Global Information Assurance Certification Paper

Paul Mason Ford

Incident Reporting & Automation

INTRODUCTION

During recent years, the rate of scans, probes, and intrusions have been increasing at a dramatic rate. Some organizations require that these incidents be reported to various incident-handling organizations, while for others, it is part of being a responsible Internet site. This has created a situation that requires an automated method to process routine incident reports. Most of the incident reporting process can be automated, as long as proper safeguards are in place. Care has to be taken in the automating incident reporting to prevent the accidental transmission of erroneous or incomplete reports.

When our organization first started producing incident reports by hand in 1998, the incidents normally consisted of about 10 scans a day. Processing the reports by hand required on average about 10 minutes of labor for each report. This required about 90 man-minutes to process incident reports. On Mondays, the reports regarding the incidents that occurred over the weekend had to be processed, about 30 of them. This required about 5 man-hours to process these reports. At the peak, about 50 reports were being generated a day. To manually process this much data would require about 500 man-minutes (8.3 man-hours).

The solution to the increased workload was the development of an in-house application to automate most of the tasks required to generate routine incident reports. This application analyzes the intrusion detection data, filters it, performs whois and DNS lookups, and matches the data to ports known to be in use by crackers. The application does not replace human analysis or is used for the production of reports regarding systems that have been compromised. It performs most of the work without human intervention and requires only about 30 seconds for analysis and submittal per message.

IMPORTANCE OF INCIDENT REPORTING

For many years, information security specialists felt that by not sharing information about incidents, they would keep quiet the fact that problems even existed. Many businesses still have a problem with the idea of releasing negative information to the public for fear that it would draw negative attention or the value of their company would be decreased. This gave crackers the advantage. By their sharing of information, they are able to build upon each other's work and carry out more improved and dangerous exploits. By the system admins not sharing information, they were unaware that problems existed and how to correct the problems. For crackers, this created an "open season" effect on information systems.

There are numerous advantages to submitting incident reports. According to CERT, the major reasons why you should report incidents are:

1. To receive technical assistance,
2. Correlation of events,
3. Statistics collection,

4. Increased security awareness,
5. Better security documentation,
6. Organizational policy, and
7. Because you are a responsible site on the Internet.

By providing incident reports to the appropriate incident handling organizations, they can use the information to improve information security. Improvements that these organizations are providing are technical assistance on how to correct security problems and raising security awareness by alerting administrators about vulnerabilities and bad security practices. Also, some law enforcement agencies are incident handling organizations. These agencies use incident reports to start investigations that lead to the prosecution of those who launch attacks against information systems. Reporting incidents provides valuable data to organizations that work to improve information security.

INCIDENT REPORTING GUIDELINES

What and to whom do you report? The Forum of Incident Response and Security Teams (FIRST), currently has nearly 70 members. This means that you need to work with your organization to determine the proper incident handlers. As for what to include in the report, the table below lists guidelines from three major incident handlers (Carnegie Mellon University's CERT, FBI's NIPC, & DoN's FIWC):

Table 1. Incident Report Data Fields.

Item	Guidelines
Incident Reference Numbers	Provide a unique incident number for each report. Reference any other applicable incident report numbers. (CERT)
Point of Contact Information	Provide as much POC information as possible; mailing address, e-mail address, telephone numbers (voice, pager, fax). (CERT, NIPC, FIWC)
Disclosure Information	Include a short disclosure or non-disclosure statement about what data should or should not be available to others. (CERT) Information may be shared with "The Public" or "InfraGard Members with Secure Access"? (NIPC)
Physical Location	Provide address for where the system is located. (NIPC, FIWC)
Mission/Mission Critical	What is the mission of the system involved? Is the system critical to the organization's mission? (NIPC, FIWC)
Operating System & Hardware	Provide operating system and hardware information. (NIPC, FIWC)
Security Measures	List what security measures are in place; firewall, IDS, auditing, encryption, etc. (NIPC, FIWC)
How Identified	How was the attack identified? (FIWC)

Hosts Involved	Include host names and IP addresses of sources and destinations involved. (CERT, NIPC, FIWC) Also, dumping data from whois and rwhois can provide additional information.
Description of Activity	Describe the activity. Were any vulnerabilities exploited, modifications made to the system, or software installed? (CERT) Was the attack a virus, denial of service, distributed denial of service, Trojan horse, trap door, or other? (NIPC) Actions attempted. (FIWC)
Evaluation of Attack Success	Did the attacker succeed in penetrating the system? Did damage result? (NIPC, FIWC)
Classification	List classification of system. Was any classified data compromised? (NIPC, FIWC)
Log Extracts	Include log entries that are related to the incident. Remove any unrelated entries to avoid confusion. If numerous log entries exist, include a sample of the entries and the total number of entries generated by the incident. Provide a description of the format may be helpful. (CERT)
Date/Time & Duration	Provide the date, time, and duration of the incident. (NIPC, FIWC)
Time Zone and Clock Accuracy	Provide the time in GMT offset to avoid international time zone confusion. State whether the times in the log are accurate or not. If not, state the difference. If the clock is synchronized with a time source, state so. (CERT)
Any Response Expected	State whether the report is for informational purposes only or if you are seeking assistance from an incident handler. (CERT)
Corrective Action	What actions have been taken to mitigate risk; disconnect, backup, checked binaries, etc.? (NIPC)

This list shows that detailed data is requested by each incident handling organization. To properly complete an incident report regarding a compromised system, the system administrator will need to collect detailed data during the analysis of the incident. Based on this list, only scans, probes, and connection attempts that do not result in a security compromise can be handled with only a minimum amount of manpower.

AUTOMATED INCIDENT REPORTING

Using software to generate routine incident reports can greatly reduce the amount of time required, provide more accurate information, and perform more complicated data filtering. However, great care must be taken to ensure that an analyst reviews the reports and that the data used to generate the report is correct. The software solution can be a script or program that uses various standard network utilities to gather information, then

format and send reports. Our organization uses a Visual BASIC program that processes log files from the firewalls. Future enhancements will permit the utilization of data from multiple intrusion detection systems to provide more detailed data on incidents.

Automated incident reporting does NOT work in all situations. Incident reports should be manually processed if a compromised information system is involved, new network security system is brought online, or further investigation of the event is required. Investigations of compromised systems require detailed data (see Table 1) about the system involved, full automation of the incident reporting is not practical or advised. Since many intrusion detection systems base their detection on signatures within packets, many IDSs can generate false positive data. It takes time for the analyst to recognize which alerts are false positives and to adjust the configuration to reduce false positives. Automated incident reporting using data from new IDS systems is not recommended.

BEFORE sending incident reports, there are some prerequisites. First, ensure that you have accurate times on all systems. This will assist with the correlation of the data from multiple systems (hosts, network sensors, firewalls, etc.). Also, it will assist the incident handling organizations with the correlation of events from multiple sites. Second, it is important to have well-established network security systems and configurations in place. If new firewall software, IDS sensor, firewall strategy, or IDS configuration is installed, the data could contain false positives. This could be embarrassing to your organization and will cause additional work for the incident handlers. Finally, send the reports to a local e-mail address and review the reports as they would appear to the recipients. Verify that all information is correct. A week or so may be required to correct any problems that arise, do not perform testing for just a day and think that the software is working properly.

Our automated reporting system processes the data in several stages:

1. Filtering – Some incident handling organizations have guidelines on what data to report. The guideline that our organization utilizes is based on a standard provided by FIWC. The basic components of the guideline are; a) ports of interest, b) # of packets within 12 hours to a single network address space, or c) # of packets within 12 hours to multiple network address spaces. Ports of interest can be found at http://www.simovits.com/nyheter9902.html. The program performs two passes on the data to determine which sources have met the criteria for the amount of traffic and/or port of interest.
2. DNS lookups – nslookups are performed on both source and destination addresses to resolve the host names of the systems involved. The program creates a file and then shells out to use the standard nslookup utility.
3. Whois lookups – whois queries are performed on the source addresses to identify the ownership of the source network. The whois.arin.net, whois.ripe.net, whois.apnic.net, and is-1.nic.mil sites are queried. The results are analyzed to find the entry that best describes the source network.

4. Resolve protocol/ports – the program looks up the protocols and ports utilized in the incident in a file maintained by IANA. It can be retrieved at http://www.isi.edu/in-notes/iana/assignments/port-numbers.
5. Ports of interest matching – the program inserts a comment noting the ports of interest that were matched for each packet.
6. Report formatting – the data collected is formatted into the message format requested by FIWC, as shown in Figure 2 on the next page. Since an incident can produce numerous log entries, the data is summarized to the first and last twenty entries. A total of the log entries is then listed in the report.
7. Report review – once the program has formatted all of the reports, each report is displayed so that the analyst can review the information for completeness and accuracy, see Figure 1. If the analyst detects an error, it can be corrected by selecting the "Edit Report" function. This function also permits the analyst to insert additional data from other intrusion detection systems such as SHADOW or Snort. Selecting "Edit Report" brings up the report in WordPad to permit freeform editing of the message. After exiting WordPad, the program reads the modified message and redisplays it. Finally, selecting "Discard Report" skips the transmission of the report. This function is used when a false positive is detected.

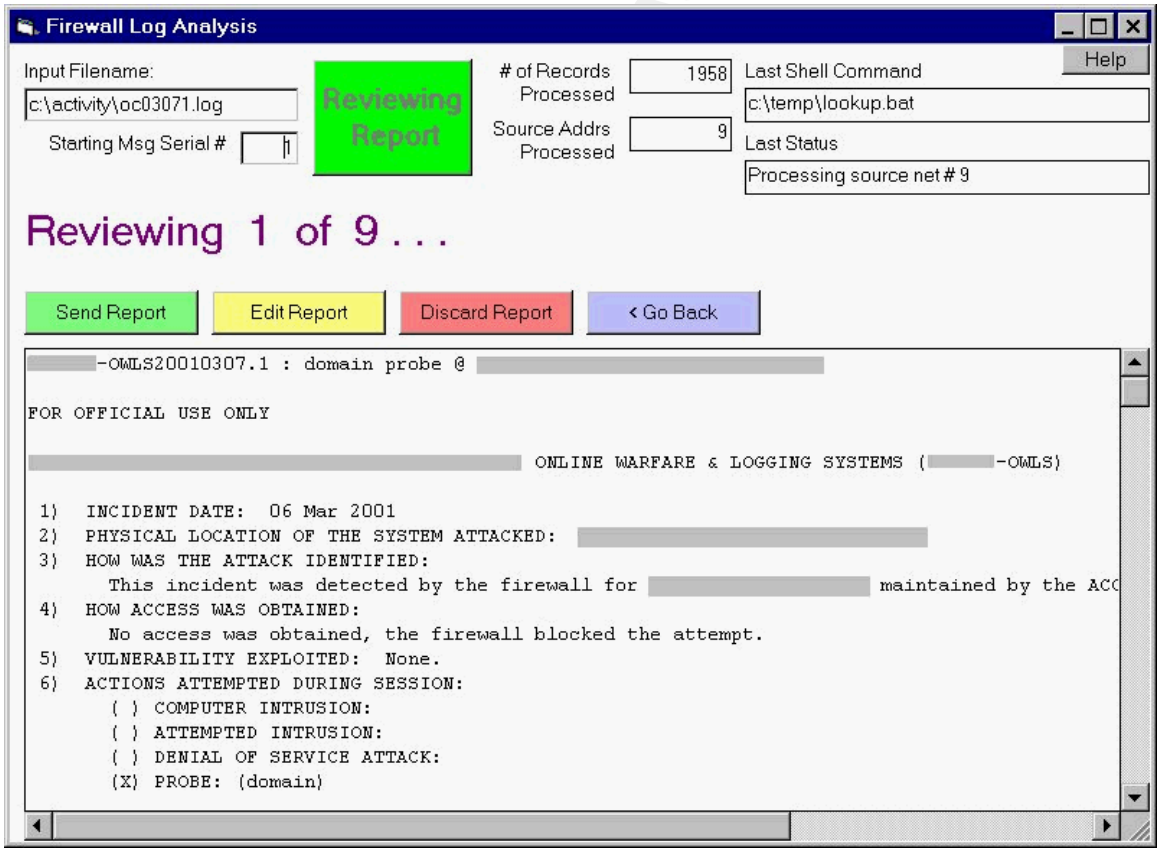

Figure 1. NetGuard Gardian Firewall Log Analysis & Incident Reporting Tool Display.

8. Report transmittal – when the analyst selects "Send Report" the incident report (see Figure 2) is sent via an SMTP program called, "Blat". This program can transmit any file in various formats via SMTP to an e-mail server. The incident report is also

formatted into HTML (see Figure 3) to increase the readability of the message that is sent to local administrators for review.

```
OWLS20010307.10 : various ports probe @ Command Name

Command Name ONLINE WARFARE & LOGGING SYSTEMS

 1)  INCIDENT DATE:  07 Mar 2001
 2)  PHYSICAL LOCATION OF THE SYSTEM ATTACKED:  Command Location
 3)  HOW WAS THE ATTACK IDENTIFIED:
       This incident was detected by the firewall maintained by the
Network Operations Group, Command & Code.
 4)  HOW ACCESS WAS OBTAINED:
       No access was obtained, the firewall blocked the attempt.
 5)  VULNERABILITY EXPLOITED:  None.
 6)  ACTIONS ATTEMPTED DURING SESSION:
       ( ) COMPUTER INTRUSION:
       ( ) ATTEMPTED INTRUSION:
       ( ) DENIAL OF SERVICE ATTACK:
       (X) PROBE: (various ports)
       ( ) OTHER SUSPICIOUS INCIDENT:
 7)  HIGHEST CLASSIFICATION OF INFORMATION INVOLVED:  UNCLASSIFIED
 8)  EVALUATION OF ATTACK SUCCESS:  Firewall blocked the attempt.
 9)  DAMAGE OR EFFECTS RESULTING FROM ATTACK:  None.
10)  HARDWARE CONFIGURATION:  N/A
11)  OPERATING SYSTEM:  N/A
12)  SECURITY SOFTWARE INSTALLED:  N/A
13)  ORIGINATION POINT OF INCIDENT:
       192.168.188.106    eu106.st188-net74.ip.com
14)  INDICATION OF ADDITIONAL ACTIVITY:
       No other traffic to the source address' network that was noted.
15)  IP ADDRESS:
       192.168.67.203
16)  NAMES USED:
       unassigned  (192.168.67.203)
17)  MISSION OF SYSTEM ATTACKED (E.G. ADMINISTRATION, COMMAND AND
     CONTROL, MESSAGE HANDLING, ETC.):  Nonexistent Host(s)
18)  POINT OF CONTACT
    A. NAME:  Network Operation Center
    B. UNIT/COMMAND:  Command Name
    C. DSN PHONE NUMBER:
    D. COMMERCIAL PHONE NUMBER:
    E. POSITION (SYSTEM ADMINISTRATOR, ISSO, ETC.):  Network System Administrator
    F. E-MAIL ADDRESS:
    G. PLAIN LANGUAGE ADDRESS WITH APPROPRIATE OFFICE CODES:
H. MAILING Address:
19)  ADDITIONAL INFORMATION (IE. LOG FILES)
Firewall Data:
Tue Mar 06 18:14:31 2001  Alert indicated in rule. Source 192.168.188.106:80, Destination
192.168.64.203:1338, protocol:6(tcp).
Port of Interest Match:  Millenium Worm
...
Tue Mar 06 18:58:04 2001  Alert indicated in rule. Source 192.168.188.106:25, Destination
192.168.65.194:2283(lnvstatus), protocol:6(tcp).
Port of Interest Match:  Hvl RAT

Total hits from source =  21

Additional Narrative:

[whois.ripe.net]
% Rights restricted by copyright. See http://www.ripe.net/ripencc/pub-
services/db/copyright.html
inetnum:     192.168.0.0 - 192.168.197.255
netname:
...
source:      RIPE

END REPORT -- OWLS20010307.10 : various ports probe @ Command Name
```

Figure 2. Sample Automated Incident Report in Text Format.

OWLS20010221.3 : unknown probe @ *Command Name*

Command Name ONLINE WARFARE & LOGGING SYSTEMS (NSWCDD-OWLS)

1) INCIDENT DATE: **20 Feb 2001**
2) PHYSICAL LOCATION OF THE SYSTEM ATTACKED: ***Command Location***
3) HOW WAS THE ATTACK IDENTIFIED:
This incident was detected by the firewall maintained by *Command & Code* .
4) HOW ACCESS WAS OBTAINED:
No access was obtained, the firewall blocked the attempt.
5) VULNERABILITY EXPLOITED: None.
6) ACTIONS ATTEMPTED DURING SESSION:
( ) COMPUTER INTRUSION:
( ) ATTEMPTED INTRUSION:
( ) DENIAL OF SERVICE ATTACK:
(X) PROBE: (unknown)
( ) OTHER SUSPICIOUS INCIDENT:
7) HIGHEST CLASSIFICATION OF INFORMATION INVOLVED: **UNCLASSIFIED**
8) EVALUATION OF ATTACK SUCCESS: Firewall blocked the attempt.
9) DAMAGE OR EFFECTS RESULTING FROM ATTACK: None.
10) HARDWARE CONFIGURATION: N/A
11) OPERATING SYSTEM: N/A
12) SECURITY SOFTWARE INSTALLED: N/A
13) ORIGINATION POINT OF INCIDENT:
192.168.8.192 local-server.carolina.com
No other traffic to the source address' network that was noted.
15) IP ADDRESS:
192.168.67.121
192.168.67.77
16) NAMES USED:
unassigned (192.168.67.121)
unassigned (192.168.67.77)
17) MISSION OF SYSTEM ATTACKED (E.G. ADMINISTRATION, COMMAND AND CONTROL, MESSAGE HANDLING, ETC.): **Nonexistent Host(s)**
18) POINT OF CONTACT
A. NAME: Network Operation Center
B. UNIT/COMMAND: *Command Name*
C. DSN PHONE NUMBER:
D. COMMERCIAL PHONE NUMBER:
E. POSITION (SYSTEM ADMINISTRATOR, ISSO, ETC.): Network System Administrator
F. E-MAIL ADDRESS:
G. PLAIN LANGUAGE ADDRESS WITH APPROPRIATE OFFICE CODES:
H. MAILING Address:
19) ADDITIONAL INFORMATION (IE. LOG FILES)
Firewall Data:
Tue Feb 20 18:39:11 2001 Alert indicated in rule. Source 192.168.8.192:88, Destination 192.168.67.121:1024(), protocol:6(tcp). Port of Interest Match: NetSpy
Tue Feb 20 18:44:03 2001 Alert indicated in rule. Source 192.168.8.192:88, Destination 192.168.67.77:1024(), protocol:6(tcp). Port of Interest Match: NetSpy
Total hits from source = 2
Additional Narrative:
[whois.arin.net]
. . .
Record last updated on 11-Jul-2000.
Database last updated on 21-Feb-2001 07:13:10 EDT.
END REPORT -- OWLS20010221.3 : unknown probe @ *Command Name*

Figure 3. Sample Automated Incident Report in HTML Format.

PLANNED IMPROVEMENTS

Some organizations collect data regarding incidents from multiple sources. Firewalls, routers, SHADOW, Snort, ISS RealSecure, VPN gateways, and host systems can provide additional data about incidents. One method to collect the data into a central location is using syslog. The version of syslog that our organization utilizes, Kiwi's Syslog Daemon, permits data to be passed to an external program and database. The next major version of the automated incident reporting software will use the database to perform queries to extract the data collected from multiple systems from the database. This will permit even more detailed information regarding incidents without requiring additional personnel.

CONCLUSION

Reporting incidents to incident handling organizations permits them to provide better solutions to information security problems. Automating incident reports for routine scans, probes, and attacks that do not result in a system compromise permits more information to be sent to incident handling organizations with a minimum of human intervention. Also, with the increasing number of incidents, automating the reports reduces the data to a manageable level. This permits the analysts to concentrate on improvements to information security systems and practices. Automated incident reporting does not replace detailed analysis and reporting when a system compromise is suspected.

Works Cited

"Cyber Incident Reporting Guidelines". National Infrastructure Protection Center. Federal Bureau of Investigations. Online. 5 March 2001. <http://www.nipc.gov/incident/cirr.pdf>

Ford, Paul M. "NetGuard Guardian Firewall Log Analysis & Incident Reporting Tool." Version 1.6.0. Chugach Telecommunications & Computers, Inc. Software. 7 March 2001.

"Incident Reporting Guidelines". CERT Coordination Center. Online. 5 March 2001. <http://www.cert.org/tech_tips/incident_reporting.html>

Neal, Mark, et el. "Blat for Windows". Version 1.8.5b. Software. 13 March 2000. <http://www.interlog.com/~tcharron/blat.html>

"OPNAV Instruction 2201.2: Navy and Marine Corps Computer Network Incident Response". Chief of Naval Operations, US Department of the Navy. 3 March 1998. <http://neds.nebt.daps.mil/Directives/2201_2.pdf>

"Ports used by Trojans." von Braun Consultants and Simovits Consulting. Online. 7 March 2001. <http://www.simovits.com/nyheter9902.html>

"Port Numbers." Internet Assigned Numbers Authority. Online. 7 March 2001. < http://www.isi.edu/in-notes/iana/assignments/port-numbers >

Ross, Andrew. "Kiwi's Syslog Daemon". Kiwi Enterprises. Version 6.2.4. Software. <http://www.kiwi-enterprises.com/>

Last Updated: August 17th, 2017

Upcoming Training

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
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
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 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
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS New York SEC401**	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
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
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
Community SANS Omaha SEC401	Omaha, NE	Oct 23, 2017 - Oct 28, 2017	Community SANS
Community SANS New Orleans SEC401	New Orleans, LA	Oct 23, 2017 - Oct 28, 2017	Community SANS
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive