Interested in learning more about security?

SANS Institute InfoSec Reading Room

Blueprint for CIS Control Application: Securing the Oracle E-Business Suite

This paper looks at how the Critical Security Controls can be used to secure Oracle's E-Business Suite (EBS), using an approach that considers application- as well as network-related issues.

Blueprint for CIS Control Application: Securing Oracle E-Business Suite

A SANS Spotlight

Written by Barbara Filkins

September 2017

Sponsored by
Onapsis

Introduction

In January 2017, Oracle's E-Business Suite (EBS) was confirmed by ERP analyst firm Panorama Consulting[1] as one of the four leading ERP packages on the market. During the same period, Oracle released a Critical Patch Update (CPU) warning of a record-breaking 121 vulnerabilities in EBS alone, 118 of which can be exploited remotely over a network without requiring user credentials.[2] That number doesn't include two issues affecting Oracle Database Server and 18 affecting Fusion Middleware, on both of which EBS depends.[3]

Critical Patch Update releases in April and July 2017 named a combined total of 608 vulnerabilities—33 of which affected EBS and 28 of which might be exploited remotely without authentication. Among them was an issue affecting all currently supported versions of EBS that could allow an attacker "to exfiltrate sensitive business data without requiring a valid user account in the system," affecting all currently supported versions of EBS.[4]

What Is Oracle E-Business Suite?[5]

EBS is an Internet-enabled platform that supports several applications, each licensed separately, allowing an enterprise to select the most suitable combination for their business needs:

- Customer Relationship Management (CRM)
- Service Management
- Financial Management
- Human Capital Management
- Project Portfolio Management
- Advanced Procurement
- Supply Chain Management (SCM)
- Value Chain Planning and Execution

The ever-increasing number of critical flaws remediated may be more a reflection of renewed attention from Oracle than limitations in the design and implementation of EBS. Nevertheless, SANS realizes how important it would be for those implementing or maintaining EBS to have solid guidelines on how to secure an implementation, especially if founded on consensus-based, open-standard security controls such as the Critical Security Controls (CSC) from The Center for Internet Security (CIS). In this paper, we will look at how the CIS Controls can be used to secure EBS using an approach that takes into account both application- and network-related issues and can be applied to other complex, standards-based solutions, as well.

[1] "2017 Report on ERP Systems and Enterprise Software," www.panorama-consulting.com/resource-center/erp-industry-reports/2017-report-on-erp-systems-and-enterprise-software [Registration required.]

[2] "Oracle Critical Patch Update Advisory," AppendixEBS, Oracle, January 2017, www.oracle.com/technetwork/security-advisory/cpujan2017-2881727.html

[3] "Oracle Critical Patch Update Advisory," AppendixEBS, Oracle, January 2017

[4] "Oracle Patches Record-Breaking 308 Vulnerabilities in July Update," *Security Week*, July 19, 2017, www.securityweek.com/oracle-patches-record-breaking-308-vulnerabilities-july-update

[5] "Oracle E-Business Suite," www.oracle.com/us/products/applications/ebusiness/overview/index.html

A Method for Control

We begin by identifying the key enterprise processes that support the CIS Controls, tailoring them as needed to establish a foundation for EBS standard operating procedures. See Table 1. This action should be based on an architecture review that includes not only the basic platform architecture but also the workflows and data structure variations demanded by the enterprise's choice of EBS applications. Figure 1 shows the steps in the approach we will be taking.

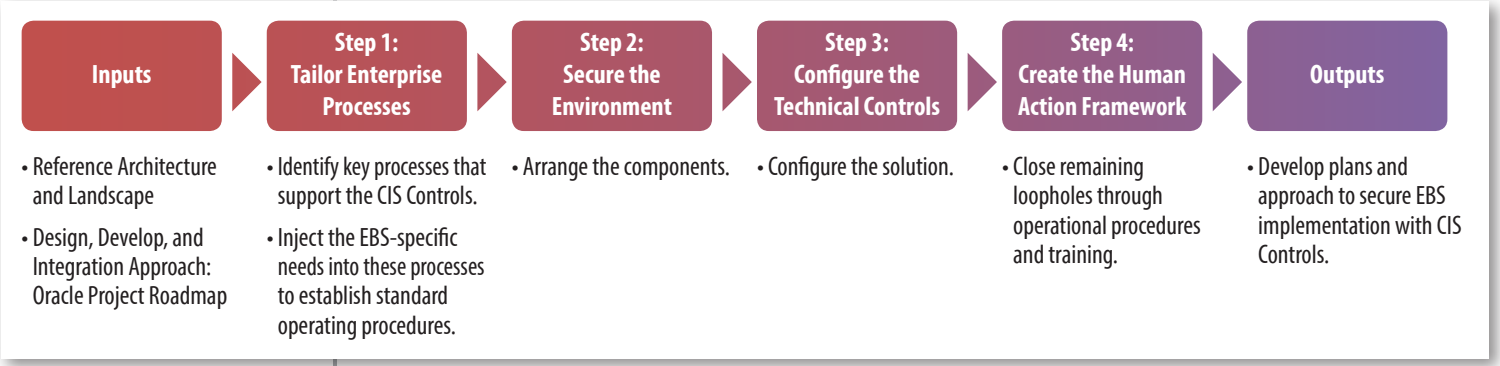

Figure 1. Approach to Applying the CIS Controls[6]

Table 1. Step One: Tailor Key Enterprise Operating Processes for EBS

Key Process	CIS Control	Description	How This Control Applies to EBS Architecture
Configuration Management (CM) and Asset Inventory	1	Inventory of Authorized and Unauthorized Devices	Define hardware and software configuration items that pertain to EBS servers, services and components. Establish and maintain an approved baseline configuration for these items through formal change/configuration management (CM) practices. (Note: Follow the security requirements laid out in the Oracle E-Business Suite Security Guide for the EBS version you use[7] and the Oracle change management processes as outlined in the Oracle Project Management Guide.) Implement automated asset inventory management tools that can also support CM activities.
	2	Inventory of Authorized and Unauthorized Software	
	3	Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	
	9	Limitation and Control of Network Ports, Protocols, and Services	Perform automated port scans against all EBS assets to establish a known effective baseline. Compare future port scans against this baseline to validate/identify changes.
Vulnerability Assessment and Patch Management	4	Continuous Vulnerability Assessment and Remediation	Run the automated vulnerability-scanning tool against all EBS servers weekly, and deliver a prioritized list of most critical vulnerabilities to each system. Correlate event logs with vulnerability scan outcomes. Implement a process that applies Critical Patch Updates to the EBS implementation, and verify correct implementation. Compare results from continuous vulnerability scanning to verify that vulnerabilities were addressed through patching, a compensating control or acceptance of a reasonable business risk. Establish a process to risk-rate the vulnerabilities based in the exploitability and potential impact of the vulnerability.

[6] "Blueprint for CIS Control Application: Securing the SAP Landscape," June 2016, www.sans.org/reading-room/whitepapers/analyst/blueprint-cis-control-application-securing-sap-landscape-37010

[7] EBS Version 12.1, http://docs.oracle.com/cd/E18727_01/index.htm; EBS Version 12.2: https://docs.oracle.com/cd/E26401_01/index.htm. Click the HTML link under the Index section near the top of the Overview section; then search the Oracle E-Business Suite Master Booklist for the specific document you need.

Key Process	CIS Control	Description	How This Control Applies to EBS Architecture
Account Management	5	Controlled Use of Administrative Privileges	Define the structure of EBS roles and responsibilities along with access requirements related to business requirements. Individual users, especially administrators, must have authorizations, privileges and access that are no higher than necessary to perform their tasks. Note: Refer to the Oracle EBS Security Guide for the appropriate release.
	14	Controlled Access Based on the Need to Know	
	16	Account Monitoring and Control	Define all roles with limited authorization objects, and assign the roles to the user. Make sure the roles are generic for job position and not tailored to an individual user. Validate that all account creation and updates are properly approved and follow the right procedures.
Auditing and Log Management	5	Controlled Use of Administrative Privileges	Focus auditing on the use of administrative privileged functions, and monitor for anomalous behavior.
	6	Maintenance, Monitoring, and Analysis of Audit Logs	Perform regular audits to ensure all users have the proper access, and avoid segregation-of-duties conflicts.
	14	Controlled Access Based on the Need to Know	Protect the EBS file system where the application and database are located with the appropriate access control. Follow the rule of "need to know." Enable audit logs for data changes, sign-on audit and session information, database connections and page access tracking.
Data Classification and Protection	13	Data Protection	Review location of sensitive data within the EBS, and define appropriate protections according to the enterprise data classification policy.
	10	Data Recovery Capability	Ensure all EBS assets are part of the data recovery plan.
	12	Boundary Defenses	Document flow patterns for all data, especially when related to sensitive information.

Environment: A Tiered Architecture

The underlying EBS platform architecture is a framework for multi-tiered, distributed computing that supports EBS applications. In this model, various servers or services are distributed among three levels. See Figure 2.

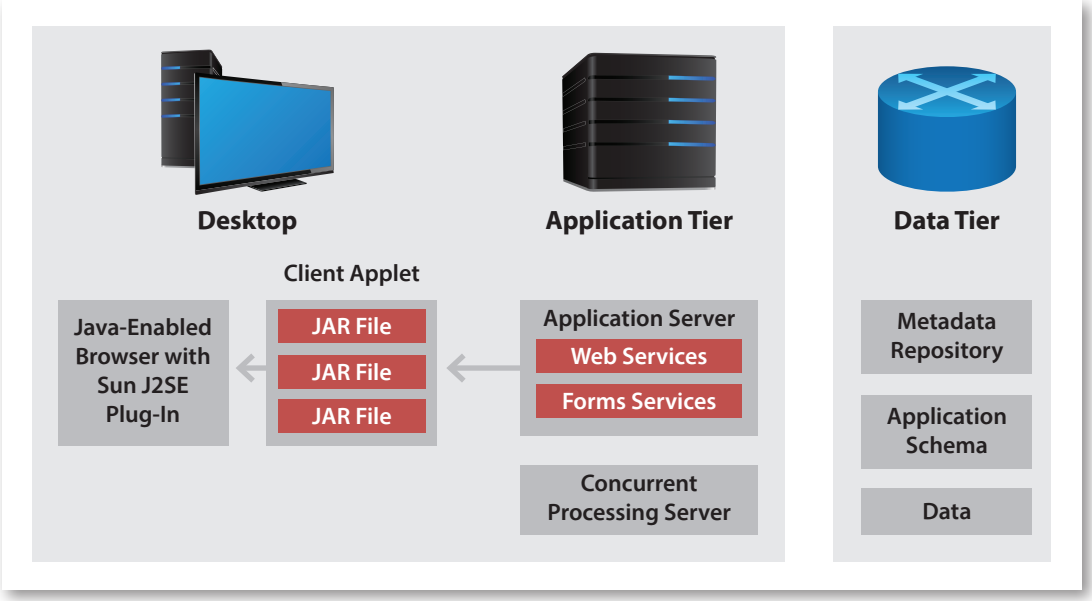

Figure 2. Oracle Reference Architecture[8]

[8] "Oracle E-Business Suite Concepts, Release 12.2," https://docs.oracle.com/cd/E26401_01/doc.122/e22949/T120505T120508.htm

The EBS platform represents a traditional three-tier architecture:

- The presentation or desktop layer presents a user interface via a standard web browser, providing a single point of access to HTML-based, forms-based and business intelligence applications within the EBS.

  Security concerns need to take into account that the client browser is Java-enabled with J2SE plug-in, communicating with the application layer through a collection of Java Archive (JAR) files. The browser will use the Oracle Java Virtual Machine (JVM) as opposed to the browser's native JVM.

- The application layer hosts the various servers and service groups that process the business logic, and it manages communication between the desktop and the database layers. It mediates all communication between the desktop and the database layer.

  This layer may also contain concurrent processing servers that offload background processes, such as long-running reports, from the main servers to allow better utilization of hardware resources, improve throughput and fault tolerance and maintain a central point of control.

- The database layer hosts the Oracle database(s), which store, process and manage all EBS data and metadata, as well as maintain EBS online help information.

Securing the Architecture

Tables 2, 3 and 4 outline the CIS Controls that are directly applied to the EBS architecture. First, in Table 2, we ensure that the overall architecture is secure, using the CIS Controls to plan our EBS security architecture. Doing so exposes only what is necessary to allow connection to Oracle servers and services within each layer, and ensures that data and application software maintain integrity.

Table 2. Step 2: Secure the Architecture

Architecture Element	CIS Control	Description	How This Control Applies to EBS Architecture
Data and Application Security	10	Data Recovery Capability	Ensure that each system is automatically backed up at least weekly, more frequently if storing sensitive information. Establish a backup architecture that ensures all files are properly protected via physical security or encryption, both at rest and in transit. Extend these protections to remote backups and cloud services if needed.
	13	Data Protection	Deploy network perimeter tools that monitor and block unauthorized attempts to access and exfiltrate sensitive data across network boundaries, while alerting information security personnel. Configure systems so that they will not write data to USB tokens or USB hard drives unless there is a valid business need for this support.
	18	Application Software Security	Comply with all EBS versions and support timelines. Implement the Web Application Firewall (WAF) for EBS. (Note: The EBS WAF is deployed in Oracle HTTP Server [Apache] and is Oracle's EBS mod_security.) Maintain separate production and nonproduction (e.g., development, test, training and staging) system environments. Ensure that the customs were developed and configured with secure code and artifacts.

Architecture Element	CIS Control	Description	How This Control Applies to EBS Architecture
Client/Browser	7	Email and Web Browser Protections	Ensure that only fully supported web browsers and Java plug-ins (i.e., Sun JRE plug-in) are used with EBS. Uninstall or disable any unnecessary or unauthorized browser or plug-in. Log all URL requests in Oracle HTTP Server.
	15	Wireless Access Control (Note: This will depend on the end users' use of wireless to access the EBS.)	Configure network vulnerability scanning tools to detect wireless access points connected to the wired network. Identified devices should be reconciled against a list of authorized wireless access points. Identify and disable all unauthorized (or rogue) access points. Ensure that all wireless traffic leverages at least Advanced Encryption Standard (AES) encryption used with at least Wi-Fi Protected Access 2 (WPA2) protection.
Server/System Configuration	3	Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	Harden file systems, programs, products and configurations according to best practices, concentrating on: • Authentication: account management, password management and other account-related activities • Authorization: restrictions to executables, data files, web pages and administrative tools • Audit: configuration, ongoing review and purging Determine the ports, protocols and services meeting validated business needs that are allowed to run on each EBS server. Configure host-based firewalls for each EBS server, and use host-based IDS to ensure consistency with network firewall(s) configuration by implementing IP restrictions at web server and database listener levels.
	8	Malware Defenses	Employ anti-malware detection across all EBS servers.

Architecture Element	CIS Control	Description	How This Control Applies to EBS Architecture
Communication and Boundary Protection (Internal and External)	9	Limitation and Control of Network Ports, Protocols, and Services	Determine whether additional protected enclaves are needed that further restrict access to the most sensitive information. Ensure consistency with server configurations, such as host-based firewalls or port filtering tools implemented on EBS servers, in laying out network boundary protections and segmentation. Deploy and operate critical services on separate physical or logical host machines (e.g., application and database servers). Strategically place application firewalls in front of any EBS server to verify and validate the traffic going to the server.
	11	Secure Configurations for Network Devices Such as Firewalls, Routers, and Switches	Implement IP filtering to help prevent unwanted access. Block all RPC ports on the router unless running NFS between networks or network segments. Implement a default OFF policy, opening only required ports. Create access control lists in **`/etc/ssh/sshd.conf`** to limit which users can connect to the local machine. Turn off unused services in **`/etc/inetd.conf`**, or disable inetd if no services require it.
	12	Boundary Defense	Use firewalls as required to secure boundaries or segment networks: • Use a firewall machine (one that filters packets or a proxy server) or a router that has firewalling capabilities between the Internet and the business intranet, as well as the intranet and internal servers. • For software firewall solutions, dedicate a machine to be the firewall. • *Do not* assume that using Network Address Translation (NAT) substitutes for a firewall. Deploy IDS sensors on EBS networks that look for unusual attack mechanisms and detect compromise of these systems through the use of signatures, network behavior analysis or other mechanisms to analyze traffic. Implement blacklists that deny communications with (or limit data flow to) known malicious IP addresses and/or whitelists that limit access only to trusted sites.

Next, in Tables 3 and 4, we provide a finer-grain implementation of the technical controls and supporting policies.

Table 3. Step 3: Configure the Solution's Technical Controls to Align with CIS Controls

CIS Control	Description	How This Control Applies to EBS Architecture
1	Inventory of Authorized and Unauthorized Devices	Detect all assets with automated discovery tools, and incorporate results in an asset management repository that can be used to maintain baseline configurations. Note: Assets include all EBS servers, including concurrent, forms, web and database servers, as well as key network devices.
2	Inventory of Authorized and Unauthorized Software	Use the whitelist feature "Allow Unrestricted JSP Access" to enable only the necessary JSP. Use the whitelist feature "Allow Unrestricted Redirects" to enable the redirects only for necessary JSP.
3	Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	Implement a baseline configuration for browsers that access the EBS. Implement a remote monitor that verifies the secure configuration elements.
4	Continuous Vulnerability Assessment and Remediation	Establish automated tools and procedures that perform continuous vulnerability assessment and remediation. (Note: See Table 1 for related processes.)
5	Controlled Use of Administrative Privileges	Minimize administrative privileges, and use administrative accounts only when they are required. Continually check which users have assigned system administrative responsibilities. Change all default passwords in EBS application and database layers. Configure the system to alert on any unsuccessful login to an administrative account, and alert after more than a certain number of unsuccessful logins by a specific end user.
6	Maintenance, Monitoring, and Analysis of Audit Logs	Validate audit log settings for each EBS server, ensuring logs include a date, timestamp and specific elements for each logged event. Ensure all systems have adequate storage space for the logs generated and that an alert is generated when log storage space runs low.
9	Limitation and Control of Network Ports, Protocols, and Services	Block unauthorized services or traffic, and generate an alert.
10	Data Recovery Capability	Configure automated backups across all EBS servers.
12	Boundary Defense	Deny communications with (or limit data flow to) known malicious IP addresses (blacklists), or limit access to only trusted sites (whitelists). Conduct periodic tests by sending packets from bogon source IP addresses into the network to verify that they are not transmitted through network perimeters.
14	Controlled Access Based on the Need to Know	Enable HTTPS for encryption following the instructions in My Oracle Support Document 1367293.1 for Oracle E-Business Suite 12.2 and My Oracle Support Document for 376700.1 Oracle E-Business Suite 12.1. In both cases, use TLS 1.2 version.
16	Account Monitoring and Control	Remove inactive accounts not associated with business processes and owners. Check that session timeout is configured in profile **`ICX_SESSION_TIMEOUT`** to be as low as possible. Configure the attempt access lockout after invalid login with profile **`SIGNON_PASSWORD_FAILURE_LIMIT`**. Profile the typical account usage by determining normal time-of-day access and access duration. Generate reports that indicate users who have logged in during unusual hours or have exceeded their normal login duration. The report information source is the sign-on audit and session information. Verify that the passwords stored in the database are hashed with a strong algorithm and accessed only with administrative privileges.

And finally, in Table 4, we make sure that these technical controls are aligned with policies, standard operating procedures and best practices.

Table 4. Step 3 (Continued): Align Technical Controls with Administrative/Management Controls

CIS Control	Description	How This Control Applies to EBS Architecture
3	Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	Establish policies on allowable browsers and secure configuration for each. Perform all the remote administration of servers over secure channels such as TLS or IPSec.
4	Continuous Vulnerability Assessment and Remediation	Document policies and procedures to support processes for vulnerability assessment and patch management as outlined in Table 2.
5	Controlled Use of Administrative Privileges	Establish policies and procedures to minimize and audit administrative privileges, and use administrative accounts only when they are required. Administrators of the system must have roles with the specific authorizations and privileges to perform their tasks.
6	Maintenance, Monitoring, and Analysis of Audit Logs	Establish requirements for EBS logging and correlation with other log sources. Develop policy and operational procedures for reviewing EBS logs on a periodic basis, using automation wherever possible. Implement tools to monitor and correlate logs to detect anomalies on EBS-related activity. Ensure that time services are consistent. Establish specific policies and procedures related to monitoring and analysis of logs.
10	Data Recovery Capability	Establish policy and practice around backups to include the following: • Automated backup schedule that is at least weekly, more often for systems storing sensitive information • Backup media tests on a regular basis by performing a data restoration process to ensure the backup is properly working
13	Data Protection	Develop a data and information classification policy that guides the establishment of network/system boundaries and specific protection requirements.
16	Account Monitoring and Control	Establish policies and procedures around account monitoring to include the following: • A process to remove inactive accounts that are not associated with business process and owner • Reports that profile the typical account usage by determining normal time-of-day access and access duration. Reports should be generated that indicate users who have logged in during unusual hours or have exceeded their normal login duration. The report information source is the sign-on audit and session information. • Procedures for password strength and integrity

The Human Action Framework

Our last step (Step 4) is to consider how to close any remaining loopholes through operational procedures and training. Several control families are directly operational in nature, and the requirements should be part of how the EBS implementation is supported:

- **CIS Control 17: Security Skills Assessment and Appropriate Training to Fill Gaps.** EBS solutions are complex, and different skills are required to properly maintain and secure each one. An organization will first need to establish different functional roles and provide the training to support roles such as EBS application and network architects, administrators and developers.

  Use security skills assessments for each mission-critical role to identify skills gaps. Use hands-on, real-world examples to measure mastery. If you do not have such assessments, use one of the available online competitions that simulate real-world scenarios. Train developers and database administrative staff in secure coding.

- **CIS Control 19: Incident Response and Management.** Incorporate EBS-specific procedures into the organization's incident response infrastructure (plans, defined roles, training, communications and management oversight). Ensure all required logs have been enabled, and consider implementing a centralized repository to collect all the logs and activity to maintain a history for forensics purposes.

  Ensure there are written incident response policies and procedures that include a definition of personnel roles for handling incidents.

- **CIS Control 20: Penetration Tests and Red Team Exercises.** Use vulnerability scanning and assessment tools as a starting point to guide and focus penetration tests.

  Conduct regular external and internal penetration tests, either white or black box, to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully.

  Use a scoring method to identify the vulnerabilities and issues in EBS. Consider the use of dynamic application security testing (DAST) at key stages in testing, roll-out and post-production monitoring.

Security in Oracle Projects

In the long run, EBS security issues are fundamentally no different from any other interconnected business system that suffers from many of the maladies that the CIS Controls, especially the first five families, are designed to mitigate.

Organizations successfully addressing these first five CIS Control families establish a strong foundation for EBS security, as well as other complex applications built around open-source platforms, with a clear growth path for maturity beyond what is a basic investment.

About the Author

Barbara Filkins, a senior SANS analyst who holds the CISSP and SANS GSEC (Gold), GCH (Gold), GSLC (Gold) and GCPM (Silver) certifications, has done extensive work in system procurement, vendor selection and vendor negotiations as a systems engineering and infrastructure design consultant. She is deeply involved with HIPAA security issues in the health and human services industry, with clients ranging from federal agencies (Department of Defense and Department of Veterans Affairs) to municipalities and commercial businesses. Barbara focuses on issues related to automation—privacy, identity theft and exposure to fraud, as well as the legal aspects of enforcing information security in today's mobile and cloud environments.

Sponsor

SANS would like to thank this paper's sponsor:

onapsis

Last Updated: November 19th, 2017

Upcoming SANS Training

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

SANS San Francisco Winter 2017	San Francisco, CAUS	Nov 27, 2017 - Dec 02, 2017	Live Event
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZUS	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Khobar 2017	Khobar, SA	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Munich December 2017	Munich, DE	Dec 04, 2017 - Dec 09, 2017	Live Event
European Security Awareness Summit & Training 2017	London, GB	Dec 04, 2017 - Dec 07, 2017	Live Event
SANS Austin Winter 2017	Austin, TXUS	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Frankfurt 2017	Frankfurt, DE	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Bangalore 2017	Bangalore, IN	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DCUS	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS SEC460: Enterprise Threat Beta	San Diego, CAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SEC599: Defeat Advanced Adversaries	San Francisco, CAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, NL	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Dubai 2018	Dubai, AE	Jan 27, 2018 - Feb 01, 2018	Live Event
SANS Las Vegas 2018	Las Vegas, NVUS	Jan 28, 2018 - Feb 02, 2018	Live Event
Cyber Threat Intelligence Summit & Training 2018	Bethesda, MDUS	Jan 29, 2018 - Feb 05, 2018	Live Event
SANS Miami 2018	Miami, FLUS	Jan 29, 2018 - Feb 03, 2018	Live Event
SANS London February 2018	London, GB	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS Scottsdale 2018	Scottsdale, AZUS	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS Southern California- Anaheim 2018	Anaheim, CAUS	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS Secure India 2018	Bangalore, IN	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS London November 2017	OnlineGB	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced