Global Information Assurance Certification Paper

Real-Time Security Awareness – Effectively detecting and managing security threats

Chuck Kelly

Version 1.2B

April 14, 2001

Introduction

There has been a significant amount of discussion and papers written on the concept of Enterprise Security Management (ESM). The concept is a complex one that involves connecting virtually every aspect of security together into one cohesive system. However, is this really achievable or more importantly desirable? In some large organizations, the separation of some of this technology may be warranted to achieve a more manageable infrastructure. This would allow for more rapid deployment of tools by which companies could start yielding benefits more quickly rather than trying to get their arms around one giant monolithic security system. ESM can be clearly divided into two distinct areas that include "Security System Administration" (SSA) and Real-Time Security Awareness (RTSA), which was introduced by SANS.

SSA is what we hear about most and involves managing enterprise security policies through a centralized system. This includes technologies like Single Sign On (SSO) for user authentication throughout the enterprise, user access control to network resources, password policy management, and in the case of some products system health monitoring.

RTSA is the concept of consolidating security alerts on a centralized system that allows for automated analysis and event correlation for potential security threats in real-time. RTSA enabled products would provide the security manager an overall view of what is happening across the enterprise and it would support multiple vendor security products and sources in near real-time from a central console. Consequently, the number of personnel whose time must be devoted to monitoring multiple security products and sources would be reduced. Hence the key difference between SSA and RTSA, administration and monitoring respectively.

This paper will focus on RTSA. It will discuss why the need exists for centralizing security alerts and how the systems work in conjunction with the various security systems that are deployed throughout the enterprise. It will also discuss product offerings from some of the vendors in this space and how each of them addresses this issue. And finally, we will take a look at how the industry in responding with common protocols to address information exchange between systems.

Background

The landscape of Internet security management has changed significantly over the past 15 years. When the popularity of the Internet started to increase in the early 1990's there weren't a lot of tools available to help security professionals deal with different aspects of security such as intrusion detection. Back then; most organizations developed some of their own programs to facilitate the monitoring of their network systems. In general only larger institutions had the resources available to develop applications to help fill in the gaps where existing security tools fell short.

As demand for the Internet increased so has the need for better security tools. Over the past several years, a number of companies have stepped up to the plate by bringing a whole host of products to market to help security professionals keep their systems secure. These products include Network Intrusion Detection (NID), Host Intrusion Detection (HID), network scanning packages, firewall enhancements, etc. Companies were more than eager to deploy these technologies with hope of making their networks more secure. If an organization followed best practices and adopted some form of defense in depth, chances are it deployed similar products from multiple vendors to increase the chances of detecting an intrusion. However, each time a new tool was deployed, someone from the security team had to be assigned to manage and monitor the tool. As companies continued to build out their security infrastructures, they eventually realized that there was something missing.

Security team members were soon inundated with a myriad of alerts crying out that someone was attacking their network. Most of these alerts were usually false positives but scattered in the mix were a few valid alerts. However, since none of these systems were connected to each other it was quite time consuming to verify the validity of the alerts and to correlate the alerts across multiple systems. To bring some perspective to the amount of data that needs to be processed consider the following.

According to Chris Jordan (refer to "Analyzing IDS Data" at www.securityfocus.com),

"When implementing Intrusion Detection Systems (IDS), large organizations must deal with a substantial collection of information that may be overwhelming. For example, OC-12 connections can generate about 850 megabytes of event data in an hour. How to collect and organize the incoming data is a significant issue in developing a large-scale IDS infrastructure."

When you take into account all security systems deployed in the enterprise, it is quite conceivable for a large organization to accumulate upwards to a terabyte of data over a seven-day period. How much data is kept and for how long depends on an organizations security policy. However, there is no argument that it should be kept for some period of time if the intent is to do any form of forensics after an intrusion has been detected.

Effectively managing this data is one of the major problems that most companies are facing. With hackers continually finding new ways to break into networks, chances are it is only a matter of time before they will get in. A security principle that is emphasized during SANS training is, "prevention is ideal, but detection is a must." Therefore not only is detection a must, detection must be achieved in real-time and not several hours or days after the intrusion has occurred. With each day that goes by, hackers are getting more proficient and can quickly compromise critical corporate data in a matter of minutes.

Vendors are scrambling to address this issue and some are making great strides in the development of RTSA products. Three companies are in the forefront, Internet Security Systems (ISS), e-Security, Inc., and Tivoli. Each vendor is highlighted with their respective product offering. The following information provides a brief overview of these products and the approach these vendors have taken to address RTSA. It should be noted that none of these products is perfect. All the products mentioned have pros and cons as to how they handle the concept of RTSA. However, as market acceptance gains momentum, the security community stands to benefit in the form of enhanced features and improved interoperability with third party products.

Internet Security Systems (ISS) – SAFEsuite Decisions

Company Background

Christopher Klaus (now chief technology officer) and Thomas E. Noonan (now chief executive officer) formed Internet Security Systems (ISS) in 1994. Together they launched the company's first product, Internet Scanner that Christopher Klaus invented two years earlier. The software used a revolutionary technology that could actively identify and recommend corrective actions to network security problems.

Since then, ISS has focused its attention on Internet security solutions and has developed an entire portfolio of software and services. The Atlanta-based company went public in 1998 and continues to be a recognized leader in network security management software for security assessment and intrusion detection.

Product Information

ISS's SAFEsuite Decisions (ISD) product is the company's offering in the area of enterprise security management. This product offers a report view of an organization's enterprise security and includes data analysis capabilities to help in the decision-making process.

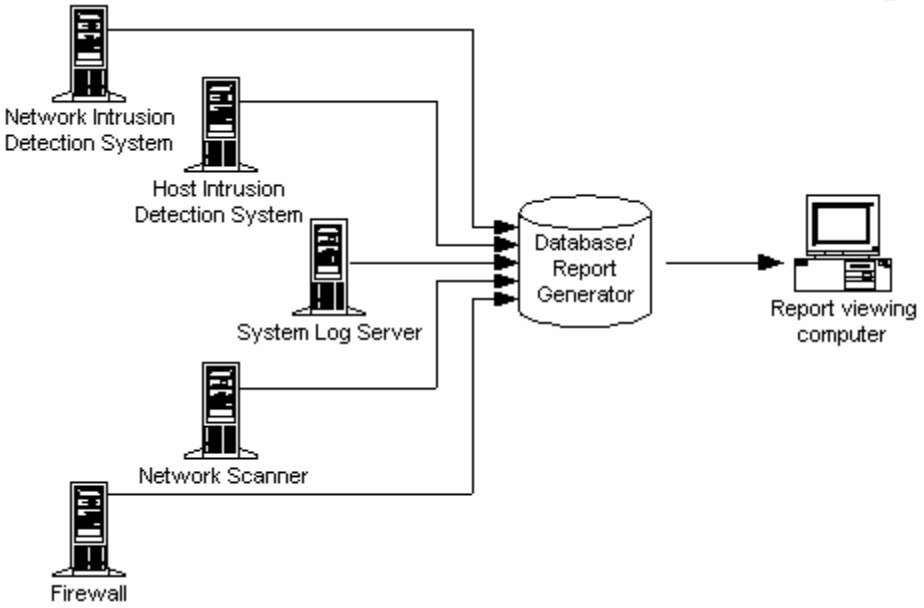
ISD is fully integrated with the company's security tools including Internet Scanner, Database Scanner, and RealSecure. The product also integrates with select third-party firewalls and intrusion detection systems. When deployed in the enterprise, ISD becomes a single source of security analysis to help security professionals identify trouble spots. Security engineers can once again focus on strategic security issues instead of data collection and analysis.

There are five main components to ISD which include:

- Reports – Over 80 predefined reports are included with the product. They are based on consolidated, correlated, and coordinated cross-product analysis of security data. Reports can be modified to meet business requirements.
- Enterprise Database – This component houses all of the security data. The product relies on a relational database product and either MS SQL or Oracle can be used.
- SAFElink – This component ensures the data is secure (encrypted) when it is communicated across the network.
- Attack and Vulnerability Exceptions – This feature allows for the user to determine if certain vulnerabilities are acceptable or expected. These

vulnerabilities can then be optionally excluded from reports that indicate risk and security condition.

- Reporting Infrastructure – This feature allows the user to run, schedule, and view the ISD reports from a UNIX or Windows NT workstation



ISS SAFEsuite Decisions Architecture Diagram

Summary

ISD has great potential. The product makes sense for companies that already have some ISS products deployed like Real Secure. The product integrates quite well with members of its own product line and also a few third party products. However, there are some issues to be aware of if you are considering this product.

- No real-time reporting –ISD leverages the data available in the SAFEsuite Enterprise Database. This database potentially contains a significant volume of data. SAFEsuite Decisions Reports analyze the contents of the database and provides actionable information based upon all of the data available. The information on the reports is as "up to date" as the information in the SAFEsuite Enterprise Database. The frequency of database loading is configurable.
- No central console/GUI to display a graphical picture of the overall security health of the network.
- ISD requires the use of at least one other ISS product to function, Real Secure or ISS Scanner. Event correlation is possible when both Real Secure and the ISS Scanner products are used. Event correlation with third party products is possible by modification of the database schema.

e-Security – Open e-Security Platform (OeSP)

Company Background

In 1996 Harris Corporation realized the growing threat of intrusions on their network management system. They decided to develop security software to combat this very issue. As a result of successfully developing and deploying this technology in house the idea to commercialize the product came about. In 1999, the resulting software solutions were purchased and enhanced for the commercial market by e-Security, Inc. Their charter was to offer the first open, integrated, and flexible security-specific software that provides a comprehensive picture of enterprise security from a single console monitor.

Product Information

The OeSP integrates the entire enterprise security environment by linking isolated resources from multiple vendors to provide a complete view of a company's security environment. The software provides a graphical representation of the security health of the network and security managers can actually see and respond to network abuse, attacks or intrusions, as well as identify, assess, and minimize vulnerabilities.

e-Security's products are fully integrated through a three-tiered architecture.

- Tier 1 - IT infrastructure, otherwise known as the event sources.
- Tier 2 - Communication infrastructure, consisting of Agents and IntellAgents.
- Tier 3 - Enterprise security management functionality, consisting of the Open e-Security Platform including the Correlation Engine and the e-Security Management Desk.

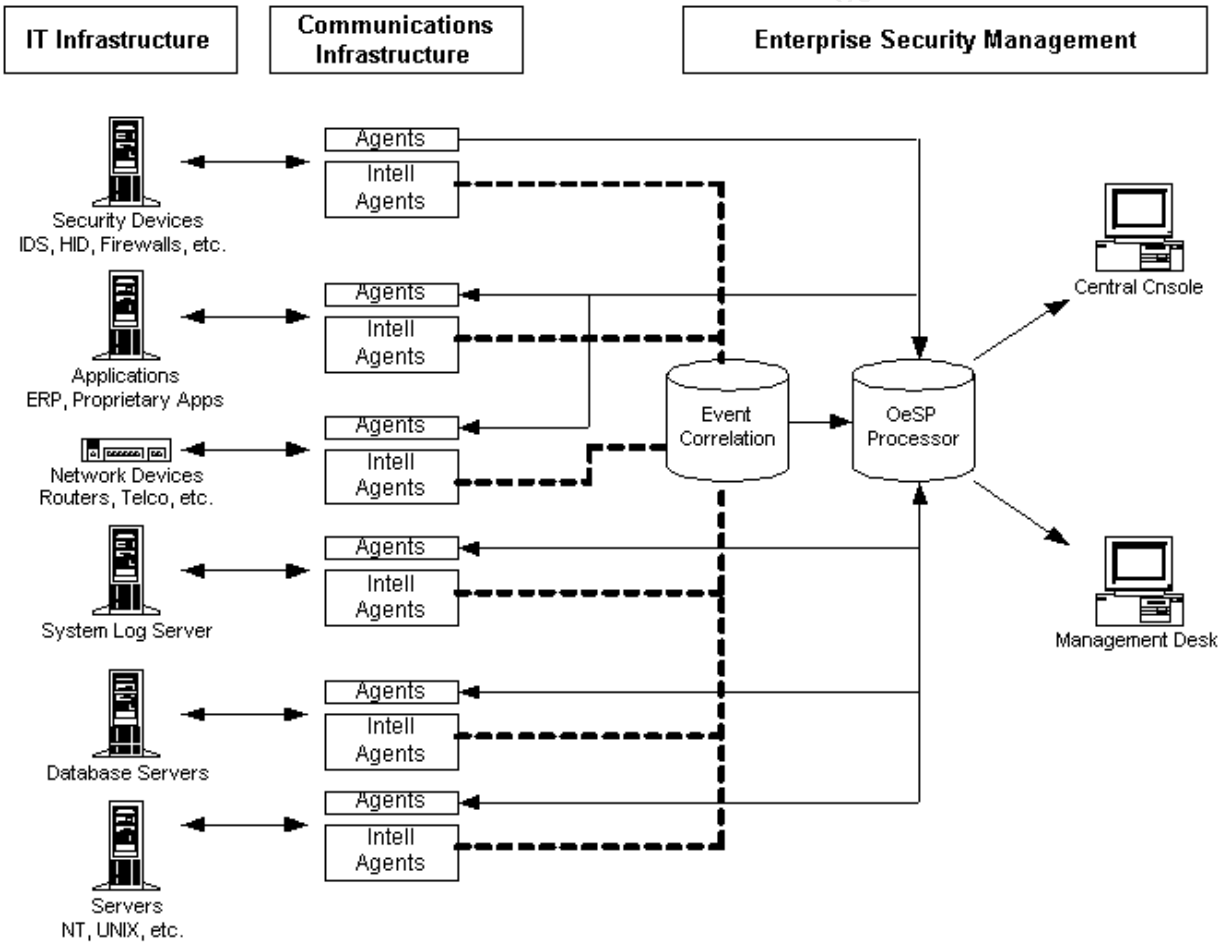
OeSP is designed so a lot of the work is done by the IntellAgents. The agents run on the security devices. They do prescreening of all events on the device as defined by a set of rules. If the event meets a certain criteria, it is forwarded on. As a result, the central processing system is only dealing with events that have already been screened. This prevents a lot of irrelevant information from getting in the way of efficient event correlation. The product also stores the data in an Oracle database and the schema can be modified based on customer requirements. Role based administration ensures that user level access can be controlled.

In addition to the OeSP, four other components are included with the product.

- e-Security Administrator Workbench (e-SAW) and Agents – The OeSP utilizes the Simple Network Management Protocol (SNMP) v1-v3 in order to communicate with devices and monitor their security related events. However, there may be devices on your network that are not SNMP enabled. For these devices, e-Security provides the e-SAW for creating e-Security Agents (SNMP proxy agents) that can monitor the device's events and convert them to SNMP to communicate with the OeSP. e-Security Administrator Workbench has a drag and drop interface that allows the user to create rule-based e-Security Agents to link to multiple security points. Options for SSL encryption ensure the data is transmitted securely.

- e-Security Management Desk (e-SMD) - The e-SMD provides Intelligent Incident Response by taking the appropriate action to intrusions based on policies and work flow procedures. Some of the options available include the selection of critical personnel, automatic analysis of the threat and risk, and the ability to measure response success against security-related service level agreements. e-SMD also has a reporting function.

- Central Console - The OeSP consoles can be displayed on any client that supports X Windows. Windows users will have to install an X Windows emulation program. Customizable views are available for the client. Alerts always flow up through aggregation to the highest-level view, while the OeSP allows the user to drill down to the view with the specific event(s).



Open e-Security Platform Architecture Diagram

Summary
e-Security's OeSP product shows great promise in the area or RTSA. In addition, the product currently integrates with more third party security products than any other vendor. By providing a GUI based development tool, custom agents could be developed rapidly which is a big plus given the dynamics of the security industry.

Tivoli – SecureWay Risk Manager
Company Background

Tivoli Systems Inc. was founded in 1989. Its focus was to help leading companies around the world reduce the cost and complexity of managing networks, systems, databases, and applications. IBM purchased Tivoli in March of 1996 but the company kept the Tivoli name and continues to be managed as a separate company. Today the company provides open, highly scalable, and cross-platform management solutions that span networks, systems, applications, and business-to-business-commerce.

It wasn't until January 2000 that Tivoli announced the creation of the Tivoli SecureWay business unit, which was tasked with providing technology for enterprise security management. One month later Tivoli SecureWay Risk Manager was announced.

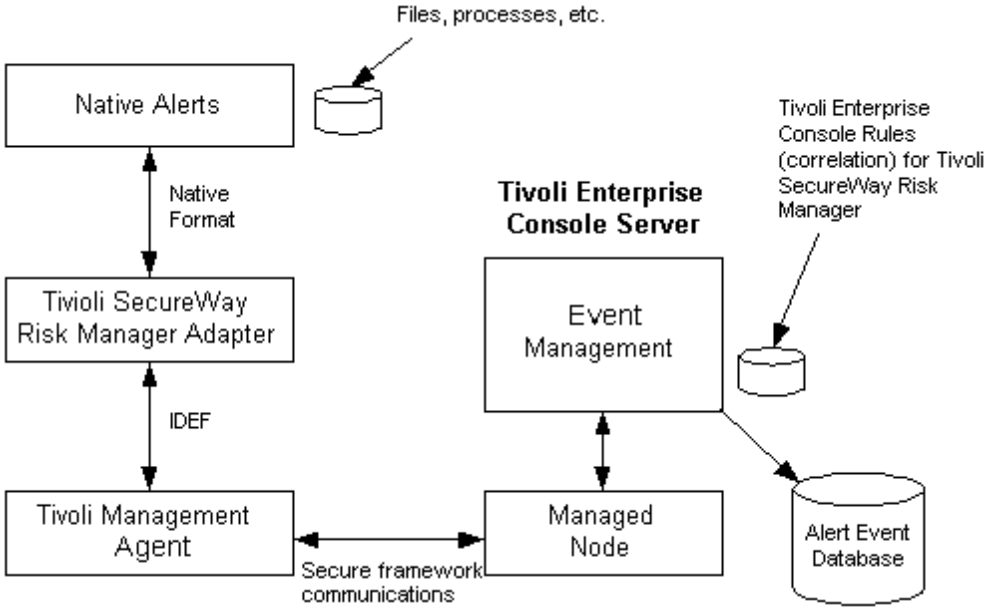
Product Information
Tivoli SecureWay Risk Manager is an open, cross platform, standards based risk management solution for the enterprise. It provides functionality that allows organizations to centrally manage attacks and threats by correlating security information from various security sensors including firewalls, intrusion detectors, vulnerability scanning tools and other security checkpoints.

The integrated security management capability enables system administrators who are not security experts to monitor and assess security risks in real-time with a high degree of integrity and confidence across an organization's multiple security checkpoints.

Tivoli SecureWay Risk Manager is an add-on to the Tivoli Enterprise Console application that leverages the event management system to manage enterprise security threats. Each of the managed technologies, such as firewalls, intrusion detection systems, routers, and hosts, has Tivoli SecureWay Risk Manager-compliant adapters, rules, and tasks that enable security analysts to manage their enterprise from a single control point.

Adapters are software processes that monitor event sources and convert the events generated from event sources into a standardized format that can be securely forwarded to the Tivoli Enterprise Console Event Server using the Tivoli Framework. An event source is anything capable of generating a security alert; such as a firewall log file or alerts generated from network and host-based intrusion detection systems.

Tivoli SecureWay Risk Manager supports the Intrusion Detection Exchange Format (IDEF) standard for alert sources to communicate event data to management systems. Standardizing on a common data format makes it easy for new event sources to leverage the distributed correlating, reporting, and decision support capabilities of Tivoli SecureWay Risk Manager. New event sources can be easily integrated by using the provided development toolkit.



Tivoli SecureWay Risk Manager Architecture Diagram

Summary

Tivoli's product offering is perhaps the most feature-rich of all three products discussed in this paper. They have had the longest run time for developing event correlation software and have successfully used that experience in the area of security. In addition, Tivoli is the only vendor of the three mentioned in this paper that is actively supporting the IDEF standards, which will be discussed next. The only issue that I have noted for this product is its limited support for third party security products. However, given the resources that Tivoli has at its disposal, this will probably not be the case over the course of the next several months. As more companies engage Tivoli consulting, more products will be integrated into their third party portfolio.

Open Standards
Several emerging open-systems standards are currently being developed in the area of intrusion detection including:

- The Common Intrusion Detection Framework (CIDF)
- The Common Vulnerabilities and Exposures (CVE)
- The Intrusion Detection Exchange Format (IDEF)

It is hoped that these standards will be finalized so more vendors will start to adopt them. Doing so will allow for better communication between various third party security systems.

Common Intrusion Detection Framework (CIDF) - CIDF enables different intrusion detection and response components to interoperate and share information. These components include:

- Sensors that generate intrusion-related information
- Analysis engines that determine whether some anomaly or intrusion has occurred warranting a response
- Response components, including network management, firewalls, filtering routers, and hosts.

Common Vulnerabilities and Exposures (CVE) - The CVE list is a dictionary of standardized names for vulnerability and other information. CVE standardizes the names for all publicly known vulnerabilities and security exposures.

Intrusion Detection Exchange Format (IDEF) - IDEF is a common intrusion-language specification that describes data formats and enables communication between intrusion detection systems and management systems.

Conclusion
We have looked at three different vendors that address the concept of RTSA differently. Since there are no official standards that have been fully embraced by the industry, it is no surprise that these vendors are somewhat autonomous in their software system designs. Hopefully the day will come when the security industry has a tool like networking currently enjoys today. HP Openview Node Manager has been a long-standing product in the area of network and systems management. It has provided the basic framework in which third party developers can build functionality using the concept of "plug-ins." The security community would benefit greatly from a tool based on a standard framework for security management. Using an industry standard, common set of protocols, the system could be expanded as needed to meet the needs of the enterprise.

References

[1] Real-Time Security Awareness (RTSA) – SANS
http://www.sans.org

[2] Deron Powell - Enterprise Security Management (ESM) (December 20, 2000)
http://www.sans.org/infosecFAQ/policy/ESM.htm

[3] Chris Jordan – Analyzing IDS Data (June 19, 2000)
http://www.securityfocus.com/announcements/126

[4] Internet Security Systems – Product: SAFEsuite Decisions
http://www.iss.net/

[5] e-Security, Inc. – Product: Open e-Security Platform
http://www.esecurityinc.com

[6] Tivoli – Product: SecureWay Risk Manager
http://www.tivoli.com

[7] Common Intrusion Detection Framework (CIDF)
http://www.isi.edu/gost/cidf/

[8] Common Vulnerabilities and Exposures (CVE)
http://www.cve.mitre.org/

[9] Intrusion Detection Exchange Format (IDEF)
http://www.ietf.org/html.charters/idwg-charter.html

[10] Network Intrusion Detection – An Analysts Handbook
Stephen Northcutt and Judy Novak, New Riders Second Edition September 2000

[11] Hewlett-Packard – Product: Openview Node Manager
http://openview.hp.com

Last Updated: May 26th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
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