GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

An Introduction to the Computer Security Incident Response Team (CSIRT) Set-Up and Operational Considerations

Author Tom Campbell, CISSP, ABCP
Date Submitted March 2003
Practical Requirements GSEC v.1.4b

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Table of Contents

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Abstract

The socio-economic environment of today is evolving and becoming more security conscious. People are taking an increasing number of steps to ensure their safety and security and, demanding the same of organisations in both government and industry. These changes in turn are being echoed in demands of information technology security. People are demanding that their personal information that is being processed, transmitted, or stored electronically be done so securely. The demands are being recognized by government and industry alike and are beginning to be reflected in the forms of laws and business practices.

Threats and vulnerabilities, in one form or another, will likely always affect information technology. Organisations will need to continually identify where they are at risk and find ways to mitigate it. However, preventative actions are not always foolproof. As such, methods of detection must be put in place to identify when a compromise has taken place. Response activities, in turn, need to be established to deal with these detections. This is where the need for a Computer Security Incident Response Team (CSIRT) becomes more apparent.

A Computer Security Incident Response Team (CSIRT) is one of the best ways to bring together the expertise necessary to deal with the wide range of possible computer security incidents that can arise. This paper will introduce the reader to the CSIRT and what is required to build and operate one.

The paper will define and explain the need for a CSIRT. The paper will go on to introduce the possible roles and responsibilities, requirements for construction and operation and the possible organizational structure of a CSIRT.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Background

Before discussing Computer Security Incident Response it is a good idea to take a minute to see how and where it fits into the whole computer security picture. First and foremost is to define exactly what constitutes computer security.

Computer Security

Computer Security:

Computer security is the preservation of the confidentiality, integrity and availability of all information that is processed, stored and transmitted using a computer.

Confidentiality is the property that information is made available or disclosed only to authorized individuals, entities or processes. Integrity is the accuracy and completeness of information and assets and the authenticity of transactions. Availability is the accessibility of systems, programs, services and information to authorized users when needed and without undue delay.

Computer Security can be divided into four operational categories:

- Prevention Operations;
- Detection Operations;
- Response Operations; and
- Recovery Operations.

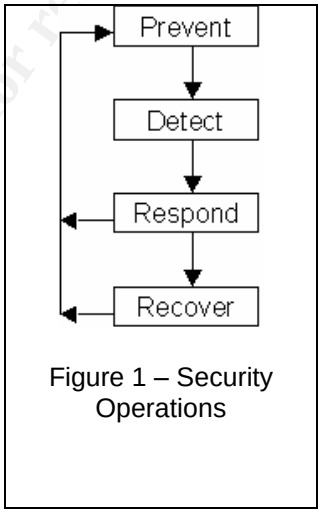

Figure 1 – Security Operations

Preventative Operations

Preventative operations are all the activities performed to prevent the compromise of the confidentiality, integrity and availability of all the information that is processed, stored, and transmitted using a computer. Prevention activities range from creating an information security policy to conducting user training sessions to implementing technical solutions such as access controls or firewalls.

Detection operations

Detection operations are all the activities performed to detect the compromise or attempted compromise of the confidentiality, integrity, and availability of all the

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

information that is processed, stored and transmitted using a computer Detection activities range from compliance inspections to whistle-blowers to implementing technical solutions such as Intrusion Detection Systems or Integrity Assurance Software.

Response operations

Response operations are all the activities performed to respond to the compromise or attempted compromise of the confidentiality, integrity, and availability of all the information that is processed, stored and transmitted using a computer. Response activities range from unplugging the network cable to blocking an IP address at the firewall.

Recovery operations

Recovery operations are all the activities performed to recover the confidentiality, integrity, and availability of the information that is processed, stored and transmitted using a computer after a compromise. Recovery operations range from initiating the Business Continuity or Disaster Recovery Plan to conducting user awareness sessions to implementing technical solutions such as disk mirroring or automated backups.

Computer Security Incident

The next step is to learn what it is exactly we are responding to, and as the name suggests, we are responding to computer incidents. So let's define exactly what constitutes a computer security incident.

Computer Security Incident:

A Computer Security Incident is an adverse event that negatively impacts the confidentiality, integrity and availability of information that is processed, stored and transmitted using a computer.

Although they may not always be readily apparent, a computer incident has the following characteristics:

- The attacker or attack origin;
- The tool used;
- The vulnerability exploited;
- The actions performed;
- The intended target;
- The unauthorized result; and

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- The attack objective.

Categories and Types of Security Incidents

The following table from the Incident Cost and Modelling Project, outlines some possible categories and types of security incidents.

Category	Types
Service Interrupts	- Denial of Service - Mail Bomb - Ping Attacks - Multiple Request Attack - Root Compromise - Packet Floods - IRC Bots - Virus Infections
Computer Interference	- Port Scans - System Mapping - System Probe
Unauthorised Access	- Identity Theft - Unauthorised Release of Data - Theft or Modification of Data
Malicious Communication	- Threats - Hate Mail - Harassment Mail - IRC Abuse - Flaming directly to Individual
Copyright Violation	- MP3 - Warez: Sites - Video Copyright - Content Violation
Theft	- Physical Theft of Hardware and Peripherals - Theft of Software - ID Theft - Credit Card Theft - Password Theft
Commercial Use	- Unauthorized Commercial Activity
Unsolicited Bulk Email	- Spam - Chain Mail - Mass Mail

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Other Illegal Activities	- Child Pornography

Table 1 – Categories and Types of Incidents[1]

Computer Security Incident Response

With a computer security incident defined, it is fairly easy to then define computer security incident response.

Computer Security Incident Response:

Computer Security Incident Response is the set of activities performed in response to a Computer Security Incident.

Now, hopefully with a better understanding of how and where Computer Security Incident Response fits into the whole computer security picture, it is time to look at the Computer Security Incident Response Team.

© SANS Institute 2004, Author retains full rights.

[1] Committee on Institutional Cooperation. Incident Cost and Analysis Modelling Projects (ICAMP) II.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Defining a CSIRT

CSIRT Defined

A Computer Security Incident Response Team (CSIRT) is a prearranged group, comprised of personnel with expertise from various facets within an organisation, prepared to deal with the response activities related to computer security incidents for a defined constituency.

It is important to note that for the purpose of this paper, prevention activities are not the responsibility of the CSIRT, though in some organisations this may not be the case. In addition, detection and recovery activities are not the direct responsibility of CSIRT but are not entirely removed from its operation.

CSIRT Acronyms

A CSIRT can go by other names and acronyms including but not limited to:

Acronym	Name
CIRT	Cyber or Computer Incident Response Team
CERT	Cyber or Computer Emergency Response Team
CIRC	Cyber or Computer Incident Response Capability
CERC	Cyber or Computer Emergency Response Capability
SIRT	Security Incident Response Team
SERT	Security Emergency Response Team
SIRC	Security Incident Response Capability
SERC	Security Emergency Response Capability
IRT	Incident Response Team
ERT	Emergency Response Team
IRC	Incident Response Capability
ERC	Emergency Response Capability

Table 2 – CSIRT Acronyms

CSIRT Goal

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The overall goal of the CSIRT is to maintain the security service triad of confidentiality, integrity, and availability to electronic information and information technology assets in response to computer security incidents.

CSIRT Objectives

The objectives of the CSIRT are:

1. Define the incident response policies, procedures and services provided.

2. Create an incident reporting capability.

3. Handle the incident:
    a. Identify the incident;
    b. Contain the incident; and
    c. Eradicate the incident.

4. Recover from the incident:
    a. Determine the cause of the incident;
    b. Repair the damage; and
    c. Restore the system.

5. Investigate the incident:
    a. Identify the cause;
    b. Collect evidence; and
    c. Assign blame.

6. Assist in the prevention of a reoccurrence of the incident.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The Need for a CSIRT

Computer Security Incident Response is not an option. No matter how well protected an organisation is there is no such thing as zero risk, even with trained personnel, proper technology and tested procedures. It is impossible to accurately and consistently, predict the type, frequency or severity of attacks. Vulnerabilities are published at an ever-increasing rate and as the complexity of technology increases, so does the likelihood that the number of vulnerabilities will in turn. The nature of computers and networking is increasing the initial threat base and introducing new motivations and capabilities that did not previously exist. The result is that computer security incidents will occur.

There is an entire security operational phase dedicated to detection. Numerous detection mechanisms including technological, human, and procedural exist and are often employed but it is of little sense to put intrusion monitoring and detection mechanisms in place if there is no plan to deal with the intrusions when they occur.

Benefits

There are numerous benefits spanning various quantifiable and qualifiable categories that the existence of a CSIRT provides to an organisation. Benefits include such areas as:

Economic

The existence of a CSIRT often reduces the amount of staff and staff time required to handle an incident compared to not having a CSIRT. This translates to less time required by the incident handlers to manage the incident and reduces the amount of lost productivity of the workers affected by the incident. As the age old adage professes: time is money. The less time wasted handling incidents the less spent on the costs of the incident handlers and the smaller the loss to productivity. This is all in addition, of course, to lost revenue, cost of damages and any insurance deductible.

Public Relations

News of incidents can severely damage an organisation's reputation but efficient handling minimises potential for negative exposure. The existence of a CSIRT demonstrates that an organisation is taking the responsibility of incident handling seriously. In addition, a CSIRT will usually have communication procedures in place to deal specifically with communicating the proper information to the proper audiences. This will help dispel rumours and ensure only factual information is reported to

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

audiences such as employees, the public, the press, the shareholders, other organisations or the authorities.

Legal

Legal responsibilities are changing as the industry matures that may soon place the onus on organisations to secure their networks and stop attacks originating from them as the result of an attack, also known as downstream liability. A CSIRT may become a necessity to comply with government regulations. A CSIRT will also help deal with any liability issues that may arise due to the distribution of information whether correct or erroneous on attacks involving another organisations or product vulnerabilities.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Return on Investment

The return on investment (ROI) of a CSIRT is not a straightforward or easily calculated number but just as with the return on security investment (ROSI), with a little effort it can be determined. In short, a CSIRT doesn't make money but rather focuses on reducing the losses due to the occurrence of an incident by containing, eradicating, and recovering from it as quickly and efficiently as possible. The earlier the incident is contained, the lower the chances of widespread damage. Additionally, a shorter the recovery period translates into a reduction in the amount of lost productivity.

Annual Loss Expectancy

To determine the costs of security incidents, we must first examine the Annual Loss Expectancy (ALE) of security incidents. The ALE of a security incident is the amount of losses in dollars multiplied by the likelihood of the loss occurring multiplied by the amount of times it is likely to happen over the course of a year. This gives us the calculation:

ALE of security incidents = Loss ($) x Likelihood (%) x Frequency (#)

This is where incident costing comes into play. Incident costing will be examined in further detail later in the paper. Two types of costs exist when dealing with security incidents: quantifiable costs, such as the wages of the incident handlers, and qualifiable costs, such as loss to reputation. In addition these cost categories can be divided into costs incurred responding to and repairing damages resulting from the incident and costs associated with lost productivity and non-realized revenue.

This calculation needs to be performed for each type of incident. This will help identify what types of security incidents result in the largest losses. This may be the area of focus when defining the services the CSIRT will provide.

Savings Provided by a CSIRT

Determining the savings provided by a CSIRT for a particular organization requires a little research work combined with some educated guessing. You need to build some numbers. It will require looking at how the amount of damage increases over time. With certain incidents, such as viruses, damage can grow exponentially over time. With other types of incidents damage will grow at a steady rate. What needs to be determined is difference in containment, eradication, and recovery time a CSIRT provides versus not having a CSIRT. This will calculate into the

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

savings in terms of the reduction in damage to the system and reduced lost productivity.

Cost of a CSIRT

The costs of building and operating the CSIRT need to be examined. The costs will depend on the number and types of services provided, as well as, the size of the constituency they are provided to. This will help identify which services will cost the most to provide to which constituencies. This will help focus which services should be provided and to which constituency.

Actual Savings of a CSIRT

The cost of building and operating the CSIRT for a particular service and constituency should be weighed against the overall savings it provides. This gives us the calculation:

Actual Savings of a CSIRT = Savings Provided – Cost of Building and Operating

CSIRT ROI

The ROI of a CSIRT is a calculable number, which will vary according to the services provided and the constituency they are provided to. It translates not into a positive gain for an organization but rather a reduction in the losses.

Facts and Statistics

The following list of facts and statistics is meant by no means to be all-inclusive and is merely for the purpose of further illustrating the necessity of the CSIRT within the organisation. They are of excellent use in support of a business case in favour of a creating a CSIRT.

- Over time the level of knowledge required to attack has decreased while the attack complexity and the potential level of damage has increased.
- Carnegie Mellon's CERT Coordination Centre (CERT/CC) illustrates the number of reported cyber incidents has increased from six in 1988 to eighty-two thousand in 2002.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- The time required for malicious code to spread to a point where it can do serious infrastructure damage halves every eighteen months.

- The speed with which an organisation can recognise, analyse, and respond to an incident will limit the damage and lower the cost of recovery.[2]

- Results from Computer Security Institute (CSI) seventh annual "Computer Crime and Security Survey":

  - Ninety percent of respondents (primarily large corporations and government agencies) detected computer security breaches within the last twelve months.

  - Twenty-five percent (25%) of those acknowledging attacks reported from two to five incidents. Thirty-nine percent (39%) reported ten or more incidents.

© SANS Institute 2004, Author retains full rights.

[2] CERT©/CC: Computer Incident Response Team FAQ.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Roles and Responsibilities of a CSIRT

The roles and responsibilities of the CSIRT need to be clearly outlined, and the services the CSIRT provides need to be clearly defined and understood by both the CSIRT itself and its constituency. It is essential to define services, service levels, and the constituency they will be provided to. The exact functions of the CSIRT will vary depending on the organisational resources and requirements for information protection. If resources are lacking in the requisite expertise then it may require outsourcing or funding which would require a limit to the services.

The activities performed by the CSIRT can be divided into two categories: real-time incident response activities and non-real-time incident response activities. Non-real-time incident response activities can be subdivided into pre-incident and post-incident activities.

Non-Real-Time Incident Response Activities - Pre-Incident Activities

In order for a CSIRT to be effective and successful in their response activities, a good deal of preparation is required. Issues, such as what services will be provided, to which constituency, under what authority and at what cost to whom, need to be determined prior to handling an incident. There are a number of activities that can be performed including creating a charter, policy, incident reporting procedures, incident tracking and handling procedures, and incident costing. When the legwork is handled prior to the onset of an incident, the handling of the incident is more structured and likely to have a more positive outcome. It is wise to adhere to the age old adage, “an ounce of prevention is worth a pound of cure”.

Charter

The first piece of work that needs to be tackled is writing a CSIRT project charter. The charter will address issues such as the mission statement, the types of incidents addressed, the services provided, the constituency, the authority and the funding.

The mission statement should define the core activities of the CSIRT. It should also clearly outline the overall goals and objectives. Refer to the ‘Defining a CSIRT’ section of this paper for more information on the goals and objectives of a CSIRT. In addition, it should align with your organization’s security policy.

The types of incidents that the CSIRT will address must also be outlined. Refer to the ‘Background’ section of this paper for examples of categories and types of computer security incidents.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

In addition to the types of incidents that the CSIRT will respond to, should be the actual services that will be provided for each one. It is essential that there are clearly defined services for each type of incident to eliminate ambiguity. In addition to the services that will be provided, should be the service levels that accompany them. Include the hours of operation and levels of support. Is this a 24-7 capability or are incidents handled with one service level during working hours and another service level for evenings and weekends?

Next is the issue of the constituency. To whom will these services be provided? For small organisations this may not be an issue, but for large organisations a perimeter will need to be established based on boundaries such as:

- Geographical location;
- Organisational Group or Division; or
- Organisational function.

The next issue that the charter should address is that of authority. The CSIRT authority must be granted from management and clearly outlined in the security policy.

Finally the issue of funding needs to be addressed. Where will the CSIRT receive the budget it requires to provide its services? The services could be charged out proactively, like insurance, where in order to operate you must pay a premium, or reactively, by attempting to recover costs from the party responsible for the cause.

Policy

In order to eliminate any ambiguity that may arise, it is necessary to have clearly defined security policies, based on or in adherence to acts and laws, which map to procedures and standards. Simply stated, a policy is the rule and a standard or procedure is how to acceptably perform the process or function in adherence to the rule.

The first step is to research the laws of the country or region in which the organisation is operating. It is good idea to refer to legal counsel for input. Any policy an organisation writes, whether a security policy or not, must adhere to these. In addition, the organisation policies must comply with industry regulations. International and multinational organisations need to consider the legal and cultural differences of the areas in which they operate.

The main policy of importance with respect to incident response is the security policy. A complete security policy should address topics such as, access to information, information storage and disposal, and communication. If they are

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

not currently addressed in the security policy, they will need to be addressed prior to or during the construction of the CSIRT. Other policies, should they exist within the organisation, include the incident reporting policy, which should encourage an open reporting environment, and include the incident response policy, which should differentiate between human error and malicious intent.

The legal department should review all policies prior to putting them in place. With respect to the computer incident response policy, the legal department should be consulted at the very least on the liability issues. Issues of importance include downstream liability, liability of the distribution of information, and liability due to monitoring. Downstream liability deals with when a compromised computer damages another computer. Liability due to the distribution of information, whether the information was correct or erroneous, includes activities such as distributing information on an attack involving another organisation or publishing product vulnerabilities. Liability due to monitoring, deals with whether you must inform users of monitoring or any changes in monitoring practices.

Incident reporting procedures

In order for a CSIRT to respond to an incident, there must be a mechanism in place to notify it that an incident has, is, or will occur.

The first step is to determine a Point of Contact (PoC) responsible for the coordination of receiving reports and notifying the CSIRT.

Reports can be received from a number of different sources, both human and non-human, Incident may be reported in the real or non-real time review of logs from an Intrusion Detection System (IDS), an Intrusion Prevention System (IPS) or Firewalls. Employees of affected systems may report an incident or symptom of an incident. Whistleblowers may report something they have witnessed or heard. Outsiders, such as other affected organisations or, in some cases, the attackers themselves, may report the incident.

In order to ensure the efficient and timely notification of the CSIRT, accurate and up-to-date contact Information should be kept. The primary method of contact should be indicated and the CSIRT contact information should include:

- Telephone number;
- Facsimile number;
- Electronic mail address;
- Web site;
- Mailing address; and
- Additional information:
  - Operating Hours;
  - Time zone; and

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Team members.

Incident awareness and incident reporting awareness programs should be engaged. Users should be made aware of symptoms that may constitute an incident and encouraged to report incidents without fear of reprisal.

Some of the possible symptoms of an incident are listed in the following table, which has been divided into two categories obvious and discrete:

Obvious	Discrete
Web Defacement	New, modified or deleted User Accounts
Unauthorized access	New, modified or deleted files
	System Crash
	Anomalies
	Suspicious or unexplained activity

Table 3 – Incident Symptoms

Incident information tracking and handling procedures

In order to maintain control over all the information regarding the incident and reduce any possible confusion, it is a good idea to create an incident ticket.

Tickets must have a unique identification number. In the case of multiple tickets opened pertaining to the same incident, designate one the master and the subsequent the dependents, providing links between them.

Tickets should capture all the incident information. Everything should be documented including the date and time and where it was reported. If it was reported from a person, include their name, location, and contact information. If it was reported from an automated system, include the hardware manufacturer, operating system type and version, the name of the host, the physical location of host, the network address and the MAC address. This information should be collected for both the reporting system and affected system. Another important piece of information that should be kept up-to-date is the status.

Handoff procedures should be determined for when tickets are transferred between individuals or departments. Part of these procedures should include escalation and de-escalation procedures.

Finally track all time spent on CSIRT activities by all parities. This should be done at regular intervals to ensure accurate reporting.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Costing an Incident

Unfortunately costing an incident is not an exact science but with a little effort a reasonably accurate amount can be determined. The Incident Cost Analysis Modelling Project or ICAMP has provided some excellent insight into costing methodologies.

To cost an incident, both the quantifiable and qualifiable costs must be included. Additionally, not only do the actual losses need to be considered, but also, the lost opportunity for gains. What this means is, all other factors equal, if you have one of only two web sites that sells widgets and your web site becomes unavailable for a time period, customers are likely to purchase their widgets from the other web site. So the sales you would have normally realised during that time period, the gains, are lost or not gained.

When trying to cost an incident there are several considerations. There is the cost of damages, the cost of the wages of incident handlers and those prevented from working, lost revenue, loss to reputation and insurance deductible.

The wages of both the incident responders and those of the people prevented from working. There are a number of questions you will need to ask:

- Who worked on responding to or investigating the incident?
- How many hours did each of them spend?
- How many people were prevented from working because of the incident?
- How much productive time did each of them lose?
- How much do you pay each of those people to work for you?
- How much overhead do you pay (insurance, sick leave, etc.) for your employees?[3]

Lost revenue again deals with non-realised gains. Data can be extrapolated from the current revenue stream and compared against industry trends.

Loss to reputation is difficult to quantify but can result in the loss of current and potential clients.

Other considerations are lost contracts or bids, penalties for delays in payments or projects or lawsuits for breach of contract.

Real Time Incident Response Activities

[3] Dittrich, David A. *Developing an Effective Incident Cost Analysis Mechanism*.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Real time incident response activities deal with the actual handling and response measures taken once the incident has occurred.

First and foremost, the protection of human life and safety takes precedence over everything.

The figure below outlines, sequentially, the categorised activities performed by the different functional areas or groups during the handling of an incident. Every organisation is distinct in its structure and the division of the roles and responsibilities. Incident handling is made up of the incident identification, containing the incident, and eradicating the incident, and is handled by the CSIRT. Incident recovery includes identifying the damage, repairing the damage, and restoring the systems. The Business Continuity Planning or Disaster Recovery Team usually performs the recovery activities. The incident investigation is comprised of activities to identify the cause of the incident, collect evidence, and assign blame. The Security Team usually performs the investigative activities. The IT Security Team performs incident reoccurrence prevention. During the incident restitution activities the decision of whether to seek reparation for any damages or losses suffered needs to be decided by management with input from the legal department or legal counsel. Finally the incident communication activities, handled by a communications team, include the various internal and external communications.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

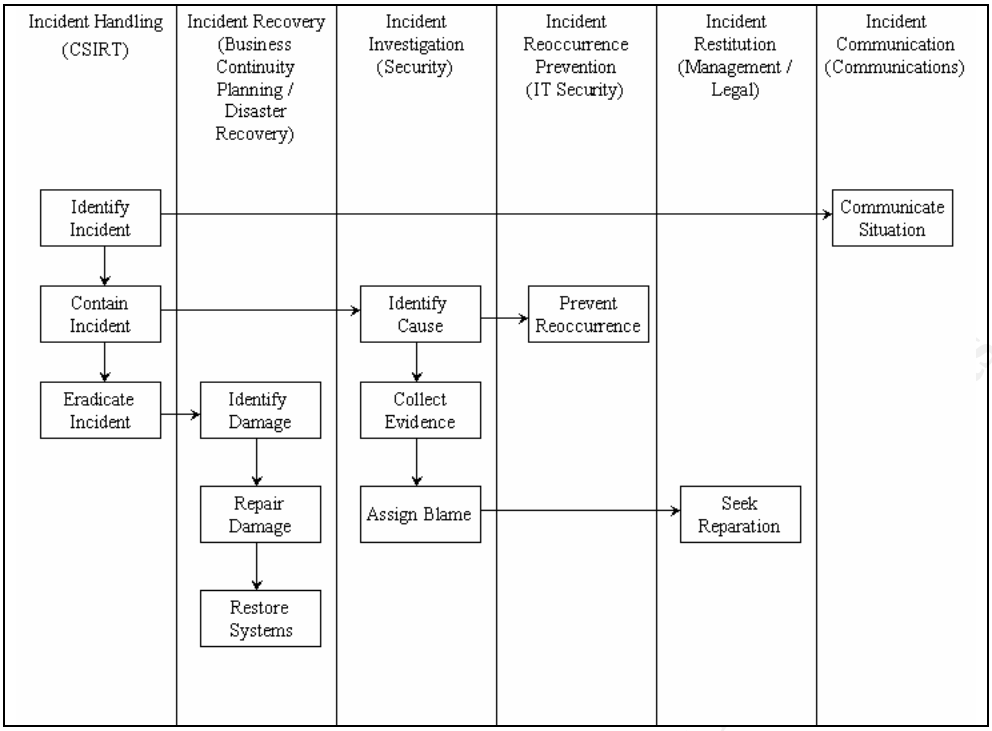

Figure 2 – Incident Response Flow

Incident Handling

The Incident Handling phase is handled by the CSIRT and is divided into three stages: identifying the incident, containing the incident, and eradicating the incident.

Incident Identification

Identifying the incident is comprised of a number of activities. The first step is to determine whether it is an actual incident or simply perceived. This requires that the incident report be verified. It also needs to be determined whether this is the first report or a duplicate report. How to handle duplicate reports should be laid out in the tracking and handling procedures.

Next, it should be determined whether it is a security incident or non-security incident to determine whether it falls under the jurisdiction of the CSIRT. The

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

types of incidents qualified as security incidents should be indicated in the CSIRT policies.

The scope of the incident needs to be determined by uncovering what has been affected.

A priority level needs to be assigned to determine the immediate resource requirements. Certain incidents, such as a virus outbreak, may need all necessary resources activated in order for it to be handled immediately to reduce the amount of damage that will occur.

Other types of incidents, such as receiving a piece of SPAM mail, will not cause immediate or widespread amounts of damage. As well, prioritising incidents will help an organisation better co-ordinate its resources if it is hit by multiple incidents simultaneously.
A simple scale that can be used to prioritise incidents is located at the right in figure 3 – Incident prioritization matrix. The factors it uses to prioritise the incidents are the level of confidentiality of the information and the severity of the damage. Both are measured using a low-medium-high scale that needs to be decided on by each individual organisation, in terms of how it will be measured.

Incident Priority Rating Matrix

Actual or Potential Damage Severity Level (1st Letter) \ Level of Information Confidentiality (2nd Letter)			
	H / L	H / M	H / H
	M / L	M / M	M / H
	L / L	L / M	L / H

L = Low
M = Medium
H = High

Figure 3 – Incident Prioritization Matrix

Once it has been verified that it is an actual security incident, the initial scope and priority assigned, it is time to activate the CSIRT. In some organisations the CSIRT is an operational team, in which case the previous steps would likely have been handled by it, and in others it is a group brought together at the time of an incident. It is absolutely essential that an up-to-date contact list be established and maintained for an emergency situation, such as an incident, where time is of the essence. Procedures should be established for the creation, maintenance, and testing of this contact list. The CSIRT contact list should include entries such as the persons job function, since in larger organisations employees may not know the name of the person to contact, as well as, their level of authority. The employee's name and contact information, including phone numbers, both office and cell, pager number, email, and any other means of contacting the individual must be included. The employee's hours of work and availability, as

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

they could be away on vacation and in both cases there may be a backup employee designated to replace him or her.

Some additional information that may want to be included on the contact list are the numbers for contacting emergency services, such as the fire or police departments or third party support providers.

Incident Containment

The purpose of containing the incident is simply to limit extent of the attack.

Temporary countermeasures should be taken should be taken appropriate to the situation. Some of these can include:

- Change network address;
- Quarantine the affected files or systems;
- Pull plug, either network or power;
- Change firewall rules;
- Increase the amount of bandwidth;
- Apply system patches;
- Monitor the system or network activity;
- Set traps; or
- Disable certain functions.

Eradicate Incident

Eradicating the incident deals with eliminating the threat from the systems to prevent it from causing further damage. Ensure all the necessary information was collected and copies were made and tested. Archive bogus files before deleting them. Correct any hardware or software bugs or configuration errors. When dealing with software, ensure the most current anti virus software is installed and operating. Clean and reformat all the infected media. When making backups, ensure they are clean.

Incident Recovery

The Business Continuity Planning or Disaster Recovery Teams are best suited to handle the recovery activities surrounding an incident. There are three stages to the incident recovery: identifying the damage that has occurred, repairing the damage, and then restoring the system. Integrity assurance software can assist in identifying subtle or hidden changes to a system. Restoring the system is simply returning the system to normal operations. The recommended recovery

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

order is critical systems first, non-critical but high demand systems second, and finally all remaining systems.

Investigation

The security team responsible for investigations should handle the incident investigation as they will have the most knowledge and experience in these situations. The three main activities include identifying the cause, collecting evidence, and assigning blame.

Identifying the Cause

Identifying the cause of an IT security incident will often require forensic analysis. Sometimes the vulnerability exploited will be obvious, other times it will require an extensive search.

Passive Techniques	Active Techniques
Logs – Network/Host IDS, FW, Apps, Email, IRC	Scan Network/Host
Monitor	Engage Attacker
Network Traffic	Interview
Host Activity	
Video Surveillance	
Phone Records	
Timecards	
Building Entry/exit logs	
Honey Pot	

Table 4 – Forensic Techniques[4]

There is wide variety of forensic tools in existence, both commercial and freely available.

When conducting an investigation there are some important actions to perform prior to shutting down host including:

- Make a list of all the processes running;
- Make a note of the status of network interface, is it in promiscuous mode;
- Make list of all the listening ports and active network connections; and
- Make copies of executable files associated with every running process on the system or dump the contents of system memory to a file.[5]

[4] Hillier, Peter, Fortier, Christian. *Cyber Incident Response*. Presentation for the 15th Canadian Information Technology Security Symposium 2003.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Collect Evidence

Computer evidence can often be divided into two types, volatile and non-volatile. Volatile evidence refers to evidence that is easily compromised or lost if not handled properly. The table below outlines some of the types of volatile and non-volatile evidence.

Volatile	Non-Volatile
Memory	Physical Equipment
Active Processes	Persistent storage
Active Network Connections	Printouts
Contents of a computer screen	Recorded Video Surveillance

Table 5 – Evidence Types

Make a bit-for-bit copy of the file system for evidence. Always remember to perform as few operations as possible prior to making the copy to maintain its integrity. Make two copies, one for forensics use and one for creating a new system disk. Finally, remove the hard drive and secure it as evidence.

It is important to preserve evidence in its original form. Record the names and contact information of all the people present and clearly detail any actions performed. Remember sometimes a picture is worth a thousand words.

Record each piece of evidence. Include a description, the location and the time it was found. For physical evidence, indicate who has handled the evidence and for electronic evidence, indicate any processing that has occurred. When the evidence has been properly recorded tag and seal it. Finally assign an evidence handler responsible for the storage of the evidence.

Take detailed notes during the investigation as they can be used in legal proceedings. Good notes will include your actions and the actions of others, when the action was taken, along with the reason for the action taken. Remember to sign and date the bottom of each page.

Assign Blame

The final step performed by the Investigative Team is to assign blame based on the evidence collected. A simplistic chart was created to assist in determination.

[5] Brezinski, Dominique, and Dittrich, Dave. Black Hat Las Vegas '00 Training Intruder Discovery / Tracking and Compromise Analysis.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Cause	Origin	Intent	Target
Human	Internal	Intentional	Direct Attack
			Indirect Attack
		Accidental	N/A
	External	Intentional	Direct Attack
			Indirect Attack
		Accidental	N/A
Non-Human	Random - Nature	N/A	N/A
	Non-Random - Initiated by Humans	Intentional	Direct Attack
			Indirect Attack
		Accidental	N/A

Table 6 – Assigning Blame

IT Security

The IT Security Team handles the incident reoccurrence prevention activities. The goal is to put a short-term solution or work-around in place to prevent the further exploitation of the vulnerability. The long-term solution that will mitigate the risk by preventing further exploitation of the vulnerability is also handled by the IT Security Team, but falls out of the context of incident response and into prevention and risk management operational processes.

Management/Legal

It is at the decision of management whether or not to seek reparation. The situation will often dictate what the best course of action is for the organization. The involvement of the authorities can lead to widespread publication of the incident and negative exposure. Legal proceedings can be lengthy and costly and management may not see adequate benefit to make these worthwhile. The legal department should be contacted in these situations to ensure any decision made is in compliance with the laws of the country or region in which it is operating.

Communications

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Communication during an incident is essential to ensure efficient and effective containment. To maintain control, the "need-to-know" principle should be observed. A communication plan must be developed. It should detail what information is to be communicated to whom, when, how and by whom.

The plan should detail precisely what information is to be communicated. Any statements made should be clear, concise, qualified, and based on substantiated facts.

The internal and external audiences that have a need-to-know should be indicated in the plan. Communication should occur with the appropriate stakeholders including the affected areas within the organisation, the affected clients or partners, the press or the authorities. It is important to realise that information communicated with audiences external to the organisation may become public.

The plan should indicate under which circumstances communication should occur. Is it for strictly informational purposes, such as status reports, or as part of notification procedures used to alert other organisations?

Additionally, the point in time that communication should take place needs to be determined. Will communication occur when an incident is declared or after it has been handled? Will communications be an ongoing process or a single occurrence?

Comment [M1]: I don't understand the sentence. "Will communications be what?"

How will communications be carried out? What communications media is appropriate, phone, cell, fax, email?

Who carries out the communications? Does a designated communications department or team handle all communications?

When creating a communication plan organisations spanning geographical areas that are subject to differing laws, such as countries, must take that into consideration.

Non-Real-Time Incident Response Activities - Post-Incident Activities

Post Mortem

An incident report should be completed at the conclusion of every incident. If possible an independent body should conduct the report. The report should detail:

- What the impact to the organisation was;

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- A chronological sequence of events;
- The incident identification information including how it was discovered, when and by whom;
- How the incident was handled;
- A list of all activities performed including personnel contacted, when, by whom and why;
- The things that were done well and those that need improvement; and
- The lessons learned.

The report is valuable for reference for similar incidents in the future, for obtaining a monetary estimate of damage, and to determine whether updates or changes to the CSIRT procedures are needed.

When completed the report should be presented to senior management to decide, with consultation and input from the legal department, whether legal action should be taken. It should also be passed to IT security to introduce preventative measures to reduce the likelihood of a reoccurrence of the incident.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Requirements of a CSIRT

In order to operate a CSIRT effectively and successfully, there is a need to add to the requirement triage of people, process, and technology, with authority and funding. Additionally, there is a need to qualify the requirements accordingly:

- Proper, up-to-date technology;
- Correct, trained people;
- Complete and tested processes and procedures;
- Defined authority and support; and
- Adequate funding.

Proper, Up-to-date Technology

The technology required to perform the CSIRT functions timely and effectively is fundamental to the successful handling of incidents. Tools for notification purposes, whether phone, cell phone, web page, email, palm pilot, or other are necessary for timely response. Forensic tools and investigative tools, including all the hardware and software need to be as advanced as possible to compete with the ever-increasing complexity of incidents and methods.

Correct, Trained People

Ensuring the CSIRT members are the right people and are properly trained is key. A CSIRT usually deals with high-stress situations and uncertain hours. Members should have personality traits that are suited for stressful and uncertain situations.

The decision needs to be made of whether CSIRT members should be made up of in-house employees or outsourced to a company providing incident response services. If the CSIRT is being kept in-house the decision of whether existing employees will be used or new employees hired specifically for the CSIRT.

Ensuring the CSIRT member's chosen receive proper training is essential to its success. Training is offered by several organisations including:

- CERT/CC - www.cert.org;
- FIRST - www.first.org; and
- SANS - www.sans.org.

It is important to dedicate a percentage of time to learning about incident trends and security technologies.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Complete and Tested Processes and Procedures

Having written plans eliminates much of the ambiguity, which occurs during an incident, and will lead to a more appropriate and thorough set of responses. A Computer Security Incident Response Policy is the basis for all processes and procedures. It is vitally important that all processes are tested regularly to determine their shortcomings, should they exist. The process to be followed during an incident should be clear and thorough.

Defined Authority and Support

The Computer Security Incident Response Policy should clearly indicate the authority granted to the CSIRT. Senior management must buy-in and support the CSIRT. There is often a degree of apprehension during an incident, causing management unrest. As well, certain areas will be forced to surrender control of their area of responsibility. The authority of the CSIRT cannot come into question during the incident, as it will only lead to unnecessary delays in the incident handling.

Adequate Funding

How the CSIRT will be funded is a vital issue. It is impossible to accurately predict either the number or severity of incidents. As such it cannot operate under a normal budget.

There are several possible methods of funding the CSIRT including an insurance model and a cost recovery model. In the insurance model all the different areas of an organisation fund the CSIRT like paying insurance. In the cost recovery model, the areas affected by the incident pay for the cost of the incident response in predetermined proportions. The insurance model can also be combined with the cost recovery model so that each area pays into a CSIRT fund like insurance and at the time of the incident the affected areas pay a deductible to offset some of the loss to the pool of money. There are many possible methods to fund a CSIRT but it is essential to predetermine how it will be accomplished.

Organisational Buy-In

Finally, to be successful, there must be a buy-in from the entire organisational. To obtain this there must be an understanding of what organisational needs the CSIRT satisfies and how it satisfies them. In addition, there should be an understanding of how the CSIRT improves the overall state of security within the

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

organisation. The key players of the CSIRT must understand the needs and benefits the CSIRT provides in order to ensure their buy-in. The key players are examined in further detail in the next section.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Areas Involved in a CSIRT

The CSIRT should be proportionally sized with respect to the organization and with the incident to ensure it has adequate personnel to perform its duty. There is a need to predetermine the chain of command for each incident type, as it may be different depending on type, or, may even change during a single incident.

Representation is suggested from, but not limited to, the following areas (Not all incidents will require representation from all the areas listed but some incidents may require representation from other areas not listed):

Area	Incident Handler Role	Function
Management	Oversight	Make decisions on issues not outlined in procedures
Information Security	Lead	Investigations
Information Technology	Support	Provide technical support as required
Physical Security	Primary	Assess Physical Damage Business Continuity Physical Property Investigation Safeguarding Evidence
Legal	Consultation	Provide legal advice when requested
Audit	Secondary	IT Audit Financial Audit
Human Resources	Consultation	Provide information with regards to situations involving employees
Communications	Secondary	Communicate with: Internal: shareholders/owner, management, staff External: press, public, vendors, law enforcement

Table 7 – Areas Involved

When choosing CSIRT members, there are certain skills and personality traits that should be sought. The most successful members are individuals who are dedicated, innovative, detail-oriented, flexible, and analytical. They are problem-solvers, good communicators and able to handle stressful situations.[6]

[6] CERT©/CC: Computer Incident Response Team FAQ.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Few organisations are either large enough or have the budget to employ a fully functional, dedicated CSIRT. As a result there are a number of courses of action.

The first is to assemble the team at the time the incident is declared. The CSIRT members must be able to drop, put on hold, or reassign their current activities in order to focus on their incident response role.

The second possibility is to have a small, dedicated CSIRT that expands with representation from the appropriate areas depending on the incident. Again all non-dedicated CSIRT members must be able to drop, put on hold, or reassign their current activities in order to focus on their incident response role.

The third course of action is to outsource the incident response role to specialized and experienced computer incident response organisations.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Conclusion

Computer Security Incident Response is not an option. No matter how well protected an organisation is there is no such thing as zero risk, even with the trained personnel, proper technology, and tested procedures. It is impossible to accurately and consistently, predict the type, frequency, or severity of attacks. Vulnerabilities are published at an ever-increasing rate and as the complexities of technology increases, so is the likelihood that the number of vulnerabilities will in turn. The nature of computers and networking is increasing the initial threat base and introducing new motivations and capabilities that did not previously exist. The result is that computer security incidents will occur.

A Computer Security Incident Response Team (CSIRT) is one of the best ways to bring together the expertise necessary to deal with the wide range of possible computer security incidents that can arise.

This paper introduced the reader to the fundamentals of CSIRT and some important considerations of what is required to build and operate one both effectively and successfully.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Bibliography

Comment [M2]: Did you follow any convention styles for your bibliography? I guess since they are all web articles, you can either alphabetically order by author or title.

1. Borodkin, Michelle. *Computer Incident Response Team.* (September 15, 2001). SANS Infosec Reading Room.
   Available at: http://www.sans.org/rr/incident/CIRT.php.

2. Brezinski, Dominique, and Dittrich, Dave. Black Hat Las Vegas '00 Training Intruder Discovery / Tracking and Compromise Analysis.
   Available at: http://staff.washington.edu/dittrich/talks/blackhat/blackhat/.

   Formatted

3. Brownlee, N., and Guttman, E. *RFC 2350: Expectations for Computer Security Incident Response.* (June 1998). Internet Engineering Task Force, Network Working Group.
   Available at: http://www.ietf.org/rfc/rfc2350.txt?number=2350.

   Formatted

4. CERT®/CC: *Computer Security Incident Response Team (CSIRT) Frequently Asked Questions (FAQ).*
   Available at: http://www.cert.org/csirts/csirts_faq.html.

5. Committee on Institutional Cooperation. Incident Cost and Analysis Modelling Projects (ICAMP) II.
   Available at:
   http://www.cic.uiuc.edu/groups/ITSecurityWorkingGroup/archive/Report/ICAMP.shtml

6. *Computer Crime and Security Survey from the Computer Security Institute (CSI) in partnership with the FBI*.
   Available at: http://www.gocsi.com/press/20020407.html.

7. Dittrich, David A. *Developing an Effective Incident Cost Analysis Mechanism*. Security Focus, June 12, 2002.
   Available at: http://www.securityfocus.com/printable/infocus/1592.

   Formatted

8. Fraser, B. RFC: *1244: Site Security Handbook.* (September 1997) Internet Engineering Task Force, Network Working Group.
   Available at: http://www.ietf.org/rfc/rfc2196.txt.

9. Hillier, Peter, Fortier, Christian. *Cyber Incident Response*. Presentation for the 15th Canadian Information Technology Security Symposium 2003.

10. Kaplan, Simone. *When Bad Things Happen to Good People.* (May 2003). CSO Magazine, csoonline.com.
    Available at: http://www.csoonline.com/read/050103/bad.html.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

11. Rhodenizer, Elizabeth. *Establishing an Information Protection Centre, Lessons Learned.* (May 2003). Paper prepared for the 15th Canadian Information Technology Security Symposium 2003.

12. West-Brown, M. J., Stikvoort, D., and Kossakowski, K. (1998). *Handbook for Computer Securirty Incident Response Teams (CSIRTs).* Carnigie Mellon, Software Engineering Institute, Pittsburg, PA.
Available at:
http://www.sei.cmu.edu/publications/documents/98.reports/98hb001/98hb001abstract.html

13. West-Brown, Moira. *Avoiding the Trial-by-Fire Approach to Security Incidents.* SEI Interactive: Security Matters, Sep 1999.
Available at:
http://interactive.sei.cmu.edu/news@sei/columns/security_matters/1999/mar/security_matters.htm.

Deleted: Rhodenizer, Elizabeth. *Establishing an Information Protection Centre, Lessons Learned.* (May 2003). Paper prepared for the 15th Canadian Information Technology Security Symposium 2003.¶
Borodkin, Michelle. *Computer Incident Response Team.* (September 15, 2001). SANS Infosec Reading Room. ¶
Available at:
http://www.sans.org/rr/incident/CIRT.php. ¶

Deleted: ¶
¶
<#>Brownlee, N., and Guttman, E. *RFC 2350: Expectations for Computer Security Incident Response.* (June 1998). Internet Engineering Task Force, Network Working Group. ¶
Available at:
http://www.ietf.org/rfc/rfc2350.txt?number=2350. ¶
¶
<#>Brezinski, Dominique, and Dittrich, Dave. Black Hat Las Vegas '00 Training Intruder Discovery / Tracking and Compromise Analysis. ¶
Available at:
http://staff.washington.edu/dittrich/talks/blackhat/blackhat/.¶
¶
<#>CERT®/CC: *Computer Security Incident Response Team (CSIRT) Frequently Asked Questions (FAQ).*¶
Available at:
http://www.cert.org/csirts/csirts_faq.html. ¶
¶
¶
¶
¶
¶
<#>Hillier, Peter, Fortier, Christian. *Cyber Incident Response*. Presentation for the 15th Canadian Information Technology Security Symposium 2003.¶

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Last Updated: September 22nd, 2017

Upcoming Training

Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
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
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague Summit & Training 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
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
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive