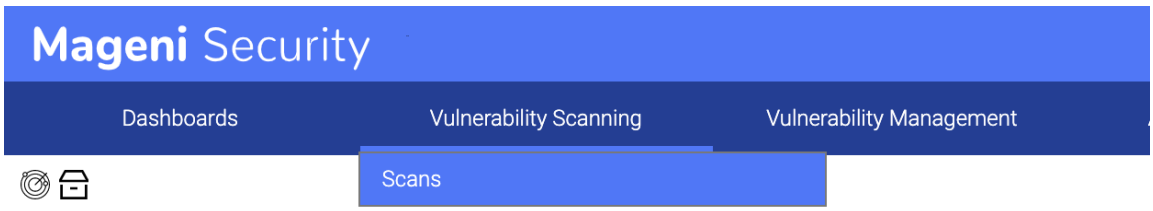
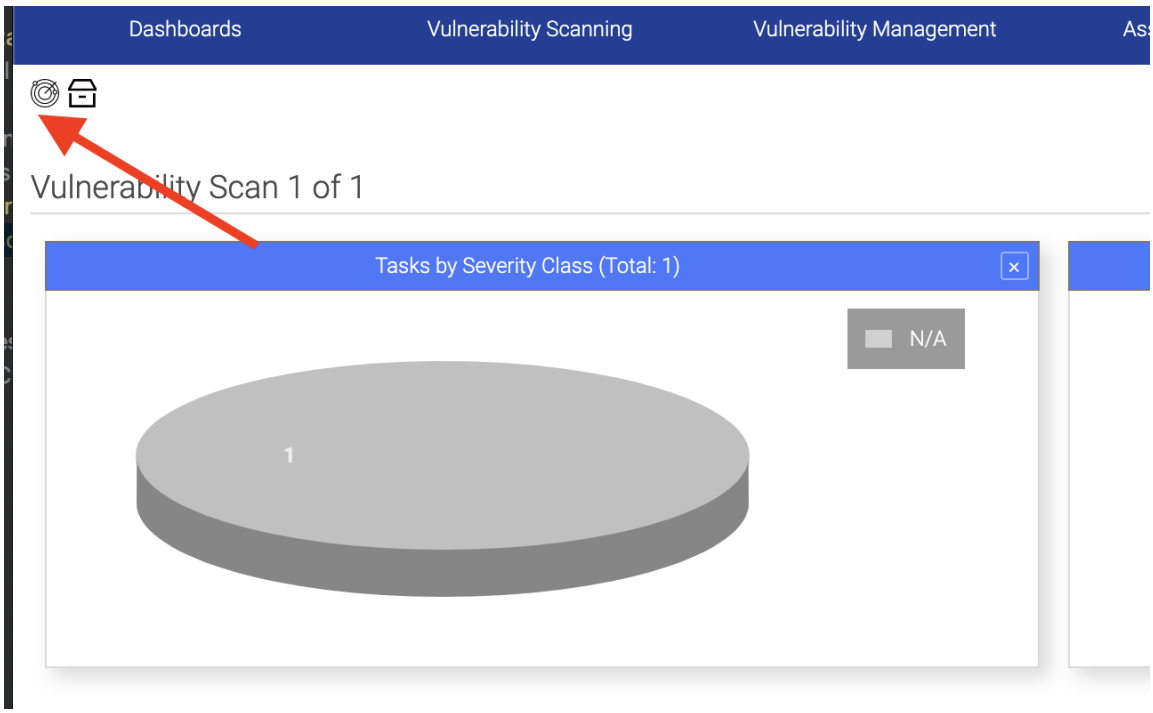
Vulnerability Scan

Run a Vulnerability Scan

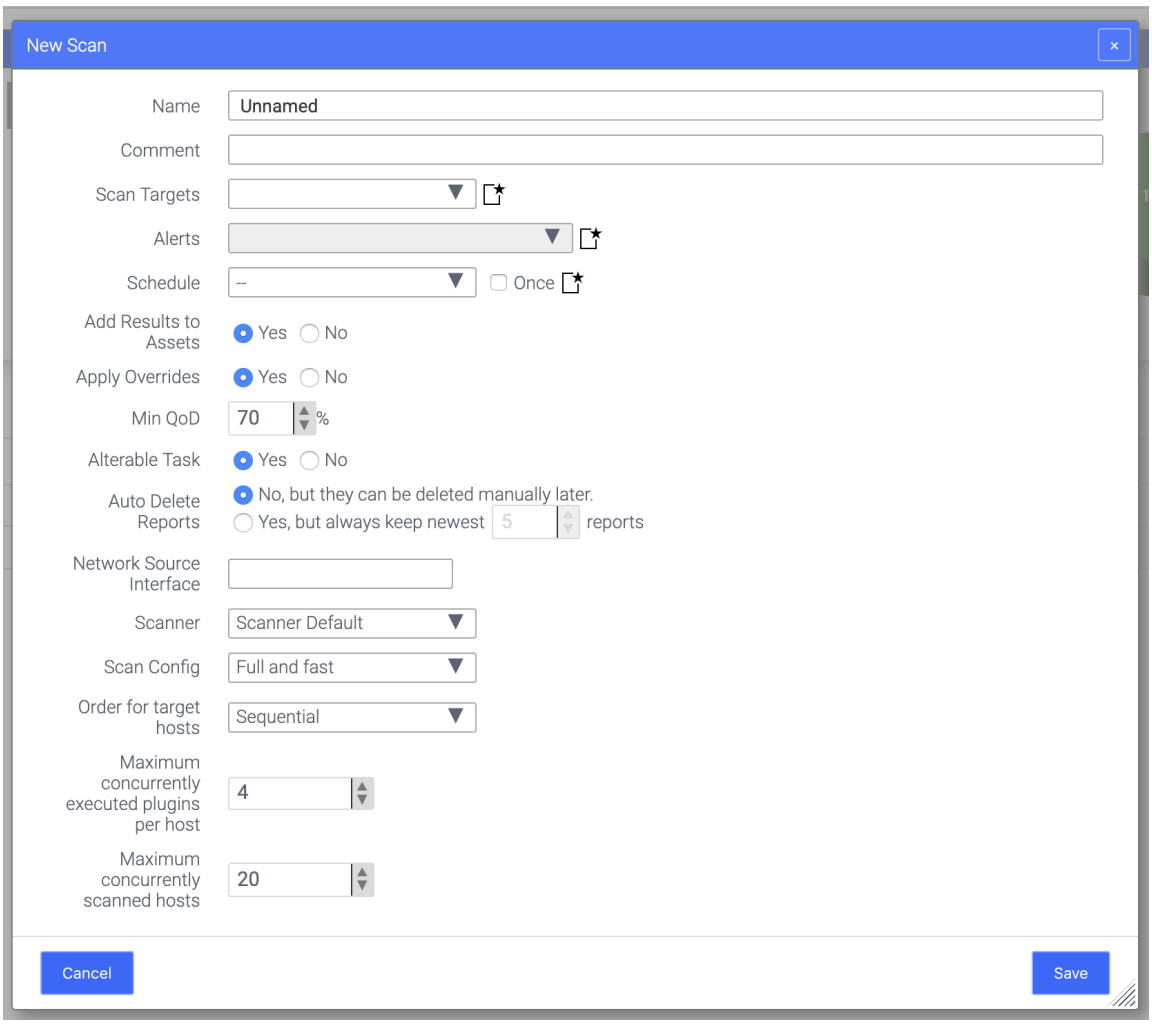
To run your first vulnerability scan in the top navigation bar, click **Vulnerability Scanning > Scans** .



The Vulnerability Scanning page will show up and you can click on the icon **Create a New Vulnerability Scan**

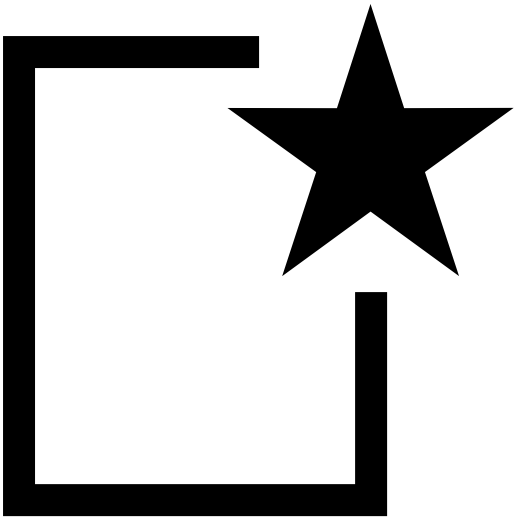
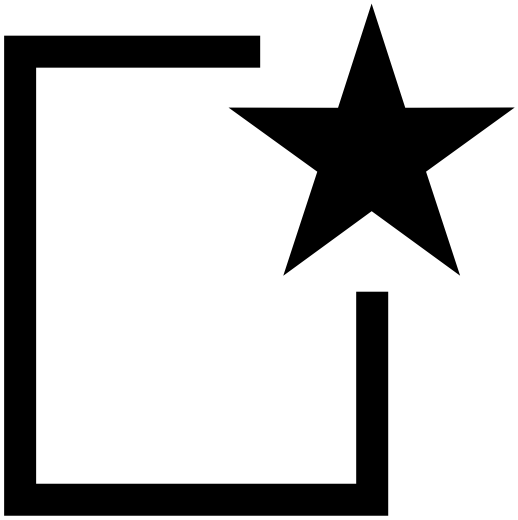


The **New Scan** window appears. From there, you can create a vulnerability scan:

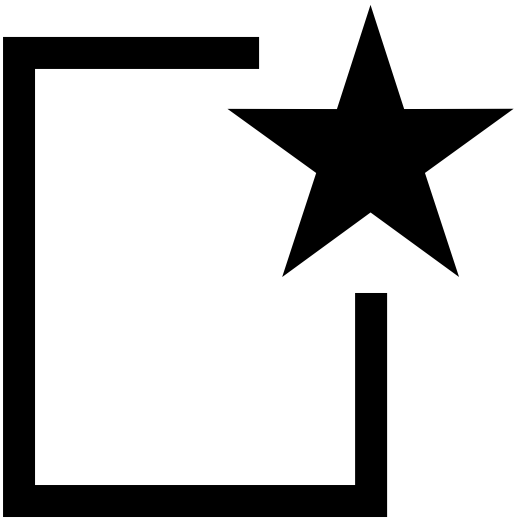

New Scan
Name
Unnamed
Comment
Scan Targets
Alerts
Schedule
--
Once
Add Results to Assets
Yes
No
Apply Overrides
Yes
No
Min QoD
70
%
Alterable Task
Yes
No
Auto Delete Reports
No, but they can be deleted manually later.
Yes, but always keep newest
5
reports
Network Source Interface
Scanner
Scanner Default
Scan Config
Full and fast
Order for target hosts
Sequential
Maximum concurrently executed plugins per host
4
Maximum concurrently scanned hosts
20
Cancel
Save

Understanding the Terms

New Scan Window

1. **Name:** Name of the vulnerability scan. For example: "Web Servers"
2. **Comment:** If you want to insert a comment in the vulnerability scan. For example: "Web Servers in NYC Location"
3. **Scan Targets:** The assets that you want to scan, you must define them clicking on  you can **create an asset**
4. **Alerts:** You can **define alerts** clicking on  for your vulnerability scan allowing you to be notified of some security events.

5. **Schedules:** You can program schedule scans to run automatically, on a regular basis. This way you always have the most up-to-date information. To create a new Schedule, click on



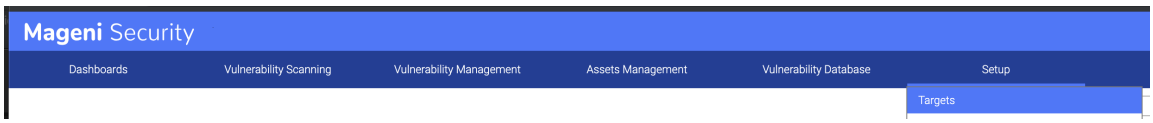
6. **Add Results to Assets:** If you want to see the asset in the scan and its results in the asset management dashboard. *Recommended to say Yes*
7. **Apply Overrides:** If you want to modify the results to change the score or report false positives/negatives. *Recommended to say Yes*
8. **Min QoD:** The minimum quality of detection.
9. **Alterable Tasks:** If you want to modify the scan later, say yes; if you don't want to modify it, say no. *Recommended to say Yes*
10. **Auto Delete Reports:** You can leave it at *No* and they can be deleted later, or specify a number of reports that you want to keep in the database.
11. **Network Source Interface:** The Network Card of the Appliance that will be used to launch the attacks.
12. **Scanner:** Scanner Type, you can chose only one of two (2):
    a. **Scanner Default:** To perform traditional vulnerabilities scans.
    b. **CVE:** To look only for CVEs in the targeted assets.
13. **Scan Config:** Scan Policy used to test an asset.
14. **Order of target hosts:** The order in which you want to scan a network. It could be random, sequential and reverse.
15. **Maximun concurrently executed plugins per host:** The maximum number of plugins executed per hosts.
16. **Maximun concurrently scanned hosts:** The maximum number of hosts scanned simultaneously.

Video Create a Scan

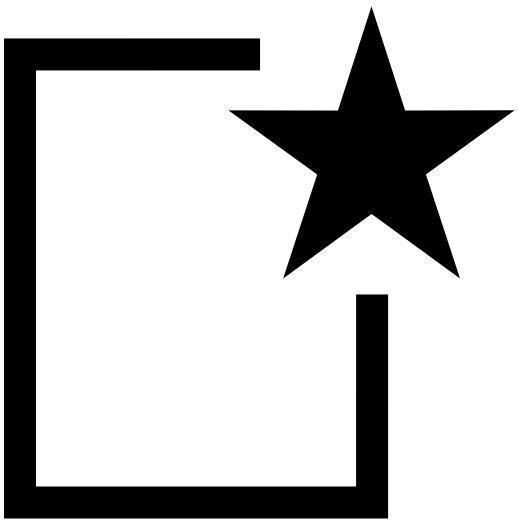
Assets Creation

How to create a Target

To create a target in the top navigation bar, click **Setup > Targets**.

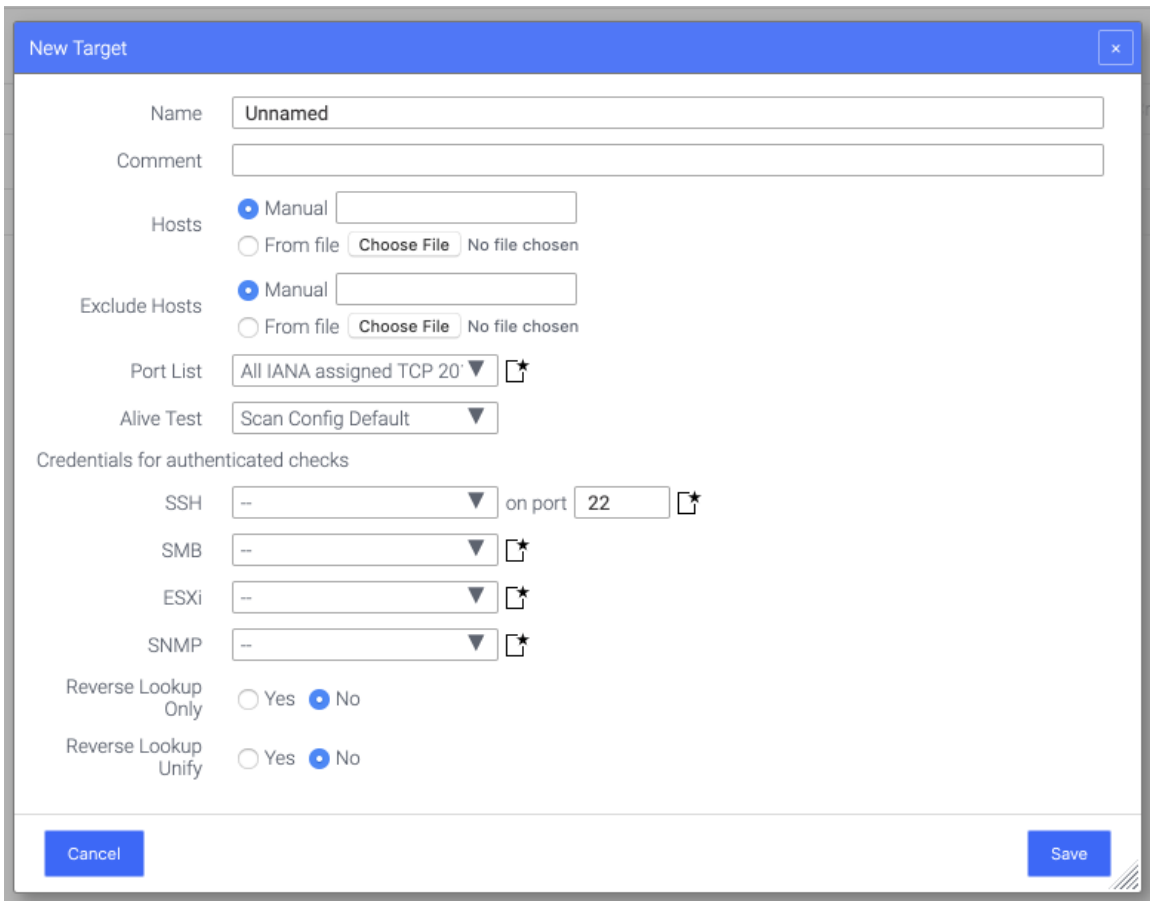


The Target Creation page will show up and you can click on the icon



New Target

The **New Target** window appears. From there, you can create a target:



Understanding the Terms

To create a target, you'll need to understand these simple terms.

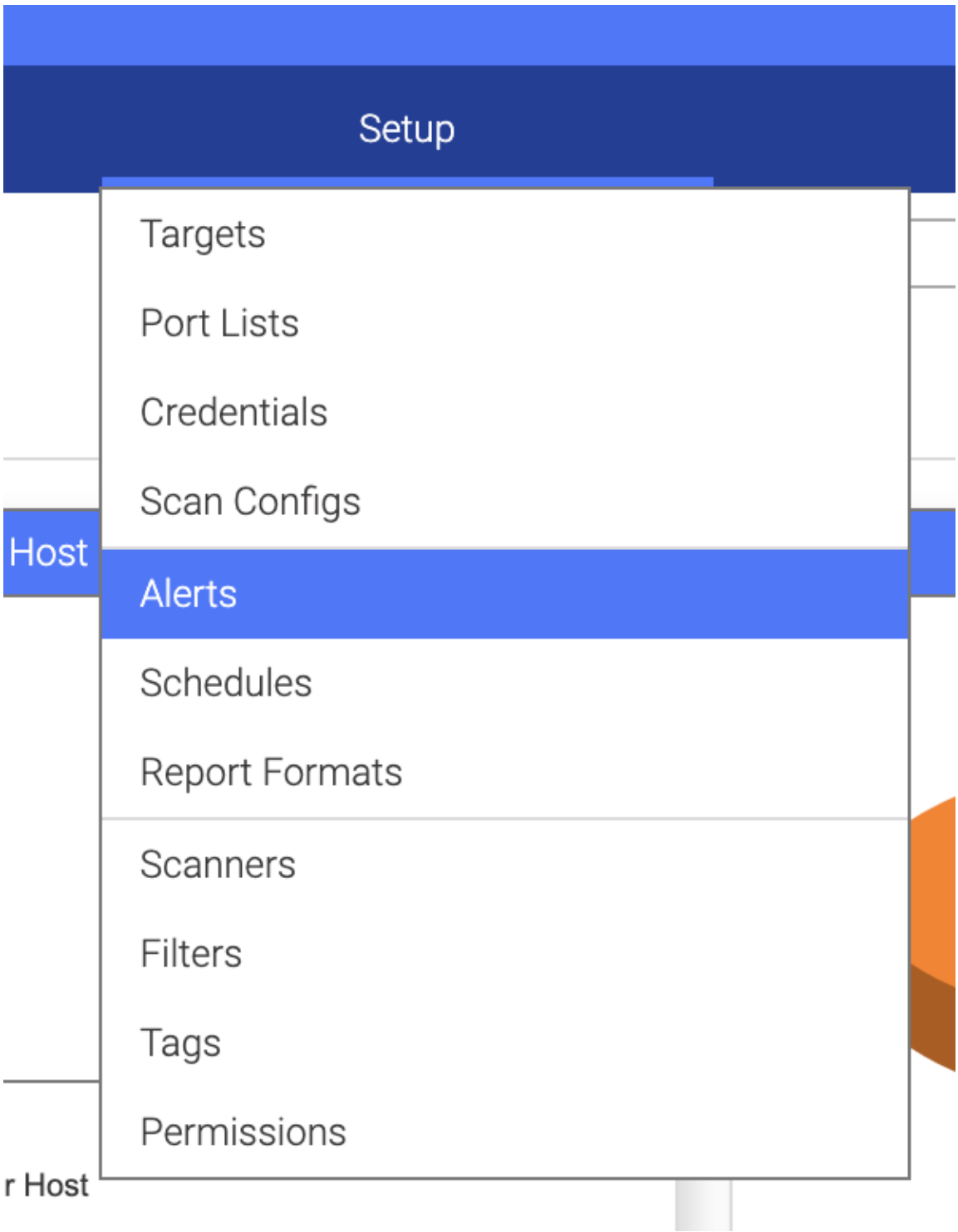
Terms:

1. **Name:** Name of the asset. For example: "Web Servers"
2. **Comment:** If you want to insert a comment. For example: "Web Servers in NYC Location"
3. **Hosts:** The assets that you want to scan.
4. **Exclude Hosts:** The assets you want to exclude from the scan.
5. **Port List:** The port range or list that you want to scan in the assets.
6. **Alive Test:** Specifies how to know if the asset is alive.
7. **Credentials:** Specifies the credentials for authenticated scans.
8. **Reverse Lookup Only:** The scanner will scan only the IP addresses that can be resolved into a DNS name.
9. **Reverse Lookup Unify:** If multiple IP addresses resolve to the same DNS name, like a Load Balancer, the FQDN will only get scanned once.

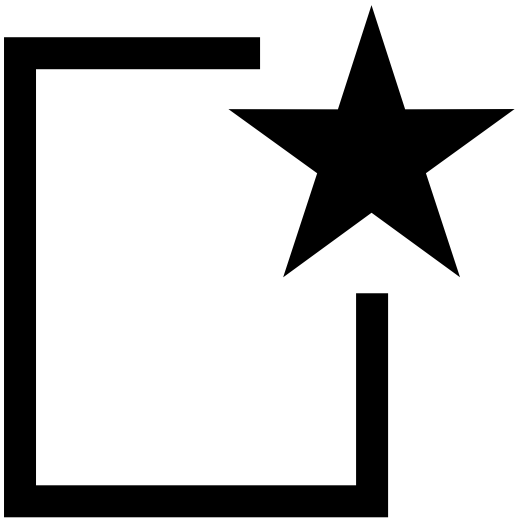
Alerts Creation

How to create an Alert

To create a target in the top navigation bar, click **Setup > Alerts**.

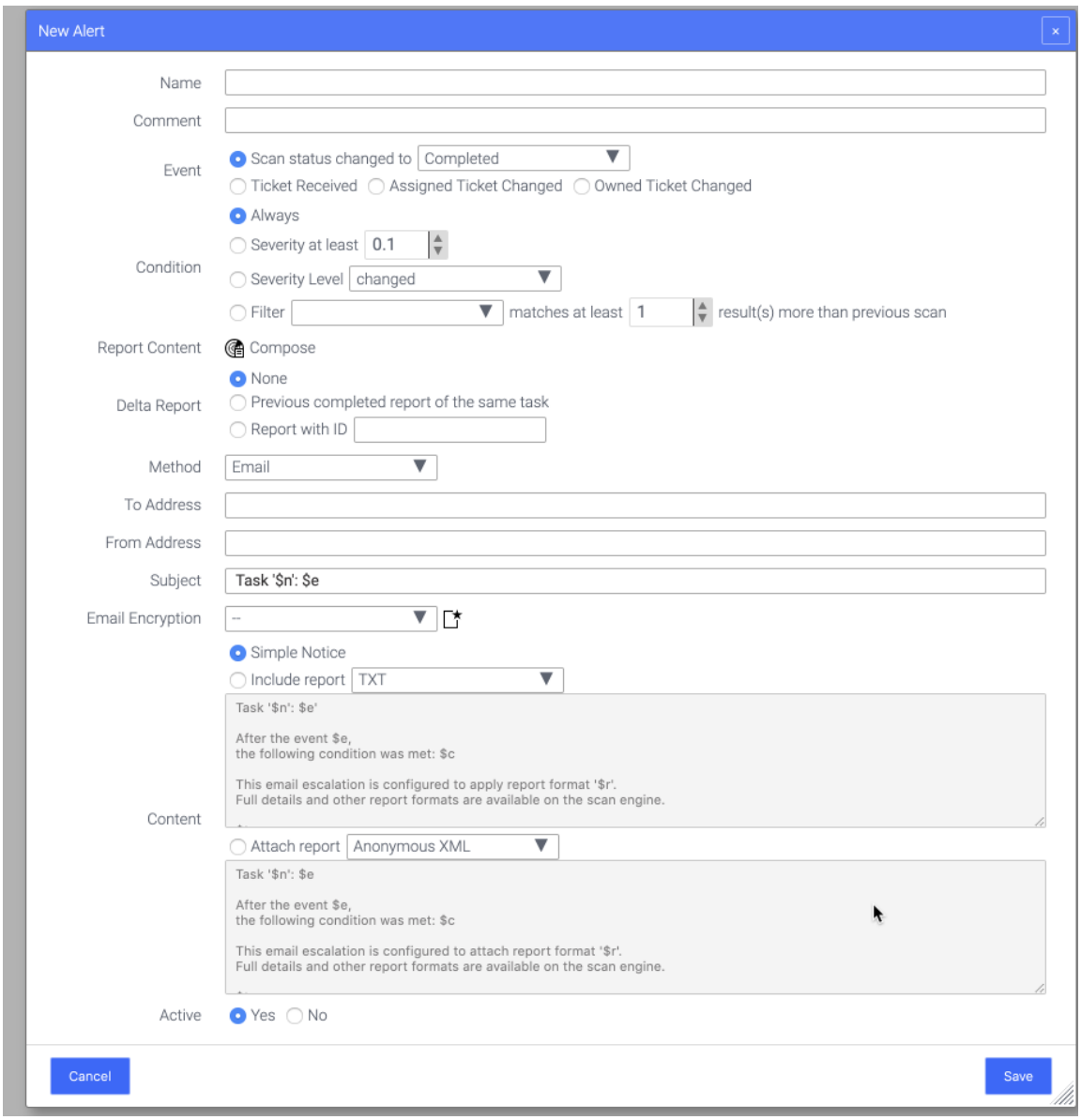


The Alert Creation page will show up and you can click on the icon



New Alert

The **New Alert** window appears. From there, you can create a target:



Understanding the Terms

To create an alert, you'll need to understand these simple terms.

Terms:

1. **Name:** Name of the alert.
2. **Comment:** If you want to insert a comment.
3. **Event:** The Platform provides several events to fire an alert.
4. **Condition:** Define the condition of the events.
5. **Report Content:** A report editor, to add the results that you want to see in the alert.
6. **Delta Report:** The difference between the reports, it can help you to find new, added or fixed vulnerabilities.
7. **Method:** The method that you want the alert to be delivered.
8. **Content:** Customize the content of the alert.
9. **Active:** Turn on or deactivate the alert.