threatER Portal Release Notes

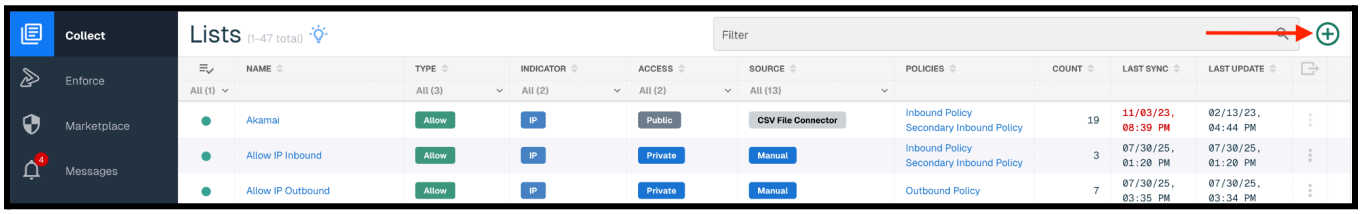
Build 204: November 12, 2025

New Feature: Customer Configurable DomainTools Domain Plugin

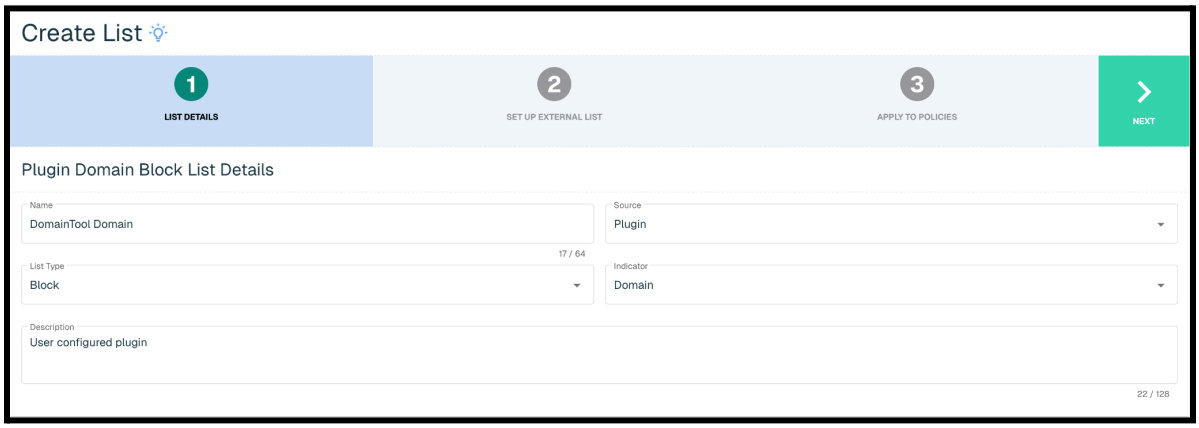
Customers now have the ability to configure and customize their own DomainTools Domain plugin directly in the threatER Portal. This gives you more control over your threat intelligence, allowing you to fine-tune risk score thresholds to achieve better precision and flexibility.

To set up your customized DomainTools Domain feed:

- Navigate to Collect
- Click on the "+" in the top-right corner



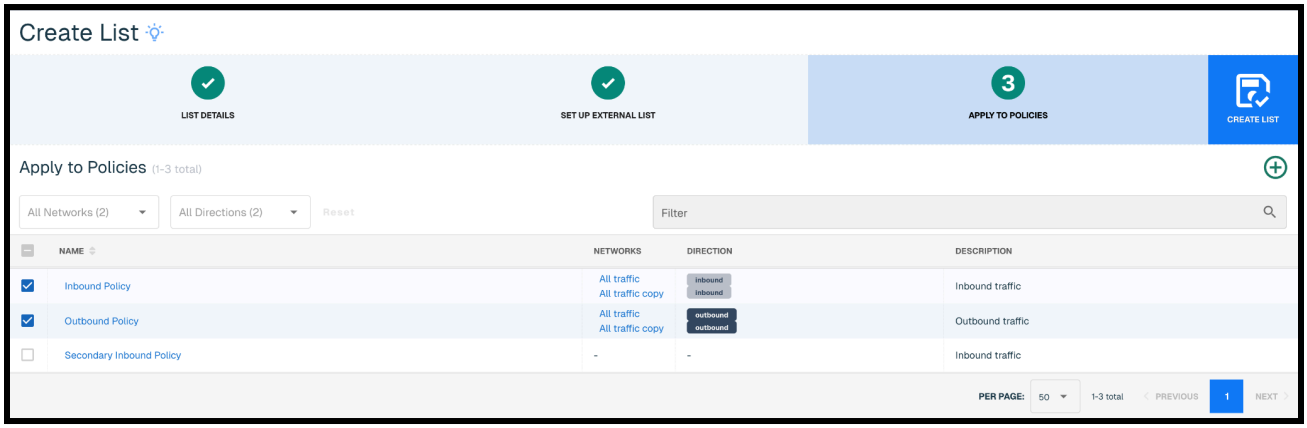
- Enter a name for the plugin (required)
- Select "Plugin" from the Source drop-down
- Select "Block" from the List Type drop-down
- Select "Domain" from the Indicator drop-down
- Enter an optional description
- Click "Next" in the wizard workflow



- On Step 2, select "DomainTools" from the plugin drop-down
- Enter an interval

- Toggle the risk score you wish to enable and set the desired score threshold
    - See below for more information on scoring
- Click “Next” in the wizard workflow

- On Step 3, select the Policies you want the list to be enabled on
- Click Create List in the wizard workflow



This list is now created and will pull entries from the DomainTools Domain feed, based on the risk scores enabled and score thresholds set. **PLEASE NOTE:** it may take up to 24 hours for the feed to initially populate with entries.

DomainTools Risk Score Reference

For guidance on configuring your score thresholds, consult the following details on the DomainTools scoring model.

Available Scores:

Score Type	Description
Overall Risk	The final score of a domain, calculated by taking the highest of the Threat Profile scores and the Proximity score.
Proximity	Quantifies the closeness of a domain to known-malicious domains. Indicates the likelihood of malicious intent based on registration details and hosting infrastructure.
Threat Profiles	Machine learning scores tuned for specific threat categories: **Malware**, **Phishing**, and **Spam**.

Domain Risk Score Ranges

Score Range	Description
100	Blocklisted - these domains have the highest likelihood of malicious intent.
90–99	Strong Confidence in near-term weaponization.
70–89	Default Recommendation - a potential threshold for suggesting malicious intent and significance in an investigation, depending on your security context and priorities.
50–69	Requires attention, depending on your organization's security posture.
1–49	Very little evidence of malicious intent.
0	Zero-listed. Domains that have no evidence of malicious intent and are often vital to the expected operation of the Internet.

Please note: The existing, out-of-the-box DomainTools Domain feed is still available to all customers. This feed consists of Domains that have an Overall Risk Score of 99-100. Additionally, a domain categorized as Spam is filtered out when the other categories have null scores.