Blumira

Detection Filters

FOCUS ON WHAT REALLY MATTERS

Detection Filters allows you to tune your own rules within the Blumira platform. Prevent triggering alerts based on your organization's known safe, normal or expected activity.

CUSTOMIZED RULES

Small teams can quickly and easily update their own rules directly in the platform:

- Create a filter to allowlist an IP address, user, device or other resource
- Edit a detection filter you've created
- Delete a detection filter you've created

THE BLUMIRA VALUE

What value do you get from Blumira's Detection Filters?

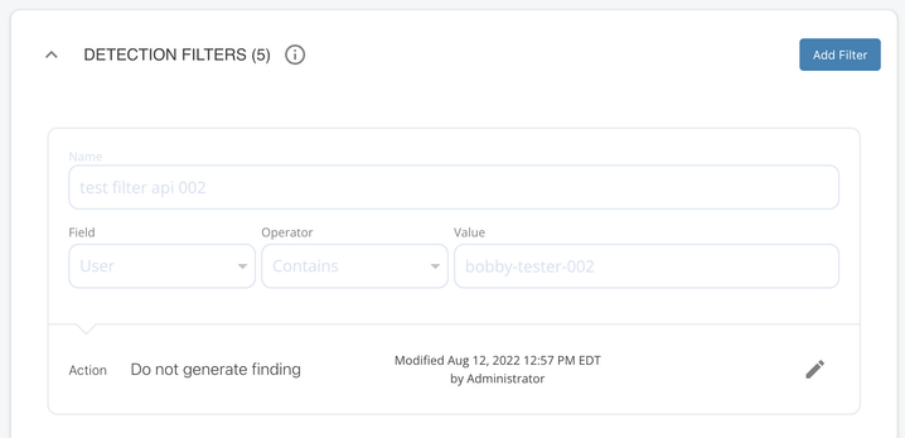
- Reduce the noise of unnecessary notifications
- Customize rules to fit your org's specific needs
- Focus your small team's time on resolving real threats

For example, if your leadership team is attending a conference outside of the country, you may want to exclude their usernames from triggering an alert every time they log in from a different location.

EASY TUNING

To add a new detection filter:

1. Navigate to **Reporting > Findings**.
2. Click a finding row, and then click **View Finding Details**.
3. Under Detection Filters, click **Add Filter**.
4. Fill out the **Name, Field, Operator** and **Value** fields.
5. Click **Save.**



This will exclude a chosen IP address, user, device, etc. from generating a finding. You can create additional filters with a separate set of conditions for a detection rule.

See our support articles to learn more!

Blumira

HOW DO WE DO THINGS DIFFERENTLY?

Meet compliance controls, save time on security tasks, focus on real threats and protect against a breach faster than ever with Blumira's all-in-one SIEM, detection and response.

AUTOMATE TASKS FOR YOU

We do all the heavy lifting for your team to save them time, including parsing, creating native third-party integrations, and testing and tuning detection rules to reduce noisy alerts.

FASTER TIME TO SECURITY

Our unique approach to detections notifies you of threats other security tools may miss, sending you real-time alerts in under a minute of initial detection to help you respond to threats faster than ever.

EASILY MEET COMPLIANCE

With a year of data retention and deployment that takes minutes to hours, we help you meet cyber insurance and compliance easily and quickly with the team you have today.

COMPARED TO THE INDUSTRY AVERAGE, BLUMIRA'S PLATFORM HELPS YOU DETECT AND RESPOND TO THREATS 99.4% FASTER, HELPING YOU SUCCESSFULLY AVOID A BREACH.*

Easy setup in hours!

Blumira does all the heavy lifting for you.

Blumira does the heavy lifting to pare down the overwhelming amount of data from logs into actionable events. That allows us to focus on revenue-enhancing activities.

Michael Cross, CIO
Greenleaf Hospitality

VOTED #1 SIEM ON G2

- BEST ROI
- EASIEST TO USE
- LIKELY TO RECOMMEND

Users Love Us

BLUMIRA FREE EDITION

Protect your Microsoft 365 environment in minutes! Sign up free (no credit card required) to get:

- Cloud SIEM with detection & response
- Automated detection rules applied
- Playbooks on how to respond to threats
- Security reports to see risk trends

SIGN UP FREE

**IBM/Ponemon 2021 Cost of a Data Breach; Blumira's 2022 State of Detection & Response*