Handling Incidents

Incident handling refers to the response an organization takes when a violation of its security policies is suspected. The FireSIGHT System includes features to support you as you collect and process information that is relevant to your investigation of an incident. You can use these features to gather intrusion events and packet data that may be related to the incident. You can also use the incident as a repository for notes about any activity that you take outside of the FireSIGHT System to mitigate the effects of the attack. For example, if your security policies require that you quarantine compromised hosts from your network, you can note that in the incident.

The FireSIGHT System also supports an incident life cycle, allowing you to change an incident's status as you progress through your response to an attack. When you close an incident, you can note any changes you have made to your security policies as a result of any lessons learned.

See the following sections for more information about handling incidents in the FireSIGHT System:

Incident Handling Basics

License: Protection

Each organization is likely to have its own process for discovering, defining, and responding to violations of its security policies. The sections that follow describe some of the basics of incident handling and how you can incorporate the FireSIGHT System in your incident response plan:

Definition of an Incident

License: Protection

Generally, an *incident* is defined as one or more intrusion events that you suspect are involved in a possible violation of your security policies. Cisco also uses the term to describe the feature you use in the FireSIGHT System to track your response to an incident.

As explained in Working with Intrusion Events, page 41-1, some intrusion events are more important than others to the availability, confidentiality, and integrity of your network assets. For example, the port scan detection features provided by the FireSIGHT System can keep you informed of port scanning activity on your network. Your security policy, however, may not specifically prohibit port scanning or see it as a high priority threat, so rather than take any direct action, you may instead want to keep logs of any port scanning for later forensic study.

On the other hand, if the system generates events that indicate hosts within your network have been compromised and are participating in distributed denial-of-service (DDoS) attacks, then this activity is likely a clear violation of your security policy, and you should create an incident in the FireSIGHT System to help you track your investigation of these events.

Common Incident Handling Processes

License: Protection

Each organization is likely to define its own process for handling security incidents. Most methodologies include some or all of the following phases:

- Preparation, page 42-2
- Detection and Notification, page 42-2
- Investigation and Qualification, page 42-3
- Communication, page 42-3
- Containment and Recovery, page 42-4
- Lessons Learned, page 42-4

Each of these phases is described in the sections that follow. The descriptions also explain how the FireSIGHT System fits into each phase.

Preparation

You can prepare for incidents in two ways:

- by having clear and comprehensive security policies in place, as well as the hardware and software resources to enforce them
- by having a clearly defined plan to respond to incidents and a properly trained team that can implement the plan

A key part of incident handling is understanding which parts of your network are at the greatest risk. By deploying FireSIGHT System components on those network segments, you can increase your awareness of when and how incidents occur. Also, by taking the time to carefully tune the intrusion policy for each managed device, you can ensure that the events that are generated are of the highest quality.

Detection and Notification

You cannot respond to an incident unless you can detect it. Your incident handling process should note the kinds of security-related events that you can detect and the mechanisms, both software and hardware, that you use to detect them. You should also note where you can detect violations of your security policies. If your network includes segments that are not actively or passively monitored, then you need to note that as well.

The managed devices that you deploy on your network are responsible for analyzing the traffic on the segments where they are installed, for detecting intrusions, and for generating events that describe them. Keep in mind that the access control policy you apply to each of the managed devices governs what kinds of activity they detect and how it is prioritized. You can also set notification options for certain types of intrusion events so that the incident team does not need to sift through hundreds of events. You can specify that you are notified automatically when certain high priority, high severity events are detected.

Investigation and Qualification

Your incident handling process should specify how, after a security incident is detected, an investigation is conducted. In some organizations, junior members of the team triage all the incidents and handle the less severe or lower priority cases themselves. High severity and high priority incidents are handled by more senior members of the team. You should carefully outline the escalation process so that each team member understands the criteria for raising an incident's importance.

Part of the escalation process is tied to understanding how a detected event can affect the security of your network assets. For example, an attack against hosts running Microsoft SQL Server is not a high priority for organizations that use a different database server. Similarly, the attack is less important to you if you use SQL Server on your network, but you are confident that all the servers are patched and are not vulnerable to the attack. However, if someone has recently installed a copy of the vulnerable version of the software (perhaps for testing purposes), you may have a greater problem than a cursory investigation would suggest.

The FireSIGHT System is particularly well suited to supporting the investigation and qualification process. You can create your own event classifications, and then apply them in a way that best describes the vulnerabilities on your network. When traffic on your network triggers an event, that event is automatically prioritized and qualified for you with special indicators showing which attacks are directed against hosts that are known to be vulnerable.

The incident tracking feature in the FireSIGHT System also includes a status indicator that you can change to show which incidents have been escalated.

Communication

All incident handling processes should specify how an incident is communicated between the incident handling team and both internal and external audiences. For example, you should consider what kinds of incidents require management intervention and at what level. Also, your process should outline how and when you communicate with outside organizations. Will some incidents require that you notify law enforcement agencies? If your hosts are participating in a distributed denial of service (DDoS) against a remote site, will you inform them? Do you want to share information with organizations such as the CERT Coordination Center (CERT/CC) or FIRST?

The FireSIGHT System has features that you can use to gather intrusion data in standard formats such as HTML, PDF, and CSV (comma-separated values) so that you can easily share intrusion data with others.

For example, CERT/CC collects standard information about security incidents on its web site. CERT/CC looks for the kinds of information that you can easily extract from the FireSIGHT System, such as:

- information about the affected machines, including:
- the host name and IP
- the time zone
- the purpose or function of the host
- information about the sources of the attack, including:
- the host name and IP

- the time zone
- whether you had any contact with an attacker
- the estimated cost of handling the incident
- a description of the incident, including:
- dates
- methods of intrusion
- the intruder tools involved
- the software versions and patch levels
- any intruder tool output
- the details of vulnerabilities exploited
- the source of the attack
- any other relevant information

You can also use the comment section of an incident to record when you communicate issues and with whom.

Containment and Recovery

Your incident handling process should clearly indicate what steps are taken when a host or other network component is compromised. The range of containment and recovery options stretches from applying patches to vulnerable hosts to shutting down the target and removing it from the network. You should also consider the importance, depending upon the nature and severity of the attack, of preserving evidence in case you pursue criminal charges.

You can use the incident feature of FireSIGHT System to maintain a record of the actions you take during the containment and recovery phase of the incident.

Lessons Learned

Each security incident, whether or not it is a successful attack, is an opportunity to review your security policies. Do you need to update your firewall rules? Do you need a more structured approach to patch management? Are unauthorized wireless access points a new security issue? Each lesson learned should feed back into your security policies and help you prepare better for the next incident.

Incident Types in the FireSIGHT System

License: Protection

You can assign an incident type to each incident you create. The following types are supported by default in the FireSIGHT System:

- Intrusion
- Denial of Service
- Unauthorized Admin Access
- Web Site Defacement
- Compromise of System Integrity
- Hoax
- Theft

- Damage
- Unknown

You can also create your own incident types, as explained in Creating Custom Incident Types, page 42-7.

Creating an Incident

License: Protection

This section explains how you create an incident.

To create an incident:

Access: Admin/Intrusion Admin

Step 1 Select **Analysis > Intrusions > Incidents**.

The Incidents page appears.

Step 2 Click **Create Incident**.

The Create Incident page appears.

If you previously copied intrusion events to the clipboard, they are displayed at the bottom of the page. See Using the Clipboard, page 41-49 for information about using the clipboard.

Step 3 From the **Type** drop-down menu, select the option that best describes the incident.

Step 4 In the **Time Spent** field, enter the amount of time you spent on the incident in the #d #h #m #s format, where # represents the number of days, hours, minutes, or seconds.

Step 5 In the **Summary** text box, type a short description (up to 255 alphanumeric characters spaces, and symbols) of the incident.

Step 6 In the **Add Comment** text box, type a more complete description (up to 8191 alphanumeric characters, spaces and symbols) for the incident.

Step 7 Do you want to add events to the incident?

- If **yes**, select the events on the clipboard and click **Add to Incident**.

  You can also add all the events from the clipboard by clicking **Add All to Incident**.
- If **no**, click **Save**.

In either case, the incident is saved with the information you entered.

Note If you want to add individual events from more than one page on the clipboard, you must add the events from one page, then add the events from the other pages separately.

Editing an Incident

License: Protection

You can update an incident as you collect more information. You can also add or delete events from the incident as your investigation progresses.

To edit an incident:

Access: Admin/Intrusion Admin

Step 1 Select **Analysis > Intrusions > Incidents**.

The Incidents page appears.

Step 2 Click the edit icon ( ) next to the incident you want to edit.

Step 3 You can edit any of the following aspects of the incident:

- change the status
- change the type
- add events from the clipboard
- delete events

Step 4 In the **Time Spent** field, enter the amount of additional time you spent on the incident.

Step 5 In the **Add Comment** text box, indicate your changes to the incident (up to 8191 alphanumeric characters, spaces and symbols) for the incident.

Step 6 Optionally, you can add or delete events from the incident:

- To add events from the clipboard, select the events on the clipboard and click **Add to Incident**.
- To add all the events from the clipboard, click **Add All to Incident**.
- To delete specific events from the incident, select the events and click **Delete**.
- To delete all events from the incident, click **Delete All**.
- To update the incident without adding or deleting events, click **Save**.

Your changes to the incident are saved.

Generating Incident Reports

License: Protection

You can use the FireSIGHT System to generate incident reports that can include the incident summary, incident status, and any comments along with information from the events you add to the incident. You can also specify whether you want to include event summary information in the report.

To generate an incident report:

Access: Admin/Intrusion Admin

Step 1 Select **Analysis > Intrusions > Incidents**.

The Incidents page appears.

Step 2 Click the edit icon ( ) next to the incident you want to include in your report.

Step 3 You have two options:

- To include all the events from the incident in the report, click **Generate Report All**.
- To include specific events from the incident in the report, select the check boxes next to the events you want and click **Generate Report**.

In either case, the Generate Report page appears, including the options for incident reports.

Step 4 Type a name for the report. You can use alphanumeric characters, periods, and spaces.

Step 5 In **Incident Report Sections**, select the check boxes for the portions of the incident that you want to include in the report: **status**, **summary**, and **comments**.

Step 6 If you want to include event information in the report, select the workflow you want to use and then, in **Report Sections**, specify whether you want to include event summary information.

Step 7 Select the check boxes next to the workflow pages you want to include in the report.

Step 8 Select the check boxes next to the output formats you want to use for the report: **PDF**, **HTML**, and **CSV**.

Note CSV-based incident reports include only event information. They do **not** include the status, summary, or comments from the incident.

Step 9 Click **Generate Report** and confirm that you want to update the report profile.

The report is generated.

Creating Custom Incident Types

License: Protection

The FireSIGHT System is delivered with the following incident types that you can use to classify your incidents:

- Compromise of System Integrity
- Damage
- Denial of Service
- Hoax
- Intrusion
- Theft
- Unauthorized Admin Access
- Unknown
- Web Site Defacement

If these incident types do not meet your needs, you can add your own. Note that you cannot delete any custom incident types.

To create a new incident type:

Access: Admin/Intrusion Admin

Step 1 Select **Analysis > Intrusions > Incidents**.

The Incident page appears.

Step 2 Click **Create Incident**.

The Create Incident page appears.

Step 3 In the **Type** area, click **Types**.

The incident management Types page appears. The default incident types are listed at the bottom of the page.

Step 4 In the **Incident Type Name** field, type a name for the new incident type.

Use alphanumeric characters and spaces.

Step 5 Click **Add**.

The new incident type is added.

Step 6 Click **Done** to close the pop-up window and return to the Incidents page.

You can use the new incident type the next time you create or edit an incident.