# PERFORMING SIGNATURE DATABASE UPDATES IN iSID

THIS CONTROLLED DOCUMENT IS THE PROPERTY OF RADIFLOW LTD. This document contains proprietary information. Any duplication, reproduction or transmission to unauthorized parties without prior permission of Radiflow is strictly prohibited. (C) Radiflow LTD. 2022

#### **Table of Contents**

Executive Summary	.3
overview	3
Signature Types	3
Signature File Retrieval	3
Signature Update Timeframe	3
Signature Integrity	3
Update Procedure	3
Update Procedure	3

#### **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 (<u>https://radiflow.com/support/</u>)

#### 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 (cyberattack or CVE), and select the update file

0	Configuration			
6 9 4	General Interfaces	Cyber attack rules configuration	er Attack Rules Cyber Vulnerabilities	
00 .h	System notifications Traffic System	Upload Restore No file chosen		
-17 939	Health Monitor Statistics Total enabled rules 13,457 Database			
•	Profiles User management	Uploads History User Upload Time	File Name	
<b>チ</b> 中	Assets			
	Cyber attack rules & Cyber vulnerabilities			
admin RADIFLOW	Third Party Integrations			

3. Click on 'Signature' button and select the signature file

8	Configuration		
▲	General Interfaces System notifications Traffic System Health Monitor Database	Cyber Attack Rules Cyber Vulnerabilities Cyber attack rules configuration Upload Restore cyber.attack.configuration.update.2020.04.21.tar.gz Signature No file chosen	
•	Profiles User management Assets	Statistics Total enabled rules 13,457 Uploads History	
192	Cyber attack rules & Cyber vulnerabilities	User Upload Time File Name	
admin RADIFLOW	ICEN servers		

4. Click on 'Upload' button

	Configuration			
•	General	Cyber Attack Rules Cyber Vulnerabilities		
A	Interfaces System notifications	Cyber attack rules configuration		
ni di	Traffic	Upload Restore		
÷.	System Health Monitor	cyber_attack_configuration_update_2020_04_21.tar.gz Signature		
e	Database	cyber_attack_configuration_update_2020_04_21.tar.gz.signature.txt		
•	Profiles	Statistics		
۶ 	User management. Assets	Total enabled rules 13,457		
•	Cyber attack rules & Cyber vulnerabilities	User Upload Time File Name		
٩	ICEN servers			
admin RADIFLOW	Third Party Integrations			

5. Confirm that you wish to perform an update

	Configuration	1		
n	General	Cyber Attack Rules Cyber Vulnerabilities		
. *	Interfaces			
•	System notifications	Cyber attack rules configuration		
	Traffic	Upload Restore		
	System	cyber_attack_configuration_update_2020_04_21.tar.gz		
÷.	Health Monitor	Upload		
8	Database	Are you sure you want to upload these files?		
Θ	Profiles	Statistics		
+	User management	Total enabled rules 13,457		
0	Assets	Uploads History		
٥	Cyber attack rules & Cyber vulnerabilities	User Upload Time File Name		
	ICEN servers			
admin RADIFLOW	Third Party Integrations			
Ō				

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

	Configuration			
• • • •	General Interfaces System notifications Traffic System	Cyber attack rules confi	Cyber Attack Rules Cyber Vulnerabiliti guration Upload Restore No file chosen	25
Health Monitor     Statistics     Total enabled rules 13,457     Database     Uploads History     Profiles				
<u>ب</u>	User management Assets	User Radiflow	Upload Time Apr 28, 2020 23:50:44	File Name cyber_attack_configuration_update_2020_04_21.tar.gz
•	Cyber attack rules & Cyber vulnerabilities			
admin RADIFLOW	ICEN servers Third Party Integrations			