Radiflow

PERFORMING SIGNATURE DATABASE UPDATES IN iSID

Table of Contents

Executive Summary

This document outlines signatures database updates for iSID Industrial Threat Protection.

Figure 1 - Radiflow iSID Industrial IDS

Overview

iSID is a software tool installed on a dedicated server or as a virtual machine.
It passively monitors the traffic of the industrial network using a copy of the data from the existing network switch via port-mirroring.

Signature Types

Radiflow offers signatures for the Cyber Attack rules database and for iSID Common Vulnerabilities and Exposures (CVE) database.
Hash algorithms and digital signing helps ensure that no rogue file or information can corrupt the existing database.

Signature File Retrieval

When a new signatures file is available an email will be sent to all current customers.
The email will contain a link (or links if required) to securely download the updates.
Additionally, a secure, password protected section is available on the Radiflow website to download signature files as necessary (https://radiflow.com/support/)

Signature Update Timeframe

Emails with the signature file link will be sent to current customers quarterly.
As was mentioned in the previous section, users can also download the signature files more frequently from the Radiflow website.
Radiflow may initiate emergency updates from time to time - We will inform our customers of such updates via email.

Signature Integrity

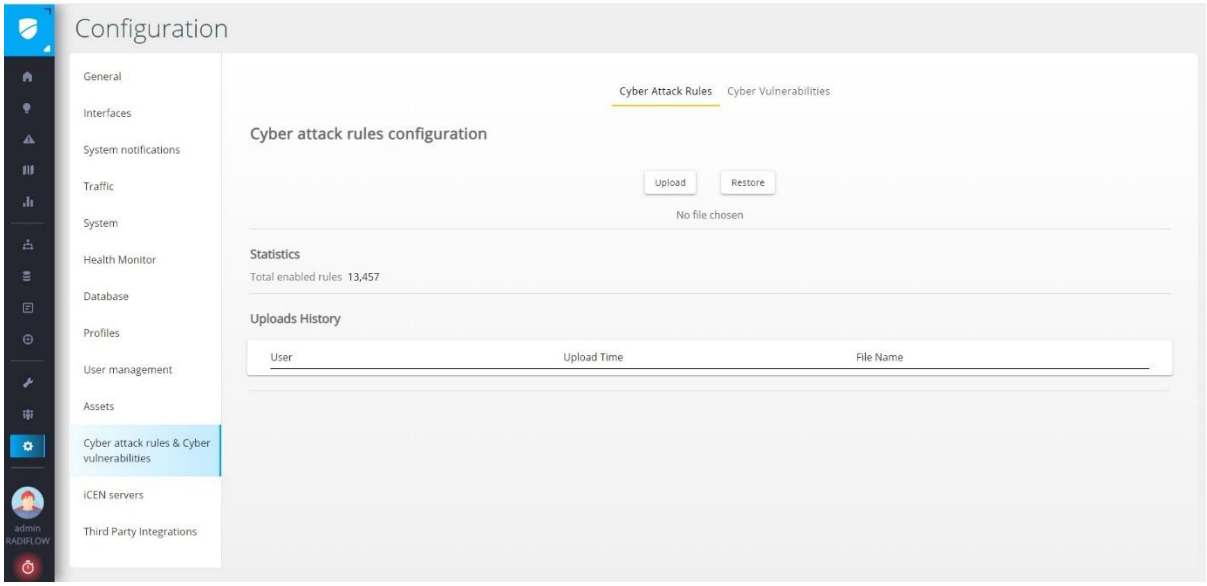
The download link, whether from an email or from the Radiflow website, will contain a SHA-256 hash to verify data integrity.
All signature files are RSA digitally signed.

Update Procedure

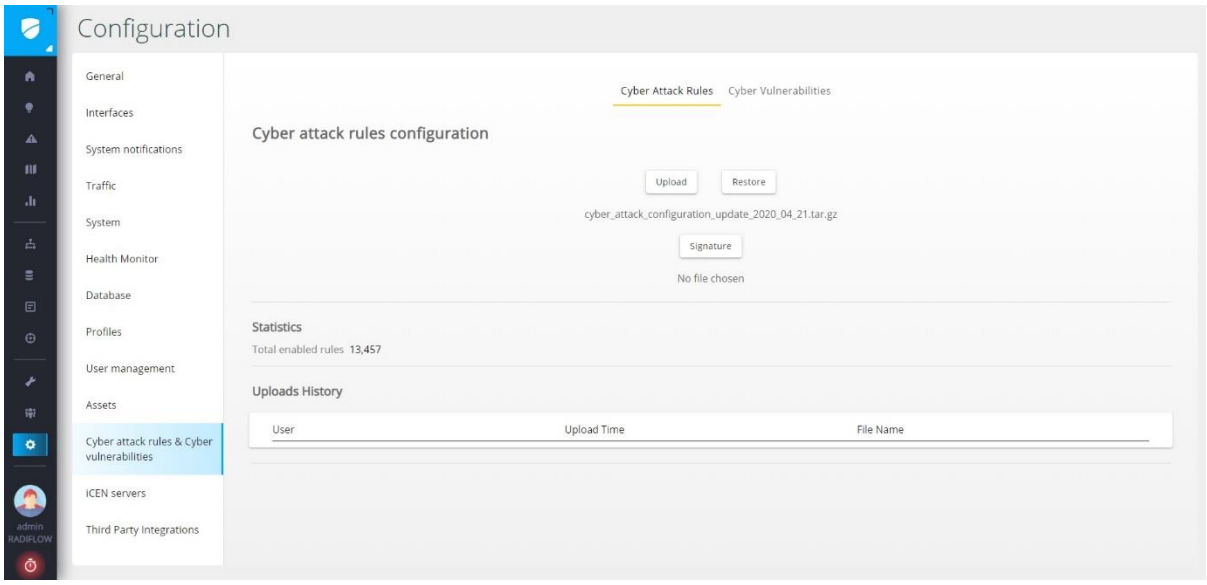
The customer is responsible for downloading the file and transferring it to the secure operational environment, to a location that can be accessed by iSID.

1. Browse to Configuration -> Cyber attack rules & Cyber vulnerabilities

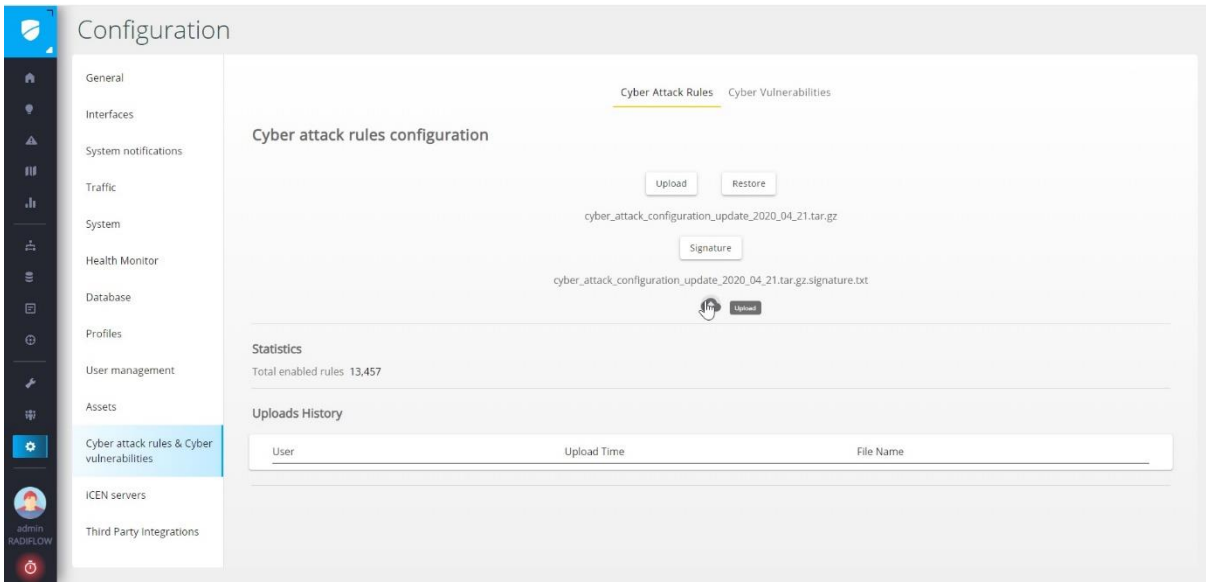
2. Click on ‘Upload’ button under the tab of the package you wish to update (cyber-attack or CVE), and select the update file



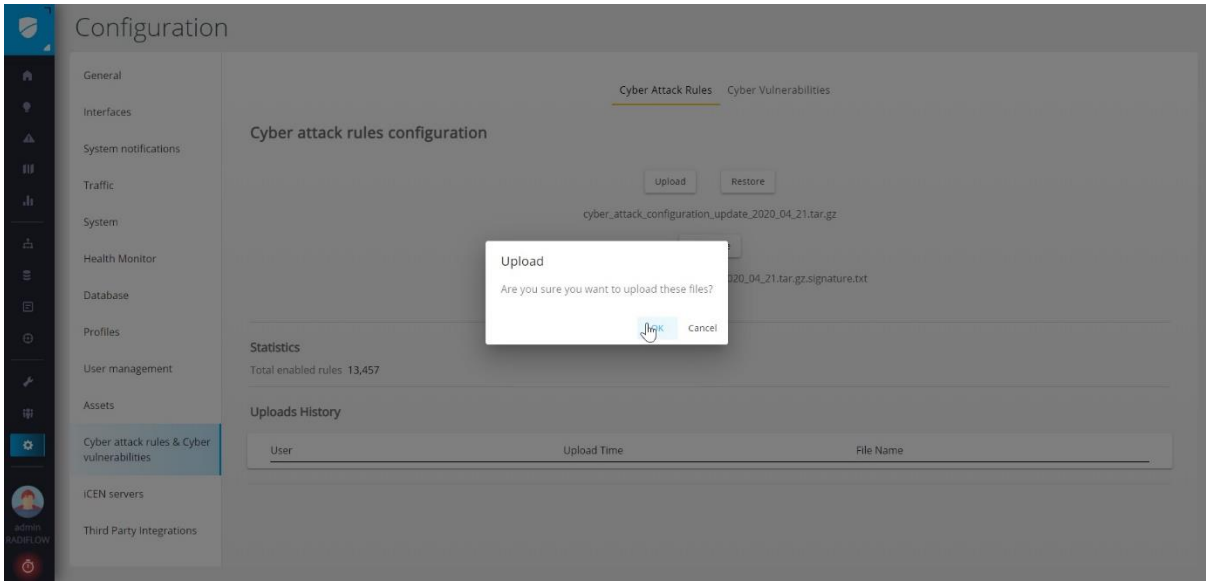
3. Click on ‘Signature’ button and select the signature file



4. Click on ‘Upload’ button



5. Confirm that you wish to perform an update



6. A notification will appear after the update was completed successfully, and the ‘Uploads history’ table will be updated