### Indicators

#### Overview

Indicators of compromise (IoCs) are digital evidence that indicate a system or network has been compromised, serving as essential information for detecting and responding to security threats. By registering IoCs in the product, users can detect threats in real-time and minimize damage during security incidents through automated responses. Timely registration and utilization of IoCs play a crucial role in enhancing an organization's security posture.

IoCs can be registered and utilized in the following situations:

**When collecting external threat intelligence**

* If new threat information is received from trusted external organizations or services such as Computer Emergency Response Teams (CERT), Information Sharing and Analysis Centers (ISAC), or security vendors, this information should be registered as IoCs.
* Example: If a specific IP address or domain is reported to be associated with malicious activity, that information can be registered to monitor and block all interactions with that IP or domain.

**When suspicious activities are detected in internal security logs**

* If suspicious IP addresses, domains, or file hashes are discovered through the analysis of security logs or events occurring within internal systems, these should be registered as IoCs.
* Example: If logs indicate repeated connection attempts to suspicious external IP addresses from within the internal network, that IP can be registered as an IoC to automatically block it or set up additional monitoring.

**When phishing attempts or malicious emails are identified**

* If phishing emails or emails containing malicious attachments are received, the email addresses, domains, and hash values of the attachments should be registered as IoCs to prevent other users from being exposed to the same attack.
* Example: If a specific email address is confirmed to have been used for sending phishing emails, that address can be registered as an IoC to block all emails from it.

**When malware infections are confirmed**

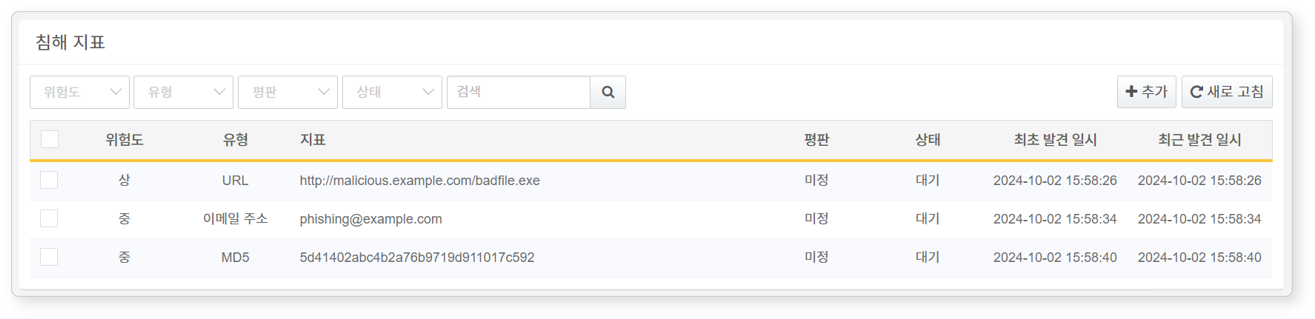
* If a malware infection is confirmed on a system, the MD5 hash value of the malware file should be registered as an IoC to prevent the same malware from spreading to other systems.
* Example: If a file's hash value is registered as an IoC on a system where malware was detected, immediate action can be taken if the same hash value is found on other systems.

**When similar patterns are discovered during security threat investigations or responses**

* If specific IPs, domains, or URL patterns that attackers repeatedly use are discovered during incident response, these can be registered as IoCs to preemptively block similar attacks that may occur in the future.
* Example: The URL pattern of a malicious website discovered during an investigation can be registered as an IoC to block access to URLs with the same pattern in the future.

#### Viewing/Search for Indicators

You can view or search the list of IoCs under **Policies > Indicators**.



* **Severity**: The severity of the IoC (Normal, Low, Medium, High)
* **Type**: The type of IoC (IP Address, Domain, URL, MD5, Email Address)
* **Indicator**: The value of the IoC
* **Reputation**: The reputation of the IoC
* **Suspicious**: The IoC is suspected of being a threat based on reputation verification results
* **Undetermined**: The reputation of the IoC has not been verified
* **Status**: The status of the IoC (Pending, Completed, Error, Retry)
* **First Detected Date/Time**: The date and time the IoC was discovered and added
* **Last Detected Date/Time**: The date and time the IoC was last detected

To find a specific IoC scenario in the list, use the search tool in the toolbar. The search tool will display IoCs that include the entered term in their indicator items. The search tool is case-insensitive.

Refresh List

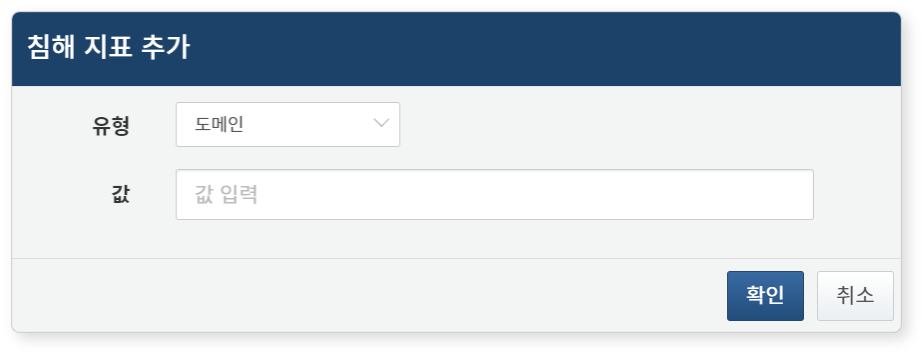
To refresh the list of IoCs with the latest information, click **Refresh** in the toolbar.

#### Adding Indicators

To add an IoC:

Click **Add** in the toolbar under **Policies > Indicators**.

In the **Add Indicator** dialog, configure the basic settings.



* **Type**: Type of the IoC (Range: IP/Domain/URL/MD5/Email Address)
* **Value**: The value of the IoC based on its type

#### Changing Indicator Severity

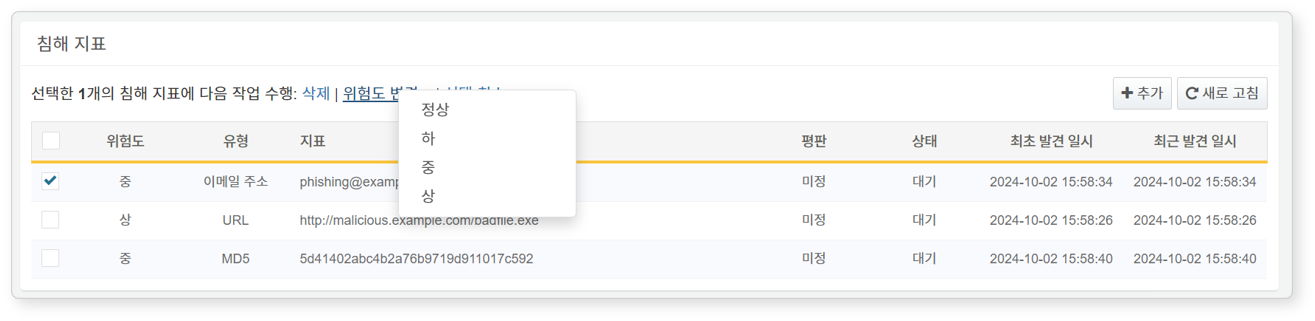
Severity can be changed in two ways: by clicking on the severity of a specific IoC for individual changes or by using checkboxes for bulk changes.

To change the severity of an IoC individually, click on the severity of the target IoC. Users can set and change the severity in the modal window that opens for the clicked IoC.

To change the severity of IoCs:

Select the checkbox for the IoC you wish to modify in the IoC list. To bulk modify the severity of multiple IoCs, select several checkboxes.

The action menu will appear in the toolbar. Click **Change Severity** in the action menu and select the desired severity level (Range: Normal, Low, Medium, High).



#### Deleting Indicators

To delete an IoC:

Select the checkbox for the row of the IoC you wish to delete in the IoC list.

* An expanded menu will appear.

Click **Delete** in the expanded menu.

#### Utilizing Indicators

The added IoCs can be configured and used in the following ways:

* Playbook start triggers
* Commands in the playbook command set related to updating IoC information