare self-managed firewall response times since it does not include the review, registration, and certification processes required for compliance regardless of who the service provider is. The security compliance processes will require sufficient front-end planning by the engineering groups and their customers. This concern must be addressed by an appropriate service level agreement (SLA) that identifies the required response times.

In addition, there will be concerns from the engineering groups related to the ability to temporarily add or modify internal firewall rules to allow specific devices/services as they are required for business purposes. As part of the information security responsibilities expect requests for this type of analysis that should be undertaken on a case-by-case basis, with the intent that a longer term solution that fully complies with policies will be undertaken within a reasonable time.

The result will be that in some instances, firewall rules exceptions will be temporarily approved with the understanding that compliant alternatives will be provided within a reasonable time, without service loss and thus no impact to the business objectives.

4.2 Isolation Options

Firewalls safeguard connections between networks with differing security requirements. A firewall system is a system for coupling networks, with the purpose of protecting against intrusions or attacks by unprotected networks, e.g. when a protected internal network is connected to an unprotected external network (e.g. the Internet). In the context of this analysis, an internal firewall is used to isolate zones that have different levels of exposure to external access.

A firewall's rules and policies are implemented using appropriate hardware and software rules. This consists of several active and passive components that control communication between the connected networks and prevents unauthorized intrusion into protected areas and unauthorized resource access data via the network.

There are several categories of risk inherent in the multiple zone scenario.

These are, in order of significance:

1. Loss of corporate information due to external intrusion through the engineering or support zones.

2. Loss of intellectual (proprietary) marketing or engineering information to external parties.

3. Loss of corporate network availability due to misdirected IP test traffic (an unintended self-inflicted denial of service attack).

4. Loss of engineering or test zone network availability due to misdirected IP test traffic.

5. The introduction of network vulnerabilities by devices under development and test due to lack of security safeguards.

As depicted in Figure 1, one potential solution is to segregate each network zone using internal firewalls that prevent access and network traffic from reaching the adjacent zones. However, it is critical to understand that such a topology places the Engineering Internal Firewall in a role equivalent to that of the External Corporate Firewall, meaning that its security requirements and firewall rules are equivalent and similar process, review, and audit rules must be followed. In addition, it places the burden on the technical groups (engineering, test, customer support) of identifying not only the business partner but also the specific access requirements, including services, protocols, and resources, do that the appropriate permissions and access rules can be implemented in a timely manner.

5 Conclusions

Increasingly competitive product development pressures have substantially reduced the time to market window. In addition, customers demand turnkey systems rather than product based solutions, which in turn requires the integration of products from a variety of vendors and business partners who might also be competitors in other product lines.

These market pressures in turn require product development organizations to quickly react in developing and integrating their products in order to stay in business. This creates the need for solutions that balance the market demands with the security policies and practices.

1. **The network topology must support layered internal security zones within the organization and across physical locations as applicable.**

Figure 1 depicts three zones, the corporate network, the test/demo network, and the engineering development network.

2. **Ensure that each network zone is isolated.**

As much as the corporate firewall isolates the corporate network from the Internet, internal firewalls provide protection between the internal zones. The fact that a zone allows external access by vendors and business partners creates a significant security risk. Keep in mind that business partners usually compete in other related product line, in particular since they are typically working on the same product market sector. Non-disclosure agreements are just that, in most cases partner/competitors are the ones we are trying to keep proprietary information from.

3. **Internal firewalls must be physically and administratively protected as much as the external corporate firewall**.

Logging of information is critical.

4. **Security policies must clearly identify the resources, permissions, protocols, services, and ports that are allowed between the internal network zones.**

A firewall with few or no rules is worse than no firewall, since it provides no protection, it requires care and feeding, and gives a false sense of security.

5. **As with any security initiative, upper management buy-in and support is essential.**

On occasion there will be tremendous political pressure to relax the rules between zones due to business reasons related to business goals. It is an uphill battle to argue a potential security risk versus the certainty of immediately losing a customer or a sale. Make sure that the appropriate management understands the purpose of each major network component and the need to follow consistent processes and standard firewall rules as defined by security policies.

6. **Keep your non-disclosure agreements with vendors and business partners in order.**

By allowing multiple business partner connections directly into their network zones, organizations might be acting as a transaction broker for these Business Partners, potentially raising the issue of implied responsibility for technical confidentiality, non-disclosure, virus/worm distributions, and hacker attacks between these companies.

In order to reduce risks, access to internal corporate resources by business partners can only take place via uniquely defined paths to resources, applications and information. There is a general requirement that uncontrolled

and unauthorized access to information in the internal company network by business partners must never be allowed.

7. **Install Intrusion Detection System (IDS) sensors in key network locations** to identify security breach attempts and to monitor for unauthorized access. Figure 1 depicts key locations for IDS sensors. (Please refer to reference 3).

8. **Identify BPs and their requirements as early as possible.**

The burden is on the marketing, sales, support, and testing groups to identify and submit for review the Business partners and the specific resources that they need access to in order to minimize business impacts.

In conclusion, implementing a secure topology and the associated review and approval processes for external access to local resources is necessary to minimize security risks while allowing the development, test, and support groups to pursue organizational business objectives.

As customers look for more integrated, turn-key systems that combine multiple vendors and place greater demand on integration and compatibility testing, this business model will require the implementation of network architectures that protect critical, proprietary resources while providing vendors, customers, and business partners with the opportunity for closer and more dynamic collaboration and thus to combine their products into the solutions demanded by today's marketplace.

References

1. Polgar, Joel A., "Data Security in a Converged Network", July 2003. http://www.siemensenterprise.com/attachments/services/SIcurity_news_release_W1348.pdf

2. Wack, John, Cutler Ken, Pole, Jamie, "Guidelines on Firewalls and Firewall Policy", National Institute of Standards and Technology, January 2002. http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf

3. Desai, Neil. "Intrusion Prevention Systems: the Next Step in the Evolution of IDS" Feb 27th, 2003, http://www.securityfocus.com/infocus/1670

4. Cisco Systems Reference Guide, "A Primer for Implementing a Cisco Virtual Private Network", August 28th, 2000 http://www.cisco.com/warp/public/cc/so/neso/vpn/vpne/vpn21_rg.htm

5. Intel Networking White Paper, "IP Security: Building Block for the Trusted" Virtual Network, 1999 http://www.intel.com/network/connectivity/resources/doc%5Flibrary/white%5Fpapers/products/ipsecurity/NPD_Whitepaper.pdf

6. U.S. Defense Information Systems Agency, "Network Infrastructure Security Checklist", Version 5, release 2,1, (unclassified), June 17th, 2004 http://csrc.nist.gov/pcig/CHECKLISTS/network_checklist_v5r2-1-062504.doc

7. Quinn-Andry and Haller, "Designing Campus Networks", Cisco Press, 1998. Chapter 8, Addressing Security Issues, 171-201

8. Chapman and Zwicky, "Building Internet Firewalls", O'Reilly, 1995, Keeping Your Site Secure, 377-440

9. CERT, Carnagie-Mellon Software Institute, "Deploying Firewalls". April 20th, 2001. http://www.cert.org/security-improvement/modules/m08.html

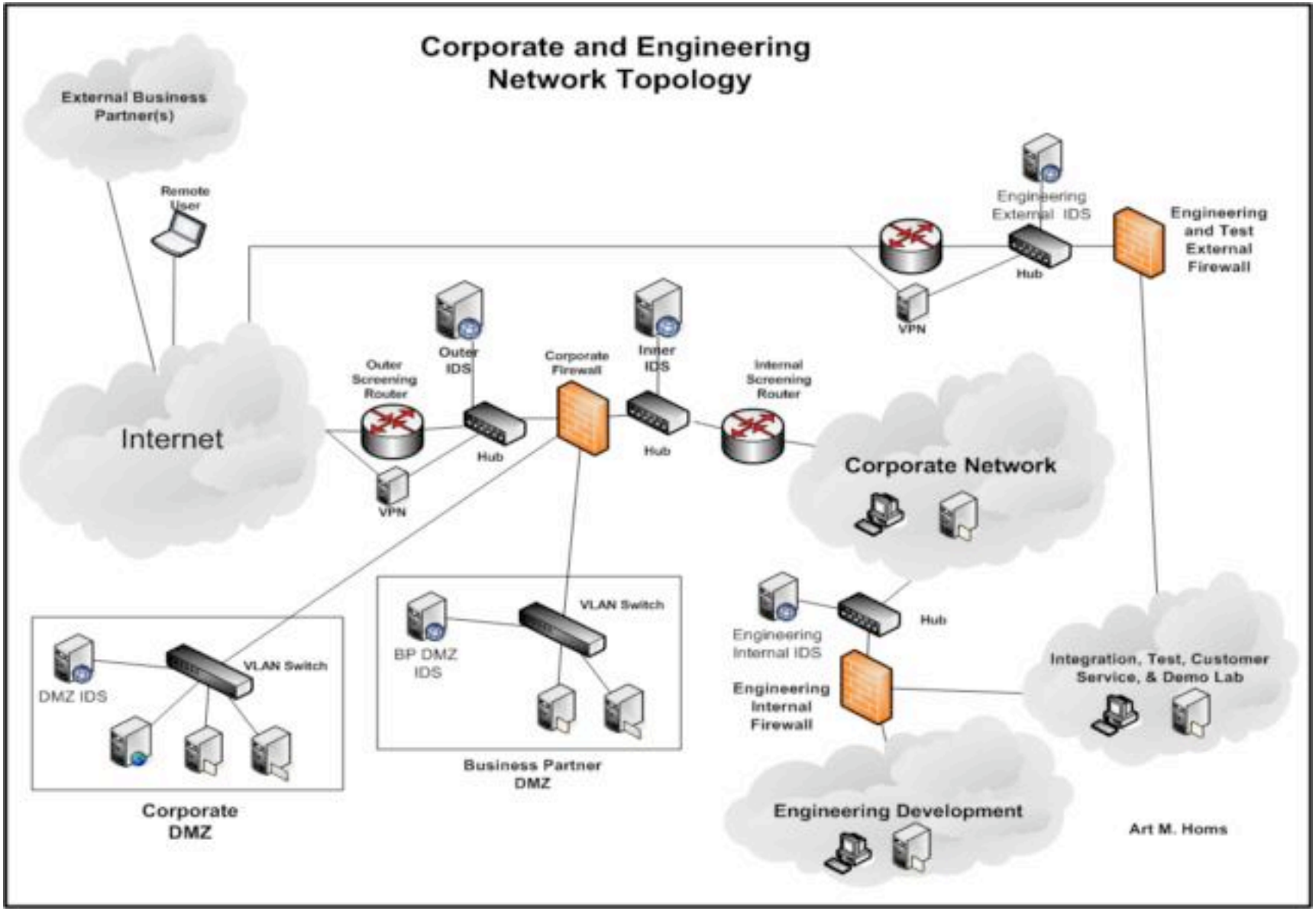
Corporate and Engineering
Network Topology
External Business Partner(s)
Remote User
Internet
Outer Screening Router
Outer IDS
Hub
VPN
Corporate Firewall
Inner IDS
Hub
Internal Screening Router
Corporate Network
Engineering External IDS
Hub
VPN
Engineering and Test External Firewall
VLAN Switch
DMZ IDS
Corporate DMZ
VLAN Switch
BP DMZ IDS
Business Partner DMZ
Hub
Engineering Internal IDS
Engineering Internal Firewall
Integration, Test, Customer Service, & Demo Lab
Engineering Development
Art M. Homs

Figure 1

Last Updated: July 20th, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
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
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 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
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
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
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
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
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
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
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 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