Contents

Intended audience ........................................................................................................... 5
How this manual is organized ....................................................................................... 5
Related documentation ................................................................................................. 5
Technical support ......................................................................................................... 6

Overview of Skybox Threat Manager ........................................................................ 7
Skybox platform ........................................................................................................... 7
About Skybox Threat Manager ..................................................................................... 9
Threat alert management process ............................................................................... 10
About the Skybox Vulnerability Dictionary .................................................................. 10
Basic architecture ........................................................................................................ 11

Setting up Skybox Threat Manager ........................................................................... 12
Workflow to set up Skybox Threat Manager ............................................................... 12
Setting up the Threat Manager environment ............................................................ 13
Setting up threat alert collection ................................................................................. 13
  Updating the Vulnerability Dictionary ...................................................................... 14
  Configuring collection of alerts from external sources .............................................. 14
Custom Vulnerability Definitions ................................................................................ 15
Customizing the display in the analyses ...................................................................... 17
Deployed product list .................................................................................................... 17
  Setting up the deployed product list ......................................................................... 18
  Maintaining the deployed product list ....................................................................... 20
Ticket phases and due dates .......................................................................................... 21
  Setting up ticket phases and due dates .................................................................... 21
  Setting up due dates when working without phases .................................................... 23
Creating triggers ............................................................................................................ 23
Configuring policies that create tickets for threat alerts ............................................... 24

Working with threat alerts ............................................................................................... 25
Monitoring threat alerts ............................................................................................... 25
  Viewing threat alerts ................................................................................................. 25
  Threat alert statuses ................................................................................................. 26
Reviewing new threat alerts .......................................................................................... 27
Reviewing updated threat alerts .................................................................................... 29
Creating custom analyses .............................................................................................. 31
Searching for threat alerts ............................................................................................ 32
Viewing vulnerability occurrences in the network ....................................................... 33
Remediation ..................................................................................................................... 34
  Remediation workflow ............................................................................................... 34
  Working with tickets ................................................................................................. 35
  Working with tickets and phases .............................................................................. 37

Skybox version 8.5.600
Skybox Threat Manager User’s Guide

Adding attachments to a ticket ............................................................ 40
Associating products with tickets ....................................................... 40
Creating custom solutions ................................................................... 41
Searching for tickets .......................................................................... 41
Reports and CSV .................................................................................... 42

Skybox Vulnerability Dictionary........................................................... 43
What information is provided about each threat alert? ...................... 43

Using tasks for automation ................................................................. 45
Task sequences .................................................................................... 45
Creating task sequences ..................................................................... 45
Viewing and editing task sequences .................................................... 48
Scheduling tasks and task sequences .................................................. 48
Task groups .......................................................................................... 49
Monitoring task results ........................................................................ 49

Reports ................................................................................................. 51
Tickets reports ..................................................................................... 51
Vulnerabilities reports ......................................................................... 52
Limiting the scope of vulnerabilities reports ..................................... 52
Predefined vulnerabilities report definitions ....................................... 53
Threat Alert Management reports ....................................................... 53
Exporting data to CSV files ............................................................... 53

Maintenance .......................................................................................... 55
Updating your Vulnerability Dictionary ................................................. 55
Backing up the model ........................................................................... 55
Preface

Intended audience

The Skybox Threat Manager User’s Guide explains how to work with Skybox Threat Manager. Use this document in conjunction with:

› Skybox Installation and Administration Guide, which explains Skybox installation, and various configuration and maintenance tasks
› Skybox Threat Manager Getting Started Guide, which explains how to use the various features of Skybox Threat Manager, using predefined data

The intended audience is any user of Skybox Threat Manager.

How this manual is organized

This manual includes the following chapters:

› Overview of Skybox Threat Manager (on page 7)
› Setting up Skybox Threat Manager (on page 12)
› Working with threat alerts (on page 25)
› Skybox Vulnerability Dictionary (on page 43)
› Using tasks for automation (on page 45)
› Reports (on page 51)
› Maintenance (on page 55)

Related documentation

The following documentation is available for Skybox Threat Manager:

› Skybox Threat Manager Getting Started Guide

Other Skybox documentation includes:

› Skybox Installation and Administration Guide
› Skybox Reference Guide
› Skybox Developer’s Guide
› Skybox Release Notes
› Skybox Change Manager User’s Guide
› Skybox Vulnerability Control User’s Guide

The entire documentation set (in PDF format) is available here.

You can access a comprehensive Help file from any location in the Skybox Manager by using the Help menu or by pressing F1.
Technical support

You can contact Skybox using the form on our website or by emailing info@skyboxsecurity.com

Customers and partners can contact Skybox technical support via the Skybox support portal

When opening a case, you need the following information:

› Your contact information (telephone number and email address)
› Skybox version and build numbers
› Platform (Windows or Linux)
› Problem description
› Any documentation or relevant logs

You can compress logs before attaching them by using the Pack Logs tool (see Packing log files for technical support, in the Skybox Installation and Administration Guide).
Chapter 1

Overview of Skybox Threat Manager

This chapter is an overview of Skybox Threat Manager.

In this chapter

Skybox platform ....................................................................... 7
About Skybox Threat Manager ................................................ 9
About the Skybox Vulnerability Dictionary .............................. 10
Basic architecture ..................................................................... 11

Skybox platform

Skybox™ Security arms security professionals with the broadest platform of solutions for security operations, analytics and reporting. By integrating with more than 100 networking and security technologies organizations are already, the Skybox Security Suite merges data silos into a dynamic network model of your organization’s attack surface, giving comprehensive visibility of public, private and hybrid IT environments. Skybox provides the context needed for informed action, combining attack vector analytics and threat-centric vulnerability intelligence to continuously assess vulnerabilities in your environment and correlate them with exploits in the wild. This makes the accurate prioritization and mitigation of imminent threats a systematic process, decreasing the attack surface and enabling swift response to exposures that truly put your organization at risk.
Skybox arms security leaders with a comprehensive cybersecurity management platform to address the security challenges of large, complex networks. The Skybox Security Suite breaks down data silos to build a dynamic network model that gives complete visibility of an organization’s attack surface and the context needed for informed action across physical, multi-cloud and industrial networks. We leverage data by integrating with 120 security technologies, using analytics, automation and advanced threat intelligence from the Skybox Research Lab to continuously analyze vulnerabilities in your environment and correlate them with exploits in the wild. This makes the prioritization and mitigation of imminent threats an efficient and systematic process, decreasing the attack surface and enabling swift response to exposures that truly put your organization at risk. Our award-winning solutions automate as much as 90 percent of manual processes and are used by the world’s most security-conscious enterprises and government agencies, including Forbes Global 2000 companies. For more information visit the Skybox Security website
The Skybox Security Suite includes:

- **Skybox Vulnerability Control**: Powers threat-centric vulnerability management by correlating intelligence on vulnerabilities in your environment, the surrounding network and security controls and exploits in the wild focusing remediation on your most critical threats.
- **Skybox Threat Manager**: Consolidates threat intelligence sources and prioritizes advisories in the context of your attack surface, automatically analyzing the potential impact of a threat and providing remediation guidance.
- **Skybox Firewall Assurance**: Brings multi-vendor firewall environments into a single view and continuously monitors policy compliance, optimizes firewall rule sets and finds attack vectors that others miss.
- **Skybox Network Assurance**: Analyzes hybrid environments end to end across physical, virtual and cloud – even operational technology – networks, illuminating complex security zones, access paths and policy compliance violations.
- **Skybox Change Manager**: Ends risky changes with network-aware planning and risk assessments, making firewall changes a secure, consistent process with customizable workflows and automation.
- **Skybox Horizon**: Visualizes an organization’s unique attack surface and indicators of exposure (IOEs), giving threat-centric insight to critical risks, visibility across an entire organization or down to a single access rule and metrics to track risk reduction over time.

The products share common services, including modeling, simulation, analytics, reporting, and automated workflow management.

### About Skybox Threat Manager

Skybox Threat Manager consolidates threat intelligence sources and identifies relevant advisories in the context of your attack surface. With detailed threat impact analysis and remediation recommendations, your team can prioritize and respond to critical threats in minutes.

- Automate the collection and normalization of threat intelligence.
- Get analyst-validated threat intelligence from Skybox Research Lab’s investigations of 30+ security data feeds and 700,000+ sites in the dark web.
- Correlate and prioritize threats with your organization’s attack surface.
- Target response at imminent threats with efficient remediation options tailored to you.
- Track remediation status with an integrated ticketing workflow and evaluate progress in gradual risk reduction.

### Product Highlights

- Consolidates threat intelligence.
- Collects data from threat intelligence feeds.
- Delivers Skybox Research Lab threat intelligence from investigations of more than 700,000 sites in the open and deep web.
Utilizes information updated daily from Skybox Vulnerability Database

- Automates threat prioritization
  - Uses alert properties, vulnerability instances and the network model for threat prioritization within the context of your attack surface
  - Provides vulnerability and impact analysis aligned with CVSS
  - Focuses your team on imminent threats to your organization and ensures potential threats don’t escalate

- Provides a centralized view of all threat intelligence
  - Creates a normalized threat alert repository
  - Customizes workflows to fit your organization
  - Integrates with 3rd-party threat intelligence feeds, including Symantec DeepSight and VeriSign iDefense

- Optimizes remediation processes
  - Reduces time and resources needed to protect against cyberattacks
  - Streamlines remediation and patching with powerful, built-in workflows
  - Automates tracking and reporting for improved visibility from the C-suite to the trenches

THREAT ALERT MANAGEMENT PROCESS

Threat alerts are modeled in Skybox as Vulnerability Definitions. Skybox imports threat alerts from an alert service and merges them into the Skybox database. Every time an alert is received, a new Vulnerability Definition is added or the relevant Vulnerability Definition in the Skybox database is updated.

The basic process of handling threat alerts includes the following:

1. Setting up of the system so that threat alerts are imported (collected) to the Skybox database on an ongoing basis
2. Reviewing Vulnerability Definitions and assessing their impact
3. For the important Vulnerability Definitions, starting a workflow (ticket); otherwise dismissing the Vulnerability Definition as irrelevant

About the Skybox Vulnerability Dictionary

The Skybox Vulnerability Dictionary consolidates vulnerability data for more than 1000 products that are used extensively in enterprise network environments, including servers and desktop operating systems, business and desktop applications, databases, runtime frameworks, networking hardware and software, and security software. This data selection is tailored to Skybox Security’s enterprise customers, according to the most relevant products and their corresponding vulnerabilities for a large enterprise network.
The Skybox Vulnerability Dictionary currently supports more than 68,000 vulnerabilities. The Skybox Vulnerability Dictionary is a result of information collected from leading public and private security data sources, and built as a superset of vulnerabilities. As a state-of-the-art vulnerability database, it is CVE compliant and implements CVSS v2 and v3 standards.

Basic architecture

The Skybox platform consists of a 3-tiered architecture with a centralized server (Skybox Server), data collectors (Skybox Collectors), and a user interface (Skybox Manager). Skybox can be scaled easily to suit the complexity and size of any infrastructure.

For additional information, see the Skybox architecture topic in the *Skybox Installation and Administration Guide*. 
Chapter 2

Setting up Skybox Threat Manager

Some setup is required before you can start using Skybox Threat Manager on a continuous basis to monitor and process threat alerts.

In this chapter

Workflow to set up Skybox Threat Manager............................. 12
Setting up the Threat Manager environment.......................... 13
Setting up threat alert collection........................................... 13
Customizing the display in the analyses................................. 17
Deployed product list .......................................................... 17
Ticket phases and due dates ................................................ 21
Creating triggers................................................................. 23
Configuring policies that create tickets for threat alerts .......... 24

Workflow to set up Skybox Threat Manager

We recommend the following workflow:

1. Set up the Threat Manager environment (see page 13), including the alert source and whether to view threat alerts as security bulletins/advisories or as individual Vulnerability Definitions.

2. Configure a task to get the threat alerts from the alert source (see Setting up threat alert collection (on page 13)).

3. (Optional) Organize the products used by your organization into a list of deployed products. The deployed product list helps users working with threat alerts to decide whether new threat alerts are relevant to your organization. You can use it for creating analyses (queries) about threat alerts based on their product types. For additional information, see Deployed product list (on page 17).

4. (Optional) Define a workflow through which each threat alert ticket must pass before it is closed:

   a. Divide the workflow into several phases (for example, Initiation, Assess Risk, Deploy Solution, and Request to Close).

   b. Specify how many days are allocated for each phase.

   For additional information, see Ticket phases and due dates (on page 21).
You can set up Skybox Threat Manager to create:

- Email alerts about critical threat alerts or new tickets (see Creating notifications (on page 23)).
- Tickets for critical threat alerts (see Configuring policies that create tickets for threat alerts (on page 24)).

**Setting up the Threat Manager environment**

Before you can work with Threat Manager, you must define the source that you use to get Vulnerability Definitions: the Skybox Vulnerability Dictionary (this is the default source), Symantec DeepSight, or VeriSign iDefense.

When working with the Skybox Vulnerability Dictionary as the alert source, you can define how you want the alerts to be displayed: as a list of security bulletins and advisories (which often include multiple Vulnerability Definitions), or as a list of single Vulnerability Definitions.

Note: Alerts can only be displayed as security bulletins and advisories when using the Skybox Vulnerability Dictionary as the alert source.

*To set up the environment*

1. Select **Tools > Options > Server Options > Threat Manager**.
2. Define **Alert Source**.
3. Define **Threat Alert Mode**: how the alerts are displayed.

   Note: Custom Vulnerability Definitions are disabled by default. If you see that they are necessary later, you can enable them (see Custom Vulnerability Definitions (on page 15)); users can add Vulnerability Definitions manually if they are not available from the selected source.

**Setting up threat alert collection**

The process of handling threat alerts is the same for all sources. However, you must configure Skybox separately to collect threat alerts from each source.

- For information about configuring Skybox to receive updates from the Vulnerability Dictionary, see Updating the Vulnerability Dictionary (on page 14).

  **Important:** Update the Vulnerability Dictionary on a regular basis even when using an external alert service as the Vulnerability Definition source.

- For information about configuring Skybox to receive updates from alert services, see Configuring collection of alerts from external sources (on page 14).

- For information about adding custom Vulnerability Definitions, see Custom Vulnerability Definitions (on page 15).
UPDATING THE VULNERABILITY DICTIONARY

Skybox includes the most up-to-date Vulnerability Dictionary at the time of release, but new updates are issued periodically. You must keep the Vulnerability Dictionary for your model up-to-date to enable correlation of newly published threat alerts.

If the Vulnerability Dictionary that you are using is more than a week old, you should update it.

To check the date and version of the Vulnerability Dictionary

Select **File > Dictionary > Show Dictionary Info**.

To enable the Dictionary Update – Daily task to run automatically

1. Click **Operational Console**.
2. In the Operational Console tree, select **Tasks > All Tasks**.
3. In the Table pane, right-click the **Dictionary Update – Daily** task and select **Properties**.
4. In the Properties dialog box, select **Enable Auto-launch**.
5. Click **OK**.
6. (Optional) Launch the task, so that it runs now.

Note: It is important to make sure that the Skybox Vulnerability Dictionary is up-to-date before you start obtaining asset and vulnerability information.

To verify that the task is running correctly

1. In the Table pane, select the **Dictionary Update – Daily** task.
2. Look at the task’s last run time and status, and in the task messages for success or error messages.
   - For information about running tasks and task messages, see the Tasks topic in the Skybox Vulnerability Control Getting Started Guide.

CONFIGURING COLLECTION OF ALERTS FROM EXTERNAL SOURCES

You can collect threat alerts using **Alert Service** tasks. These tasks trigger a Skybox Collector to log in to the alert service and download threat alerts describing new Vulnerability Definitions or updates to threat alerts for existing Vulnerability Definitions. The alert service’s product database is also downloaded as part of the task.

The first time an alert collection task runs it retrieves all Vulnerability Definitions reported in the past few years (this can take some time). Set the task to retrieve only recent alerts so that, after the 1st run, it retrieves only updates.

Note: From time to time the alert service provider might provide only a full download of the database instead of an update.

The same threat alert might be received from an alert service more than once, in which case the information in the Skybox database is updated each time (including the modification date).
Note: If your Skybox database includes vulnerability occurrences found by a scanner, you can view the relationships between those vulnerability occurrences and the Vulnerability Definitions received as threat alerts. For additional information, see Viewing vulnerability occurrences in the network (on page 33).

For information about the tasks that collect threat alerts from alert services, see:

- The Symantec DeepSight collection tasks topic in the Skybox Reference Guide
- The VeriSign iDefense collection tasks topic in the Skybox Reference Guide

CUSTOM VULNERABILITY DEFINITIONS

You might know about Vulnerability Definitions that affect your organization before they are reported by your alert service or there might be Vulnerability Definitions that affect proprietary products that are not supported by the alert service.

These Vulnerability Definitions are supported in Skybox as custom Vulnerability Definitions.

The ability to work with custom Vulnerability Definitions is disabled by default.

To enable custom Vulnerability Definitions

1. Select Tools > Options > Server Options > Threat Manager.
2. Select Custom Vulnerability Definitions.
3. You can change Source Name and Source Prefix for these Vulnerability Definitions.
4. Click OK.

Creating and managing custom Vulnerability Definitions

Custom Vulnerability Definitions are created and managed in the Custom Vulnerability Definitions dialog box. Make all necessary changes and then submit the changes to the Skybox Vulnerability Dictionary. After they are created (and submitted), custom Vulnerability Definitions are stored in the Skybox database and function in the same way as other Vulnerability Definitions, except that you must update them manually when necessary.

Note: The Custom Vulnerability Definitions dialog box is the only place where you can make changes to custom Vulnerability Definitions.

Vulnerability Definitions added or changed since the last time the changes were submitted to the Vulnerability Dictionary have a status of Pending.
Creating custom Vulnerability Definitions

To create a custom Vulnerability Definition

1. On the toolbar, click ☰.
2. In the Custom Vulnerability Definitions dialog box, click New.
3. In the New Custom Vulnerability Definition dialog box, fill in the fields as described in the following table.
4. Click OK.

The Vulnerability Definition is listed in the table as Pending. It is not yet available for use outside this dialog box. After submitting the changes, the Vulnerability Definition becomes available for general use.

Editing custom Vulnerability Definitions

When you make changes to an existing custom Vulnerability Definition, the changed version has Pending status, but the original version remains available for general use. After the changes are submitted the updated version replaces the previous version.

The properties in the Custom Vulnerability Definitions dialog box are described in the following table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Title</td>
<td>The title of the Vulnerability Definition.</td>
</tr>
<tr>
<td>Severity</td>
<td>(Read-only) The severity of the Vulnerability Definition. The severity is calculated from the information that you provide in the CVSS tab.</td>
</tr>
<tr>
<td>Source</td>
<td>(Read-only) The source of the Vulnerability Definition.</td>
</tr>
<tr>
<td>CVE</td>
<td>The CVE ID of the Vulnerability Definition, if you know it.</td>
</tr>
<tr>
<td>ID</td>
<td>(Read-only) The ID of the Vulnerability Definition, including the prefix for custom Vulnerability Definitions.</td>
</tr>
<tr>
<td>BID</td>
<td>The Bugtraq ID of the Vulnerability Definition.</td>
</tr>
<tr>
<td>Published Date</td>
<td>The date on which the Vulnerability Definition was published.</td>
</tr>
<tr>
<td>Created by</td>
<td>(Read-only) The user who created the Vulnerability Definition.</td>
</tr>
<tr>
<td>Modification Date</td>
<td>(Read-only) The date that the Vulnerability Definition was most recently modified.</td>
</tr>
<tr>
<td>Description</td>
<td>A free-form description of the Vulnerability Definition.</td>
</tr>
<tr>
<td>User Comments</td>
<td>Additional information or comments about the Vulnerability Definition.</td>
</tr>
<tr>
<td><strong>CVSS</strong></td>
<td>The CVSS base score and temporal score metrics. After filling in this information, click Calculate to obtain the CVSS base and temporal scores for the Vulnerability Definition.</td>
</tr>
<tr>
<td><strong>Affected</strong></td>
<td>Use this tab to select deployed products that are affected.</td>
</tr>
</tbody>
</table>
### Property Description

| Products | by this Vulnerability Definition and, optionally, to edit the versions of these products that are affected by the Vulnerability Definition. |

### Submitting the changes

When you submit changes for custom Vulnerability Definitions, Skybox adds the new custom Vulnerability Definitions and the changes to existing custom Vulnerability Definitions to the Skybox database. This can take several minutes.

Changes are submitted every time an alert service or Dictionary update task runs. You can submit changes manually by clicking **Submit Changes** in the dialog box.

### Customizing the display in the analyses

The Threat Manager workspace includes predefined folders and analyses (queries), which display threat alerts according to their severity, status, and age. By default, new threat alerts are displayed in the following 2 analyses:

- **Public Analyses > Incoming > High & Critical**
- **Public Analyses > Incoming > Other Severities**

These analyses list all incoming threat alerts of the specified severities. After the 1st collection of threat alerts, there might be thousands of them in these analyses that must be reviewed.

By default, the threat alerts are not filtered by reported date—all unassigned threat alerts, no matter when they were reported, are displayed. You can set the value of the **Reported Date** filter of these analyses in accordance with your organization’s policy.

**To customize an analysis**

1. In the tree, right-click the analysis and select **Properties**.
2. In the `<Analysis name>` Properties dialog box, make changes, which can include:
   - Selecting a specific **Reported Date**
   - Changing how the analysis is sorted, so that the displayed threat alerts are always listed in a specific order
3. Click **OK**.

### Deployed product list

In Skybox, you can create a list of products used by your organization—the **deployed product list**. Use this list to analyze the threat alerts to help you to decide whether they are relevant (that is, whether they affect deployed products).
The deployed product list is created from several sources. The main source is the product catalog for the alert service used by your organization, which is downloaded with the threat alerts. The product catalog includes all products supported by the alert service. You can create products that have no connection to the product catalog.

You should base the products in the deployed product list on the product catalog, because the products in the catalog are those that are recognized by the alert source as being affected by threat alerts.

Each time a threat alert is received, you can check its affected products to see whether they are mapped to the deployed product list. If any are, the threat alert affects your organization.

SETTING UP THE DEPLOYED PRODUCT LIST

The deployed product list can be a flat list of products used by your organization or the products that you select can be classified into product groups (represented by folders in the product list). For example, you can create a separate product group for each operating system family used in your organization.

You can add products to the product list in the following ways:

- Select common products from the alert service product catalog
- Manually add products that are missing from the catalog

Creating product groups

We recommend that you create product groups before adding products. However, you can create additional product groups at any time.

To create a product group

1. Click \(\text{\textbullet}\).
   The Skybox Admin window opens with the deployed product list displayed in the Table pane.
2. In the tree, right-click the Deployed Product List node and select New Product Group.
3. In the New Product Group dialog box, type a Name for the product group. You can add a comment.
4. Click OK.

Adding products

You can add a single product from the alert service by mapping it to a catalog product, if an appropriate catalog product is available.

You can add products:

- Directly from the product catalog, so that for every selected catalog product, a product with the same name is created in the deployed product list
- One-by-one, either with or without mapping to the product catalog

This is useful when you are adding a single product.
- You can map catalog products to the new product, so that it receives an alert each time a catalog product is affected. For example, you could group
all version of MySQL together, if one person is responsible for dealing with all databases.

- You can add proprietary applications and less popular deployed products that might not be in the product catalog. You must update unmapped products manually; they do not get alerts.

If you are working with product groups, you can add products:

- Directly to a product group
- To the product list without adding them to a product group

### Adding products from the product catalog

**To add products from the product catalog**

1. Right-click the main **Deployed Product List** node or the relevant **Product Group** folder and select **New Products from <Catalog name>**.

2. In the New Products from <Catalog name> dialog box, in the **Search for Products** field, type a string to use for the product search and click **Search**.

   Note: The search is not case-sensitive.

   Products in the catalog that contain the string as part of their name are listed in a table in the dialog box. The list contains all available products that you can add to the deployed product list. Products that are already included have a check mark in the **Mapped in DP List** column.

3. From the table, select the products to add to the product list and click **»**.

   Note: To see the mapping of a specific product, select the product and click **Show References**.

Each selected catalog product is added to the deployed product list as a separate product with the same vendor name and product name as the catalog product. Each selected catalog product is mapped to the corresponding new product.

### Adding single products

There are 2 ways to add single new products:

- Create them from scratch
- Copy existing products

**To create a product from scratch**

1. Right-click the **Deployed Product List** node or the relevant **Product Group** folder and select **New Product**.

2. In the New Product from <Vulnerability database name> dialog box, fill in the fields in the Product Details pane. (Only **Vendor** and **Product** are mandatory).

   In the **Installed Versions** field, add multiple versions as a comma-separated list.
3 If you do not want to map the product to a vulnerability database product (that is, you are creating a product for an application that is not part of the product list), click OK and skip the rest of these instructions. Otherwise, click Add.

4 In the Add Products from <Vulnerability database name> dialog box, in the Search for Products field, type a string to use for the product search and click Search.

   Note: The search is not case-sensitive.

   Products in the vulnerability database that contain the string as part of their name are listed in a table in the dialog box. The list contains all available products that you can add to the deployed product list. Products that are already included have a check mark in the Mapped to Deployed Product List column.

5 From the table, select the vulnerability database products to map to the new product and click Add.

   The selected vulnerability database products are mapped to the new deployed product.

6 Click Close.

7 Click OK.

   The new product is added to the deployed product list with the mapping that you selected.

To copy an existing product

1 Right-click the product that you want to copy and select Create Product Like.

   All fields are copied from the selected product to the new product, except for Change Log (History).

   The following comment is added to the new product: Copied from <vendor product> (<Original ID>)

2 Make any necessary changes to the product.

   Note: You must make a change; you cannot have 2 identical products in the deployed product list.

3 Click OK.

   The new product is added to the deployed product list with the mapping that you selected.

MAINTAINING THE DEPLOYED PRODUCT LIST

After the deployed product list is set up, you can do any of the following from the Skybox Admin window:

- Add or update information about a product (for example, the version numbers of the product that are installed or the number of installations).
- Delete products from the list
- Add new product groups and rename or delete existing product groups
When you delete a product group, products that do not belong to any other product group are also deleted.

- Add new products
- Add existing products to existing product groups

A product can belong to multiple product groups. (To add a product to a product group, right-click the product, select **Add Product(s) to Product Group**, and then select the product group to which to add the product.)

Note: Privileged users can add new products from the Threat Manager window when a threat alert is selected in the Table pane; in the Details pane, click the `<Catalog name> Products` tab, right-click the desired product and select **New Product**.

### Ticket phases and due dates

In many organizations, there are different phases in the workflow of threat alert remediation. It is often helpful to formally model this workflow, so that each time a ticket is opened on a threat alert, you can track its progress.

To model the workflow phases, you set up a system of ticket phases—a list of steps through which each ticket passes. Each phase has an owner, due date, start date and end date, and the phase owners can promote or demote the ticket through the phases, until completion.

When a ticket is created, it contains a list of its relevant phases. Initially, the ticket is assigned to the 1st phase and its owner is the owner of the 1st phase. During the life cycle of the ticket, it progresses to the next phase or goes back to the previous phase.

When a phase owner finishes working on the current phase, the ticket is passed to the next phase using a promote function. This updates the end date on the phase and moves the ticket to the next owner.

If you use phases, you can define the timeline of the ticket by specifying a due date for each phase, where phase owners must finish their changes by the specified due date. The due date of the final phase is the due date of the ticket.

You can base due dates on priorities, so that tickets with different priorities have different due dates for each phase. For example, a high-priority ticket might be expected to go through phase 1 in one day, phase 2 in one day, phase 3 in one week, and so on, whereas a lower-priority ticket might have a slower schedule.

Ticket phases and due dates are both optional (that is, you can work with Skybox Threat Manager with or without phases and with or without due dates). Ticket phases are configured using **Tools > Administrative Tools > Options**. Due dates are configured in `<Skybox_Home>\server\conf\sb_server.properties`

### SETTING UP TICKET PHASES AND DUE DATES

Define phases before users start working with tickets. You can rename them at any time; you can reorder them if there are no open tickets.

**Ticket phases**

The following is a typical list of ticket phases for threat alerts:
Assess Risk
Develop Solution
Deploy
Verification

For information about defining phases, see the Defining ticket phases topic in the Skybox Reference Guide.

After you define ticket phases, you can create analyses to view tickets of each phase separately (see Creating analyses for ticket phases (on page 37)). You can filter tickets reports to include only tickets in selected phases (see the Tickets reports topic in the Skybox Reference Guide).

Due date formulas

You can set up due date formulas for tickets that specify the length (in days) of each ticket phase. You can set a separate formula for each ticket priority. These formulas are optional; you can specify the due dates manually, on a per-ticket basis.

Due date formulas are stored as comma-separated lists of integers, where the 1st integer specifies the number of days between the ticket’s creation date and the expected end of the 1st phase and each subsequent integer specifies the number of days from the end of the previous phase to the due date for the current phase. The number of integers in the string is determined by the number of phases for the ticket type (including the Verification phase).

For example, if you have 5 phases for threat alert tickets (Initiation, Assess Risk, Develop Solution, Deploy, and Verification), the due date formula for Critical tickets might be 1,1,7,14,1, whereas the due date formula for Medium tickets might be 1,1,21,60,1. Assuming a Critical ticket is created on July 4, the default due dates for each phase of this ticket are listed in the following table.

<table>
<thead>
<tr>
<th>Ticket phase</th>
<th>Length in days</th>
<th>Due date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiation</td>
<td>1</td>
<td>July 5</td>
</tr>
<tr>
<td>Assess Risk</td>
<td>1</td>
<td>July 6</td>
</tr>
<tr>
<td>Develop Solution</td>
<td>7</td>
<td>July 13</td>
</tr>
<tr>
<td>Deploy</td>
<td>14</td>
<td>July 27</td>
</tr>
<tr>
<td>Verification</td>
<td>1</td>
<td>July 28</td>
</tr>
</tbody>
</table>

To set up the due date formulas for ticket phases

- The due date formulas are located in
  `<Skybox_Home>\server\conf\sb_server.properties`

  The following are the formula properties that you can set, where P1 is critical priority and P5 is very low priority:
  - due_date_rule_VulnerabilityDefinitionTicket_P1
  - due_date_rule_VulnerabilityDefinitionTicket_P2
  - due_date_rule_VulnerabilityDefinitionTicket_P3
  - due_date_rule_VulnerabilityDefinitionTicket_P4
Each formula has the following structure, where each letter represents an integer:

- due_date_rule_VulnerabilityDefinitionTicket_P5 = i,j,k,...,w

If due dates are not to be added automatically to a phase, use a comma (without an integer) to mark its position. For example, due_date_rule_VulnerabilityDefinitionTicket_P1 = 1,1,,,,

**SETTING UP DUE DATES WHEN WORKING WITHOUT PHASES**

You can set up due dates for threat alert tickets even when working without ticket phases. In this case, the due dates are set only according to the priority of the ticket.

When working without phases, the value of each due date formula is an integer that specifies the number of days between the ticket’s creation date and the expected completion. For example, the due date formula for Critical tickets might be 7 (days) and the due date formula for Medium tickets might be 21 (days).

To set up due date formulas when working without ticket phases

The due date formulas are configured in <Skybox_Home>\server\conf\sb_server.properties

The following are the formula properties that you can set, where P1 is critical priority and P5 is very low priority:

- due_date_rule_VulnerabilityDefinitionTicket_P1
- due_date_rule_VulnerabilityDefinitionTicket_P2
- due_date_rule_VulnerabilityDefinitionTicket_P3
- due_date_rule_VulnerabilityDefinitionTicket_P4
- due_date_rule_VulnerabilityDefinitionTicket_P5

The value for each formula property must be an integer. For example, due_date_rule_VulnerabilityDefinitionTicket_P1=6 means that tickets with Critical priority should be completed within 6 days of their creation.

**Creating triggers**

You can create event-based rules (triggers) that send email notifications for the following entities:

- Tickets: A notification is sent each time a ticket changes in a way that matches a trigger for tickets.

  For example, you can create a trigger that sends notifications to all members of the Develop Solutions group when a ticket is promoted to the Develop Solutions phase.

  Note: For tickets, you can also trigger Skybox tasks that run a script. For further information, see Ticket trigger properties, in the Skybox Reference Guide.
Threat alerts: A notification can be sent for a single threat alert or for multiple threat alerts.

For example, after collecting new threat alerts, Skybox checks the Threat Alert triggers to see whether any threat alerts meet their criteria. If multiple threat alerts meet the criteria for a single trigger, it sends a single notification with multiple threat alerts. However, a separate notification is sent for each trigger. If, for example, a trigger sends notifications to the person responsible for Windows products each time new threat alerts affecting a Windows product are received and 5 new Windows threat alerts are received from a single collection, a single notification containing all the new Windows threat alerts is sent. If other new threat alerts that match additional triggers are received during the same collection, separate notifications are sent for those threat alerts.

To create a trigger
2. In the Skybox Admin window, right-click the Triggers node and select New Trigger.
3. Select the Trigger Type.
4. Fill in the fields as described in the relevant topic in the Skybox Reference Guide:
   - Ticket trigger properties
   - Threat Alert trigger properties
5. Click OK.

Notifications are triggered and sent (according to the selected properties).

Configuring policies that create tickets for threat alerts

Threat alert policies create tickets for threat alerts. For example, you can create a policy that creates tickets for high-priority threat alerts from a specific vendor that were reported in the last week. When a Tickets – Auto Generation task runs, tickets are created for all threat alerts in the model that meet the criteria specified in the policy.

For information about how to set up threat alert policies, see the Automating tickets section in the Skybox Vulnerability Control User’s Guide.
Chapter 3

Working with threat alerts

After configuring Skybox Threat Manager to receive threat alerts on a regular basis, users can begin processing the threat alerts.

Working with threat alerts includes:

> Monitoring the incoming threat alerts to decide whether they are relevant to your organization
> Creating tickets for threat alerts that should be fixed
> Monitoring the ticket workflow
> Issuing reports as necessary about the threat alerts themselves or the tickets

In this chapter

Monitoring threat alerts ....................................................... 25
Remediation ....................................................................... 34
Reports and CSV .................................................................. 42

Monitoring threat alerts

The goals of monitoring threat alerts are:

1. To decide whether the threat alerts are likely to affect your organization’s network
2. To make sure that relevant threat alerts are ticketed and assigned to the correct staff member for handling

VIEWING THREAT ALERTS

The Threat Manager workspace includes predefined folders and predefined analyses that display threat alerts according to their severity, status, and age. In the tree, the threat alert folders are displayed with 🗒️ and threat alert analyses with 📊.
Note: The following screen capture—taken from the demo model—is intended as an example. Phases are not included in Skybox by default; you must configure them.

As new threat alerts are collected into Skybox, they are displayed in the relevant analyses.

For example, new threat alerts are assigned a status of **Unassigned**—they were never reviewed—and they are placed under the **Incoming** folder, in the analysis that matches their severity. As you assign Tickets and resolve the threat alerts, the status of the threat alerts change and they are moved to the relevant analysis and folder.

*To view threat alerts*

› From the Threat Manager tree, select an analysis.

**THREAT ALERT STATUSES**

Threat alerts have statuses that help to classify them:

› **Unassigned**: Threat alerts that are waiting for review. This is the initial status of all threat alerts.

› **In Process**: Threat alerts that have tickets with status **New, In Progress**, or **Reopened**.

› **Resolved**: Threat alerts that have tickets with status **Closed, Resolved**, or **Verified**.

› **Irrelevant**: Threat alerts that are not relevant for your organization. This status is assigned to threat alerts that are marked as irrelevant by the user and to threat alerts that have tickets with status **Rejected** or **Ignored**.

If a threat alert has tickets with multiple statuses, the status of the threat alert is set according to the ticket with the highest ticket status in the following order:
In Process (matches ticket statuses of New, In Progress, and Reopened, and custom ticket statuses in the Open status group)

Resolved (matches ticket statuses of Resolved, Verified, and Closed, and custom ticket statuses in the Done status group)

Irrelevant (matches ticket statuses of Ignored and Rejected, and custom ticket statuses in the Invalid status group)

For example, if a threat alert has 1 In Progress ticket and 1 Rejected ticket, the threat alert has a status of In Process.

The status of a threat alert is updated when any of the following events occurs:

- New tickets are created for the threat alert.
- The status of tickets for the threat alert changes.
- The threat alert is marked as Irrelevant.

REVIEWING NEW THREAT ALERTS

You must evaluate new and updated threat alerts for their relevance to your organization. Open the folder where new threat alerts are displayed and select the relevant analysis (usually, this is Public Analyses > Incoming > High & Critical). Start by reviewing all the high-priority threat alerts (those found in the High & Critical analyses) and only then handle lower-priority threat alerts.

Review the information about each threat alert as described in Viewing threat alerts (on page 25). The Affected Products tab contains a list of the software products that this threat alert can affect. If an affected product is in your organization’s product list, we recommend that you open a ticket on the threat alert. You can open multiple tickets on a threat alert. For example, if a threat alert affects Windows NT and Windows XP, and these are handled by different administrators in your organization, you can open a separate ticket for each product.

The following options are available when reviewing a new threat alert:

- Create a threat alert ticket (see page 35), and assign it.
  - When you create a ticket, the status of the threat alert changes to In Process.
- Mark the threat alert as for review: right-click the threat alert and select Set Review Indication.
- Update the threat alert’s CVSS properties (see page 28).
- Mark the threat alert as Irrelevant (see page 27), which changes the status to Irrelevant and moves the threat alert to the Irrelevant folder.

Irrelevant threat alerts

If you decide that a specific threat alert is not relevant, you can manually change its status to Irrelevant. Threat alerts that have tickets with a status of Ignored or Rejected are assigned a status of Irrelevant.
Note: If a threat alert has a status of *Irrelevant* and there are updates to the threat alert from the Skybox Vulnerability Dictionary or the alert service, the threat alert is updated and marked as for review (in the *For Review* column of the analysis), but its status does not change.

**To mark a threat alert as irrelevant**

1. Right-click the threat alert and select **Mark as Irrelevant**.
   - If the threat alert has **Open** tickets, marking the threat alert as **Irrelevant** closes its tickets automatically.

2. In the Mark threat alert as Irrelevant dialog box, type a comment in the **Enter a comment** field and click **OK**.

The **Reviewed Threat Alerts > Irrelevant** analysis lists threat alerts that are marked as irrelevant. You can reopen Irrelevant threat alerts.

**To reopen an irrelevant threat alert**

1. Find the irrelevant threat alert in the **Reviewed Threat Alerts > Irrelevant** analysis.

2. Right-click the threat alert and select **Mark as Unassigned** or **Create Ticket**.
   - If you select **Mark as Unassigned**, type a comment in the **Enter a comment** field of the Mark threat alert as Unassigned dialog box and click **OK**.
     - The threat alert is reopened with a status of **Unassigned**; it is displayed in the relevant analyses after a refresh.
   - If you select **Create Ticket**, fill in the fields in the New Threat Alert Ticket dialog box (the only mandatory field is **Owner**) and click **Save**.
     - For information about creating threat alert tickets, see **Creating threat alert tickets** (on page 35).
     - The threat alert is reopened with a status of **In Process**; it is displayed in the relevant analyses after a refresh.

**Updating the CVSS properties**

In some cases, the CVSS properties provided by the Skybox Vulnerability Dictionary might not match the CVSS properties used in your organization. In these cases, update the CVSS properties of the threat alert.
To update a threat alert’s CVSS properties

1. Right-click the threat alert in the list and select CVSS.

2. Make the desired changes in the CVSS fields.

   Note: Changes to the Base Score Metrics affect the Base Score and the Temporal Score.

3. You can restore the Vulnerability Dictionary values (click Restore Values) or view the updated and Vulnerability Dictionary values side-by-side (click Compare to Dictionary).

4. Click OK.

REVIEWING UPDATED THREAT ALERTS

Sometimes, updates are issued for threat alerts that exist in the system. When an update contains significant changes, Skybox marks the threat alert as for review.

Review these threat alerts and determine whether the threat alerts need different handling after considering the updates.
For example, a specific threat alert is reported on Windows 7 Home only, which is not installed in your organization, so the threat alert was marked as irrelevant. The update states that this threat alert can affect Windows 7 Professional, which is installed in your organization—you decide to open a ticket on the threat alert.

Note: You can create an analysis to display all threat alerts that are marked as For Review.

If you decide that an updated threat alert is relevant to your organization, do any of the following:

> If no ticket exists for the threat alert, create a threat alert ticket and assign it (see Creating threat alert tickets (on page 35)).

  When you create a ticket, the status of the threat alert changes to In Process.

> If a ticket exists for the threat alert, you can make any of the following changes to the ticket:
  - Change the priority or the status.
  - Select a due date for resolution.
  - Add a comment.
  - Select a specific solution to be implemented.
  - Check that the owner of the ticket is the correct staff member to handle this ticket. If not, reassign the ticket.

> If the same issue could be handled by 2 different staff members or teams, clone the original ticket and assign each to a different owner (see Cloning threat alert tickets (on page 31)).

> If the CVSS properties for the threat alert are not correct for your organization, update them (see page 28).

These actions turn off the For Review flag.

If you decide that a specific threat alert is no longer relevant to your organization, mark the threat alert as Irrelevant (see page 27), which closes all tickets for that threat alert and turns off the For Review flag.

If an irrelevant threat alert was updated but remains irrelevant, turn off the For Review flag manually (right-click the ticket and select Clear Review Indication).

**Significant changes**

The following changes cause updated threat alerts to be marked as for review:

> Affected products: Changes to the Product ID, Affected Version, or Running With fields

> CVSS base or temporal score changes (depending on which your organization uses as the source for the severity score)

> Solutions: Changes in the number of solutions (a new solution was added or a solution was deleted)
Other changes (for example, an updated definition, an updated solution, or changes to the CVSS metrics that do not cause a change in the score) are not considered significant enough to warrant review of existing threat alerts.

**Cloning threat alert tickets**

If you need to create additional tickets for a threat alert, you can clone a ticket and change the necessary information. The following instructions explain how to do this.

*To clone a threat alert ticket*

1. Select a ticket:
   - (When working in the Tickets workspace) Select the ticket in the Table pane.
   - (When working in any other workspace) Select the threat alert in the Table pane and then select the ticket in the **Tickets** tab of the Details pane.

2. Right-click the ticket and select **Create Ticket Like**.

   The fields in the New Threat Alert Ticket dialog box have the same values as in the original ticket, except for the read-only **ID** field, which is empty; the new ticket has a different ID number.

3. Select a different owner for the ticket and make other necessary changes.

   The **Threat Alert** cannot be changed.
   - For information about the fields of threat alert tickets, see the Threat alert ticket properties topic in the Skybox Reference Guide.

4. Click **OK**.

**CREATING CUSTOM ANALYSES**

Although Skybox comes with several predefined threat alert analyses, you can create additional analyses (and new folders to contain them) according to your organization’s requirements. For example, you can create separate analyses for threat alerts with specific severities or you can create an analysis for all Windows-related threat alerts of a specific status.

**Admins** can create new analyses in the **Public Analyses** folder; these analyses are visible in the Threat Manager workspace to all users. **Users** can create new analyses in the **Private Analyses** folder; these analyses are visible only to the **User** who created them.

*To create a folder*

1. In the tree, right-click the parent folder of the new folder and select **New > Folder**.

2. In the New Folder dialog box:
   a. Type a name and a description of the folder.
   b. Select the folder type:
      - General
      - Vulnerability Occurrence
      - Ticket
   c. Click **OK**.
To create a threat alert analysis

1. In the tree, right-click the parent folder of the new analysis and select New > Analysis.

2. In the New Analysis dialog box:
   a. Type a Name for the analysis.
   b. In the Type field, select Threat Alerts.
   c. Define the filters to use for this analysis.
      For example, select a specific status or severity, or type a string in the Title field to select the threat alerts that contain this string in their title.
   d. Click OK.

Note: The process of creating analyses for tickets and other entities is the same, but the filter properties are entity-appropriate.

SEARCHING FOR THREAT ALERTS

You can search for threat alerts without creating a permanent analysis for them, using the search function. The search is based on a match between a text string and one of the following threat alert fields:

- Title
- ID
- Description
- Affected Platforms
- Solution Description
- Related Source ID

Threat alerts that match the search string in the specified field are considered matching.

To search for threat alerts

1. Use the search area to the right of the address bar.
2. In the drop-down list, select Threat Alert.
3. In the Search field, type the desired search string (for example, part of the title or the SBV ID).
4. Click Search.
   Threat alerts that contain the search string in any of their fields are listed in the Table pane. The results include threat alerts that have the search string in a possible solution.
5. To search for the string in a specific field, click, and select the name of the field (for example, Title) in the Look in field.
6. Click Search.
   Threat alerts that contain the string in the specified field are listed in the Table pane.
VIEWING VULNERABILITY OCCURRENCES IN THE NETWORK

Skybox can import information from vulnerability scanners and system management products that include vulnerability occurrence information. Many scanners are directly supported; data from those that are not directly supported can be imported using Skybox’s integration XML (iXML).

If your model includes network information from your organization, you can use a scanner to import information about vulnerability occurrences found on assets in the network and then view the relationships between those vulnerability occurrences and the threat alerts.

The **Correlation with Scanners** analysis is a predefined analysis that displays the threat alerts that have vulnerability occurrences in the model.

**To view vulnerability occurrences**

1. In the Threat Manager tree, select **Public Analyses > Reviewed Threat Alerts > Correlation with Scanners**.
2. In the Table pane, select the relevant threat alert.
3. In the Details pane, click the **Vulnerability Occurrences** tab.

All vulnerability occurrences of this threat alert in the network are listed, together with information about them.

4. To view additional information about a specific vulnerability occurrence, select the vulnerability occurrence and then click 🕵️ to zoom in on it.

**Note:** You can create additional threat alert analyses that display only those threat alerts that have vulnerability occurrences in the model. To do this, in the **Basic** tab of the analysis, select the desired source; in the **Advanced** tab, use a value of 1 in the **Instance Count Threshold** field. For information about creating analyses, see [Creating custom analyses](on page 31).
Remediation

Skybox tracks remediation of threat alerts using threat alert tickets, which are requests to fix all occurrences of threat alerts in your organization’s network so that the specified threat alerts cannot harm your organization. Several solutions might be available to fix a threat alert, but some might not be feasible for your organization. The goal of the remediation process is to track assigned threat alert tickets and make sure that they meet their deadlines.

REMEDIATION WORKFLOW

Fixing a threat alert in a large organization requires a series of steps, which might be implemented by several different departments. The following is a typical workflow of a threat alert:

1. An administrator reviews the threat alert and determines whether it is relevant for your organization, using criteria such as whether the threat alert affects products used by the organization. If the threat alert is relevant, the administrator assesses the impact of the threat alert on the organization, creates a ticket, and specifies the time frame (due dates) for the ticket based on the impact. The administrator then assigns the ticket to someone in the Solutions department.

2. The Solutions owner reviews the solutions listed on the ticket and selects those that are relevant for your organization or specifies a custom solution. The Solutions owner then promotes the ticket to an owner in the Testing department.

3. The Testing owner verifies the correctness of the solution and checks that it does not affect your organization negatively. The Testing owner then promotes the ticket to an owner in the Deployment department.

4. The Deployment owner implements the solution, requests to close the ticket, and returns ownership of the ticket back to the administrator who opened it.

5. The administrator reviews the ticket. If the ticket cannot be closed, the administrator adds comments explaining the problem and demotes the ticket to the relevant department for additional work. Otherwise, the administrator closes the ticket.

This workflow can be accomplished informally, with users simply assigning the threat alert’s ticket to the relevant owner in the next team when they finish their work. Alternatively, you can formally model the workflow using ticket phases that are defined by your organization. As users finish their work, they use a promote function to promote the ticket to the next phase and they assign an owner for that phase. (Users can also demote the ticket or decide to skip a specific phase.) You can configure the length of time for each phase of the ticket so that, when a ticket is created, due dates are calculated for each phase.

- For information about remediation without phases, see Working with tickets (on page 35).
- For information about remediation using phases, see Working with tickets and phases (on page 37).
WORKING WITH TICKETS

This section explains how to work with tickets if your organization does not use ticket phases. If your organization does use ticket phases, see Working with tickets and phases (on page 37).

Creating threat alert tickets

When you find a threat alert that should be handled in your organization, you start the remediation process by creating a ticket.

To create a ticket for a threat alert

1. In the Table pane, right-click the threat alert for which you are creating a ticket and select Assign Ticket.
   - For information about the fields of threat alert tickets, see the Threat alert ticket properties topic in the Skybox Reference Guide.
2. If necessary, change the priority of the ticket.
3. Select an owner for the ticket.
4. Click the Browse button next to the CC field to add other people who are to receive email notification about this threat alert.
5. Use Add to select Skybox users; use Add Custom to provide additional email addresses.
6. Select a due date for the ticket.
7. If necessary, define the Network Scope for this ticket.
   - For example, if the affected product is installed in several regions and you want to create a separate ticket for each region, specify the specific network scope in the ticket.
8. The Products tab is filled with all products in the deployed product list to which this threat alert is mapped. You can add additional products from the deployed product list (including custom products) or delete products from the tab.
9. If necessary, select solutions:
   a. Click the Solutions tab.
   b. Select relevant solutions for the ticket.
10. If necessary, create a custom solution (see page 41).
11. Click Save.
   - The ticket is created and added to the list of new tickets for the selected owner.

Note: You can define policies that create tickets for threat alerts based on specific criteria. For example, you can define a policy that creates tickets for all threat alerts with Critical severity reported within the last week (see Configuring policies that create tickets for threat alerts (on page 24)).

Viewing tickets

You can view threat alert tickets:
On a per-threat alert basis: In the Threat Manager workspace, select the threat alert and, in the Details pane, click the **Tickets** tab

Using tickets folders and analyses, which group related tickets

You can view (and create) tickets folders and analyses in the Threat Manager workspace and in the Tickets workspace

For example, **Public Ticket Analyses > All Tickets > Open Tickets > New** contains a list of new tickets assigned to any owner. Tickets with the icon are threat alert tickets.

You can create additional tickets analyses in the Tickets workspace or the Threat Manager workspace, according to your specifications. For example, an analysis that displays only tickets with the following characteristics:

- **New** or **In Progress**
- **High-priority**
- Created for **Threat Alerts** (rather than specific vulnerability occurrences)

You can view additional information about a threat alert ticket from the Details pane, and you can zoom in on the threat alert and vulnerability occurrences.

### Searching for tickets

You can search for tickets without creating an analysis for them. The search is based on a match between a text string and 1 or more of the following ticket fields:

- **Title**
- **ID**
- **User Comments**
- **Status**
- **Priority**
- **Owner**
- **Solution Name**

**To search for tickets**

1. With the Ticket workspace open, click **Search** (on the toolbar).
2. In the Search panel, type a string in the **Find What** field.
3. In the **Look In** field, select the ticket field in which to search for the string.
4. Click **.**

   Tickets that include the search string in the specified field are listed in the Table pane.

### Handling tickets

If ticket notifications are defined, you receive an email alert each time that you are assigned a ticket. Otherwise, you can find your tickets by checking the My Tickets analyses in the Tickets workspace.

When you are assigned a ticket:
Chapter 3  Working with threat alerts

1. Check the relevant tabs.
2. Complete your part of the remediation process.
   For example, if you are responsible for finding solutions for threat alerts, select the relevant solutions; if no solutions are found, you can create a custom solution (see page 41).
3. Do either of the following:
   - Assign the ticket to the owner for the next part.
   - If the remediation workflow for the ticket is finished, change the status of the ticket.

For information about setting up ticket notifications, see Creating notifications (on page 23).

WORKING WITH TICKETS AND PHASES

This section explains how to work with tickets when your organization uses ticket phases. If your organization does not use ticket phases, see Working with tickets (on page 35).

Creating analyses for ticket phases

The Threat Manager workspace includes basic analyses for viewing tickets (All Open Tickets and Recently Closed Tickets) in the Tickets Lifecycle folder.

When working with ticket phases, we recommend that you create custom tickets analyses for tickets in the various phases. This simplifies the work for the ticket owners, who can then find the tickets that they must process. For example, create a Deployment Phase analysis to display all tickets in the Deployment phase. You can create a separate folder for these analyses.

To create an analysis for ticket phases
1. Right-click the folder for the analysis and select New > Analysis.
2. Type a Name for the analysis.
3. In the Analysis Type field, select Tickets.
4. From the Type field, select Threat Alerts.
5. Click the Browse button next to the Ticket Phases field and select ticket phases.
6. Define other desired filters.
7. Click OK.

Creating tickets with phases

When you find a threat alert that should be handled in your organization, you start the remediation process by creating a ticket.

To create a ticket for a threat alert
1. In the Table pane, right-click the threat alert for which you are creating a ticket and select Assign Ticket.
   - For information about the fields of threat alert tickets, see the Threat alert ticket properties topic in the Skybox Reference Guide.
2 If necessary, change the priority of the ticket.
3 Click the **Browse** button next to the **CC** field to add other people who are to receive email notification about this threat alert.
4 Use **Add** to select Skybox users; use **Add Custom** to provide additional email addresses.
5 If necessary, define the **Network Scope** for this ticket.
   For example, if the affected product is installed in several regions and you want to create a separate ticket for each region, specify the specific network scope in the ticket.
6 The **Products** tab is filled with all products in the deployed product list to which this threat alert is mapped. You can add additional products from the deployed product list (including custom products) or delete products from the tab.
7 In the **Phases** tab, assign the owners and due dates.
   By default, the 1st and last phases are assigned to you and no owners are selected for other phases; no due dates are specified for any of the phases.
   a. Assign or change owners as necessary for each phase.
   b. Click **Calculate Due Dates** to calculate the due dates for each phase according to a predefined priority-based formula; you can modify the due dates. If no formula is defined, set the due dates manually.
   
   **Note:** Each ticket priority has its own due date formula. **Admins** can enter these formulas into Skybox. For additional information, see **Ticket phases and due dates** (on page 21).
8 If necessary, select solutions:
   a. Click the **Solutions** tab.
   b. Select relevant solutions for the ticket.
9 If necessary, **create a custom solution** (see page 41).
10 Click **Save**.
   The ticket is created and added to the list of new tickets for the owner of the 1st phase.
   
   **Note:** You can define policies that create tickets for threat alerts based on specific criteria. For example, you can define a policy that creates tickets for all threat alerts with Critical severity reported within the last week (see **Configuring policies that create tickets for threat alerts** (on page 24)).

**Handling tickets with phases**

If ticket notifications are defined, you receive an email alert each time that you are assigned a ticket. Otherwise, you can find your tickets in the following ways:

- If you are responsible for a specific ticket phase, check the analysis for tickets in that phase. (If no such analysis exists, create it in the Threat Manager workspace or the Tickets workspace.)
- In the Tickets workspace, you can check the My Tickets analyses. When working with phases, the status of newly assigned tickets is **New**.
When you are assigned a ticket:

1. Check the relevant tabs.
2. Complete your phase (see Tasks for various phases (on page 39)).
3. In each phase, documents your actions and add additional information when available; you can add comments (in the User Comments tab) and attachments (see page 40).
4. Do one of the following:
   - **Promote** the ticket to the next phase.
   - If additional work is required in the previous phase before you can complete your phase, click **Demote** to demote the ticket to the previous phase.
   - Click **Reassign** to select a different owner for the ticket.

Usually, when you promote or demote a ticket, you must select the owner for the new phase. In some cases, default owners are assigned to each phase, but you can change the owner when necessary.

### Tasks for various phases

While each organization’s ticketing workflow is unique, the following list explains the tasks that are usually performed in each phase of a typical ticket life cycle.

- **Assess Risk**: This phase is for new tickets. In this phase, you define the priority of each ticket according to its risk and associate products to each ticket.
- **Develop Solutions**: In this phase, you review tickets, revise their priority, and select a solution for each threat alert or create a custom solution (see page 41).
- **Integration Testing**: In this phase, you test the solutions provided by the engineers and decide whether to promote the Tickets to the next phase (usually **Deployment**) or to demote them back to the engineers to fix the solutions.
- **Deployment**: In this phase, you deploy the solutions and update the tickets on the progress made using the deployment counters, which keep track of how many occurrences of each issue are resolved. When progress is sufficient, you promote the tickets to an administrator for verification and closure.

### Requesting ticket closure

**Note**: **Ticket Users** cannot close tickets; they can only request that a ticket be closed, which moves it to a special phase where it waits for validation and closure. Tickets must be closed by **Admins** or **Users**.

If at any point in the workflow of a ticket you think that the ticket should be closed, you can request to close it; the ticket is closed by the owner responsible for the final phase of the ticket (usually the same person who created the ticket). When you request to close a ticket, the ticket moves to its final phase for review. When a ticket is in the next-to-last phase, **Promote** also moves the ticket to the final phase.
To request ticket closure

1. Open the Request to Close dialog box:
   - If the ticket Property dialog box is open, click Request to Close.
   - In the Table pane or the Details pane, right-click the ticket and select Request to Close.
2. Select Resolved or Rejected as the status of the ticket that you are requesting to close.
3. Click OK.

Closing tickets

Users and Admins can close tickets at any point in the workflow.

For tickets that are remediated (rather than rejected), wait until the ticket reaches the final phase (usually named Verification) before closing the ticket.

To close a ticket

1. Open the Close dialog box:
   a. If the ticket Properties dialog box is open, click Close.
   b. In the Table pane or the Details pane, right-click the ticket and select Close.
2. Select Closed or Rejected as the status of the ticket that you are requesting to close.
3. Click OK.

Closed, resolved, and rejected tickets are not deleted; you can access them using Search (🔍) or an appropriate tickets analysis (for example, Public Ticket Analyses > All Tickets > Invalid Tickets > Rejected in the Tickets workspace).

ADDING ATTACHMENTS TO A TICKET

To add an attachment

1. Right-click the ticket and select Add Attachment.
2. In the New Attachment dialog box, click the Browse button; locate the required file and attach it to the ticket.
3. In the Description field, type a description of the attachment.
4. Click OK.

ASSOCIATING PRODUCTS WITH TICKETS

Associating products with a threat alert ticket adds important information for the people handling the ticket. By default, a new ticket includes all relevant product entries for the selected threat alert. However, you can decide whether to manage a single ticket per threat alert or to create a separate ticket for each relevant product and manage separate remediation threads for each product.
Use the **Products** tab to select the product or products to associate with a ticket. The products are taken from the deployed product list, which should include all IT products used by your organization.

For information about adding products to the product list, see *Setting up the deployed product list* (on page 18).

**To associate products with a ticket**

1. In the **Products** tab, click **Select Products**.
2. In the Select Products dialog box, select products from the **Available Products** list and click ![add](add) to add them to the **Selected Products** list.
3. Click **OK**.

**CREATING CUSTOM SOLUTIONS**

You can create a single custom solution per threat alert ticket. You can select the custom solution only or you can select it together with predefined solutions.

**To create a custom solution**

1. In the **Solutions** tab, click **Add Custom**.
2. In the New Custom Solution dialog box:
   a. Type a **Name** for the new solution.
   b. In the **Solution Type** field, select the relevant type.
   c. In the **Description** field, type your solution.
   d. Click **OK**.

**SEARCHING FOR TICKETS**

You can search for tickets without creating a permanent analysis for them, by using the search function in the Tickets workspace. The search is based on a match between a text string and a ticket field.

Tickets that match the search string in the specified field are considered matching.

**To search for tickets**

1. With the Threat Manager or Tickets workspace open, click ![Search](search) (on the toolbar).
2. (In the Threat Manager workspace) In the **Search For** field, select **Tickets**.
3. Type a string in the **Find What** field.
4. In the **Look In** field, select the ticket field in which to search for the string.
5. Click ![Search](search).

Tickets that match the string in the specified field are listed in the Table pane.
Reports and CSV

You can view threat alert data offline as:

▶ **Reports** (on page 51)
  - Vulnerabilities reports: Threat alert information, including tickets
  - Tickets reports: Information about tickets and ticket workflows for various threat alerts
  - Threat Alert Management reports: Information about threat alerts

▶ **CSV files** (on page 53)
  - You can export tables in Skybox to CSV files
Chapter 4

Skybox Vulnerability Dictionary

The Skybox Vulnerability Dictionary contains information that enables correlation of Vulnerability Definitions with other vulnerability databases. For example, you can see the cross-references between an iDefense or DeepSight alert, and Nessus, Qualys, and other vulnerability databases in the Vulnerability Dictionary.

When working with Skybox Threat Manager and Skybox Vulnerability Control together, Skybox uses the Vulnerability Dictionary to match between the Vulnerability Definition alerts and the vulnerability occurrences reported by scanners (or by any other means). For example, if you receive an iDefense or DeepSight alert, you can see the infected assets as reported by Nessus, Qualys, and other vulnerability scanners in the Vulnerability Dictionary.

Note: The Vulnerability Dictionary provides important information about Vulnerability Definitions even when using an external alert service as the Vulnerability Definition source.

What information is provided about each threat alert?

Skybox provides information about threat alerts that can help you to decide how to handle each incoming threat alert.

To view threat alert information

1. In the Threat Manager tree, select a threat alert ( ries) analysis.
2. Select a threat alert in the analysis.

Basic information is available in the Table pane and in the General tab of the Details pane.

The following additional information is available in the Details pane:

- **CVSS**: CVSS base and temporal scores.
- **Related Sources**: A single threat alert can have different ID numbers in different public or commercial vulnerability databases.
  
  This tab lists the CVE IDs and Bugtraq IDs of the threat alert provided by most alert services, and the corresponding IDs of the threat alert from sources and vendors that share the same CVE or Bugtraq ID.

- **Skybox Dictionary Products**: The products that are affected by the threat alert. The Mapped in DP List column shows whether the affected products are part of your organization’s deployed product list. If there are products in the deployed product list, create a ticket for the threat alert. If there are no products in the deployed product list, the threat alert can usually be marked as irrelevant.
For additional information about the deployed product list see Setting up the deployed product list (on page 18).

For information about marking threat alerts as irrelevant, see Irrelevant threat alerts (on page 27).

**Affected Platforms:** The products that are affected by the threat alert as they are listed in the Common Platform Enumeration (CPE) dictionary.

CPE names are composed of a descriptive URI:

- `cpe://{part}:{vendor}:{product}:{version}:{update}:{edition}:{language}`

  Where `{part}` is `o` (Operating System), `a` (Application), or `h` (Hardware), and empty blocks cover all possible values (that is, all versions or all editions).

  For example:
  - `cpe:/o:microsoft:windows_xp::sp1` specifies Microsoft Windows XP SP1 (all versions, editions, and languages).
  - `cpe:/a:ibm:tivoli_configuration_manager:4.2` specifies IBM Tivoli Configuration Manager 4.2 (all updates, editions, and languages).

**Tickets:** Tickets created for this threat alert.

- For additional information about a ticket, select the ticket and click ☄.
- For information about creating tickets, see Creating threat alert tickets for threat alerts (on page 35).

**Vulnerability Occurrences:** Vulnerability occurrences of the threat alert in the model.

Vulnerability occurrences are included only if scanner data was imported into the model.

**Solutions:** Known solutions for the threat alert.

**External URLs:** URLs that provide additional information about the threat alert.

**History:** Changes made to the threat alert since it was imported, including the import date, when the review flag was turned on or off, when tickets were created, and changes in the status of the threat alert.
Chapter 5

Using tasks for automation

Scheduled tasks and task sequences can be used in Skybox to automate various processes, including data updates, model maintenance, and reports.

This chapter explains how to work with task sequences and how to schedule tasks and task sequences. For information about using tasks and about each specific task, see the Tasks part of the Skybox Reference Guide.

Note: Only Admins and Users can work with tasks. Admins can work with all tasks; Users can work with a limited range of tasks, including tasks that generate reports and CSV files, tasks that create tickets, and tasks that analyze data.

In this chapter

Task sequences ................................................................. 45
Scheduling tasks and task sequences .......................... 48
Task groups ........................................................................ 49
Monitoring task results .................................................... 49

Task sequences

You can define task sequences, where each task in the sequence runs as soon as a previous task ends. This is useful when you often want to run a set of tasks in a specific order.

You can use separate task sequences for different purposes (for example, data collection and maintenance), different parts of the system, and different frequencies.

A task sequence can include task groups. The tasks in a task group are run in parallel.

For information about tasks, see the Tasks part of the Skybox Reference Guide.

CREATING TASK SEQUENCES

You create a task sequence by creating an ordered set of tasks where each task in the sequence depends on the outcome of another task. If the outcome of the previous task (the triggering task) is not what you specified, the next task is not launched. For example, you can make the Analyze – Simulate Attacks task dependent on a full scan completing with a status of Success: if the full scan completes with any errors that prevent it from having the Success status, the Analyze – Simulate Attacks task is not launched.
Subsequent tasks that depend on a task that was not launched are also not launched. If, in the previous example, the **Generate Risks Details Report** task is the next task in the sequence and it is scheduled to run after the **Analyze – Simulate Attacks** task completes, it does not run.

_to create a task sequence_

1. On the Operational Console toolbar, click ![New Task Sequence](Image).

2. Type a **Name** for the sequence.
3. Keep **Basic** selected as the type of task sequence, and click **Next**.
4. In the Sequence Tasks pane, click **Add**.
5. In the Add Task dialog box, select a task to add to the sequence and click **OK**. The task is added as the 1st task in the task sequence.
6. Add additional tasks to the task sequence:

   Note: A task can only be used once per task sequence. However, you can use different tasks of the same type in a task sequence.
a. Click Add.

The Add Task dialog box now includes additional fields to create a dependency on a previous task.

b. Select a task to add to the sequence.

A dependency is created so that this task runs after the previous task finishes with any of the specified exit codes.

c. To change the triggering task, select a different task in the Depends on Task field.

d. To change the exit codes of the triggering task, click the Browse button next to the Depends on Exit Codes field.

If the triggering task ends with a different exit code, the dependent task is not triggered.

e. Click OK.

7 Click OK.

The new dependency is added to the sequence for this task.

Creating similar task sequences

After a task sequence for a set of tasks is created, you can use it as a template for similar task sequences: Right-click the task sequence and select Create Task Sequence Like.
VIEWING AND EDITING TASK SEQUENCES

*To view task sequences*
1. In the Operational Console tree, select **Tasks > Task Sequences**.
2. Select a task sequence.
   - Tasks in the sequence are listed in the Table pane and general information or messages from the last run of the selected task in the Details pane.

*Editing task sequences*
You can add tasks to and remove tasks from a sequence and change the order of the tasks in the sequence and the exit conditions for the triggering task.

*To edit a task sequence*
1. Right-click the task sequence in the tree and select **Properties**.

Scheduling tasks and task sequences

You can define a task or a task sequence so that it runs at scheduled times (for example, on Sundays at 5 p.m. and Wednesdays at 4 a.m., on the 15th and 28th of every month, or every 15 minutes). Although tasks and sequences are usually scheduled to run on the Live model, you can schedule them to run on any model.

*To schedule a task or task sequence*
1. Navigate to the task or sequence in the Operational Console tree.
2. Right-click the task or sequence and select **Properties**.
3. In the <Task name> Properties dialog box, click the **Schedule** tab.
4. For each schedule (for example, the 1st of every month or every Sunday):
   a. Click **Add**.
   b. Select a time slice and fill in the corresponding fields.
c. If the task is to run a limited number of times, select **End after** and type the number of times that you want the task to run.

d. If necessary, in the **Model** field, change the model on which the task runs.

e. Click **OK**.

The new schedule is added to the list of schedules for this task.

5 Click **OK**.

Note: If auto-launch is not enabled for a task, it does not run on its specified schedules. However, it does run as part of a task sequence.

---

**To view scheduled tasks and sequences**

In the Operational Console tree, select **Tasks > Schedules**.

Defined schedules are listed in the Table pane and the scheduled entities are listed in separate tabs (**Tasks** and **Sequences**) in the Details pane.

---

**Task groups**

You can group a set of tasks together so that you can run them as part of a **task sequence** (see page 45).

When you create a task group, Skybox creates a separate folder for it, where you can view and edit the list of tasks in the group.

Note: You can only run a whole task group as part of a task sequence. Otherwise, you must launch or schedule each task separately. When run as part of a task sequence, the tasks in a task group run in parallel.

---

**To create a task group**

1 On the Operational Console tree, right-click **Task Groups**.

2 In the New Task Group dialog box:

   a. Type a name for the group.

   b. In the **User Comments** field, type a description of the group.

   c. To select tasks to include in this group, click the **Browse** button next to the **Tasks** field.

   d. Click **OK**.

A folder for this group is added under the **Task Groups** node.

---

**Monitoring task results**

**Task messages**

After running a task, you can check the task results to make sure that the outcome is what you expected. For example, after updating firewall configurations (using tasks), check the task results to confirm that all data was properly imported into Skybox. Check for failed tasks; if a task failed, find out why it failed, make the necessary changes, and rerun the update task for the failed firewall.
You can see a list of tasks that failed in the Operational Console window, at **Tasks > Failed Tasks**. For each task, you can see the messages from the task’s most recent run.

**Task alerts**

You can set up Skybox to send email alerts to various users for failed tasks. You can configure global settings and also configure specific settings in the task properties of a specific task. By default, tasks alerts are sent for each task that runs. However, if you do not want task alerts sent for a specific task, you can disable them in the task properties.

To **configure global task alerts**

1. Select **Tools > Options > Server Options > Task Settings > Task Alert Settings**.
2. Do any of the following in the **Email to** field:
   - Type the email addresses to which alerts are to be sent. Multiple addresses must be comma-separated, with no space between the comma and the following address.
   - Click the **Browse** button; select Skybox users who are to receive alerts and add the external email addresses of other desired recipients. All alerts are sent to each specified recipient.
3. Modify the following as necessary:
   - **Email on**: The exit codes on which to send task alerts.
   - **Messages Count**: The maximum number of messages from the failed task to include in the task alert.
4. Click **OK**.
Chapter 6

Reports

Reports in Skybox are detailed accounts of specific data in the model (for example, high-risk entities, threat alerts, overdue tickets, or top 10 entities). You can schedule reports be scheduled to run at specific times and be sent to specified Skybox users.

You work with reports in the Reports workspace.

In this chapter

Tickets reports ................................................................. 51
Vulnerabilities reports .................................................... 52
Threat Alert Management reports ................................. 53
Exporting data to CSV files............................................. 53

Tickets reports

Tickets reports contain summary and detailed information about tickets.

› Overview tickets reports are usually used to review and monitor ticket progress, and to see which tasks are assigned to who.
› Detailed tickets reports are usually used to implement the changes specified in the tickets.

Tickets reports show the status, priority, and assigned owner of tickets that meet the report criteria. You can filter these reports according to many different properties.

For additional information about tickets reports, see the Tickets reports topic in the Skybox Reference Guide.

Predefined tickets reports

Skybox includes the following predefined tickets report definitions:

› **Open Tickets – Overview**: Presents an overview of open Skybox tickets, including the priority, status, and owner for each ticket. The tickets are grouped by priority.
› **Open Tickets – Details**: Presents detailed information about all open Skybox tickets. The tickets are grouped by Priority.
› **Overdue Tickets – Details**: Presents detailed information about all Skybox tickets that are past their due dates, including the status, priority, and owner for each ticket. The tickets are grouped by owner.
Vulnerabilities reports

Vulnerabilities reports are technical reports that contain summary and detailed information about vulnerability occurrences found in the model.

Use these reports to review the vulnerability occurrences in a specific network segment or location, to filter exposed vulnerability occurrences, to show vulnerability occurrences with a specified severity level, or to show vulnerability occurrences that impose the highest risk on your organization. The reports can include trends in vulnerability occurrence statistics.

› In Overview reports, you can see counts of vulnerability occurrences that meet the report criteria. You can group the vulnerability occurrences by operating system, location, Business Units and Business Asset Groups that they affect, and Vulnerability Definitions (also known as threat alerts).

› In Detailed reports, you can see all information about each vulnerability occurrence that meets the report criteria.

› In reports that provide Details & Solutions, you can see all information about each vulnerability occurrence and known solutions for mitigating that vulnerability occurrence.

For additional information about vulnerabilities reports, see the Vulnerabilities reports topic in the Skybox Reference Guide.

LIMITING THE SCOPE OF VULNERABILITIES REPORTS

We recommend that you define vulnerabilities reports with limited scopes to avoid excessively long reports. By default, reports involving vulnerability occurrences are limited to 5000 vulnerability occurrences for Overview reports and 1000 vulnerability occurrences for Details (or Details & Solutions) reports— for detailed reports, Skybox does all analyses based on the first 1000 vulnerability occurrences it finds that match the report definition criteria. The detailed information in a detailed report is limited to the first 50 vulnerability occurrences.

You can limit the scope of vulnerabilities reports by changing any of the following properties of the definition on which they are based:

› The scope of the network to include in these reports
› The type of operating systems to include in these reports
› Any of the vulnerability occurrence properties, including:
  • Imposed risk
  • Status
  • Severity
  • Commonality
  • Vulnerability Definition
  • Scan time
To change the scope of a vulnerabilities report definition

1. Right-click the report definition name in the Tree pane and select Properties.
2. Make the desired scope changes.
   - For information about the properties of vulnerabilities reports, see the Vulnerabilities reports topic in the Skybox Reference Guide.
3. Click OK to save the information and close the Properties dialog box.

Note: An Admin can change the maximum number of vulnerability occurrences to include in reports. This is not usually recommended.

PREDEFINED VULNERABILITIES REPORT DEFINITIONS

Skybox includes the following predefined vulnerabilities report definitions:

- **Vulnerabilities – Details**: Presents detailed information about the vulnerability occurrences in the model.
- **Vulnerabilities – Overview**: Presents an overview of the vulnerability occurrences in the model.
- **Vulnerabilities – Solutions**: Presents detailed information about the vulnerability occurrences in the model and suggested solutions for each vulnerability occurrence.

Threat Alert Management reports

Threat Alert Management reports are technical reports that contain summary and detailed information about threat alerts.

- In Overview reports, you can see a list (by status) of the threat alerts that meet the report criteria.
- In Detailed reports, you can see a list (by status) of the threat alerts that meet the report criteria, and then detailed information about each threat alert, including known solutions and open tickets.

For information about reports about threat alerts, see the Threat Alert Management reports topic in the Skybox Reference Guide.

Exporting data to CSV files

You can export tables that are displayed in the Table pane or the Details pane to CSV files and then open them with an application. For example, if you select a specific threat alert analysis, you can save a table of the threat alerts in that analysis.

You can save tables containing the following types of entities as CSV files:

- threat alerts
- Tickets
To export a table to a CSV file

1. Display a table in the Table pane or in a tab of the Details pane.
   For example, to save the list of high and critical alerts that have tickets, select
   Public Analyses > In Process > High & Critical in the tree.

2. To save specific columns only, make sure that the columns to be saved are
   displayed in the table and that the other columns are hidden.
   - To display or hide columns, right-click in the header row of the table,
     select Customize Current View, and then select or clear columns.

3. Select any row in the table.
   This focuses the Save operation on the selected table.

4. Select File > Export Table to CSV.

5. In the Save dialog box, navigate to the desired location and click Save.
Chapter 7

Maintenance

This chapter describes general maintenance tasks.

In this chapter

Updating your Vulnerability Dictionary ................................... 55
Backing up the model .......................................................... 55

Updating your Vulnerability Dictionary

Skybox Security releases an updated version of the Skybox Vulnerability Dictionary on a weekly basis, with additional versions released within 1 business day of important Vulnerability Definition releases—we recommend that you check for Dictionary updates daily.

There are 2 ways to update the Vulnerability Dictionary:

› (Recommended) Use the predefined Dictionary Update – Daily task, which takes the most up-to-date Vulnerability Dictionary from the Skybox Dictionary Server. You can schedule the task.

Note: The Skybox Vulnerability Dictionary can only be updated by Admins.

For instructions about updating the Vulnerability Dictionary, see the Dictionary updates chapter in the Skybox Installation and Administration Guide.

Backing up the model

The model is backed up to a file in XML or encrypted XML format. You can load backed-up versions and use them for analyses in the What If or Forensics model.

Note: Only Admins can back up and load data.

When backing up and loading the model, the data is divided into 4 components. Make sure that you back up or load the correct components. For additional information, see the Backing up and loading the model topic in the Skybox Installation and Administration Guide.