



# BANDURA®

## Creating Denied Lists using H-ISAC Threat Intelligence


### What

H-ISAC is a global, non-profit, member-driven organization offering healthcare stakeholders a trusted community and forum for coordinating, collaborating and sharing vital physical and cyber threat intelligence and best practices with each other.

Bandura Cyber provides easy integration with H-ISAC to leverage threat intelligence allowing customers who are H-ISAC members to create denied lists using IPv4 and Domain indicators of compromise that will be used to block malicious traffic.

### How

When creating a Denied List using H-ISAC threat intelligence, you'll want to make sure you have the correct credentials for accessing H-ISAC data from the Cyware CTIX platform.

To create a list, log into the Bandura console and select either Denied or Allowed from the left menu, then choose either IPv4 or Domain. Click the green plus icon  in the top right corner. In the Create Denied or Allowed List modal that opens, Choose "H-ISAC" from the Type dropdown. Give your list a name (required) and add a description if you wish (optional). The minimum available Interval in Minutes is 720, this represents how often we will check for updates to the H-ISAC feed.

Next, you'll need to choose the feed you wish to pull indicators from. H-ISAC members will want to pull the "Amber Members" field, so select that option from the dropdown. Select the number of hours you wish the indicators to stay active in the list (our recommendation is 720). Finally,

select the radio button for the “Basic” Authentication Type and enter your username and password credentials as provided by H-ISAC.

Modal form titled "Create IPv4 Denied List" with the following fields and values:

- Enabled:
- Type: H-ISAC
- Feed Name: H-ISAC AMBER MEMBERS
- Name: H-ISAC
- Description: Threat Intelligence from H-ISAC
- Interval in Minutes: 720
- TTL Hours: 720
- Authentication Type: Basic (selected)
- User Name: member-username
- Password: [masked]

After you have filled out the fields in the plugin modal, click on “Create” to add your new list. You will see the newly created entry on your list. Please note that it may take 10-15 minutes to begin pulling the indicators from H-ISAC.

Enabled	Type	Name	Description	Entries	Last Sync	Last Update
<input checked="" type="checkbox"/>	Manual	Bandura Healthcare Ransomware	List of IP IOCs curated by Bandura Cyber	289	-	11/06/20 10:38:09 AM
<input checked="" type="checkbox"/>	Automatic	Blocklist.de	IP RBL (all)	24,368	05/20/21 2:33:14 PM	05/20/21 2:33:14 PM
<input checked="" type="checkbox"/>	Automatic	CINS Army list	cinsscore.com Active Threat Intelligence	15,000	05/20/21 2:16:15 PM	05/20/21 2:16:15 PM
<input checked="" type="checkbox"/>	Automatic	DHS Information Sharing	DHS Information Sharing	1,138	05/20/21 2:35:05 PM	05/20/21 2:31:04 PM
<input checked="" type="checkbox"/>	Automatic	ET Block IPs	Emerging Threats Blocked IPs	1,253	05/20/21 2:14:19 PM	05/19/21 6:31:19 PM
<input checked="" type="checkbox"/>	Automatic	ET Compromised IPs	Emerging Threats Compromised IPs	2,773	05/20/21 2:13:27 PM	05/13/21 6:35:16 PM
<input checked="" type="checkbox"/>	Automatic	Feodo	Feodo feed from abuse.ch	212	05/20/21 2:13:16 PM	05/20/21 1:11:14 PM
<input checked="" type="checkbox"/>	Automatic	H-ISAC	Threat Intelligence from H-ISAC	94	05/20/21 2:34:50 PM	05/20/21 2:34:50 PM

If you have any questions or need assistance in setting up H-ISAC Denied Lists please contact the Bandura Support team at [support@banduracyber.com](mailto:support@banduracyber.com) or by calling +1-855-765-4925.