

Leveraging Suricata Update



Matt Glass
CISSP, MCSE

<https://mattglass-it.com/>



Overview



Overview of suricata-update

Viewing and updating rule sources

Selecting appropriate rule sources

Custom rule sources

Enabling and disabling rules

Modifying rule behavior



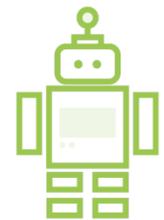
What is Suricata-update?



Rule management tool created by OISF for Suricata.



Used in the previous course to obtain Emerging Threats rules.



Used to configure rule sources and obtain rule sets.



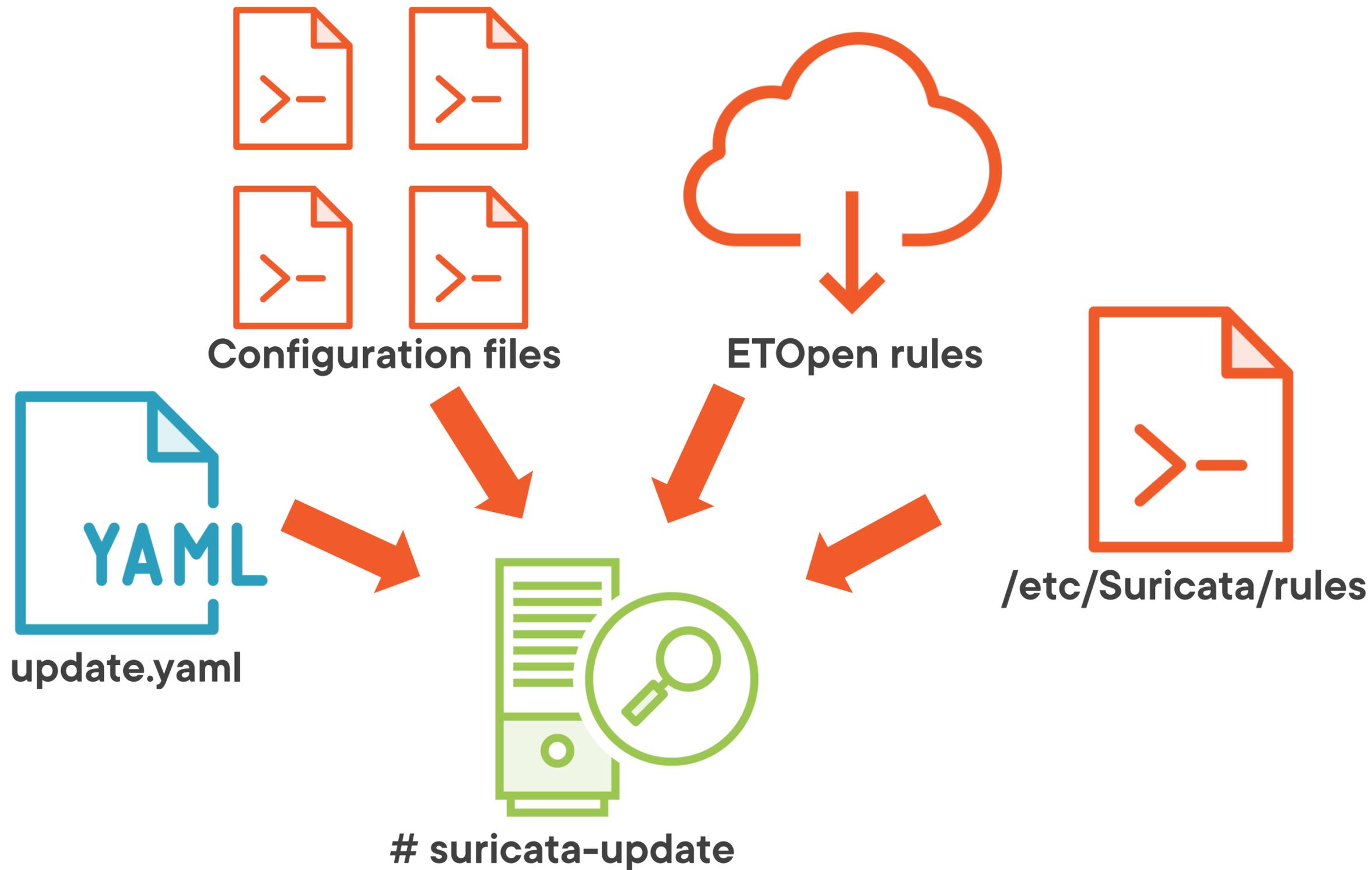
Automatically updates rules based on configuration.



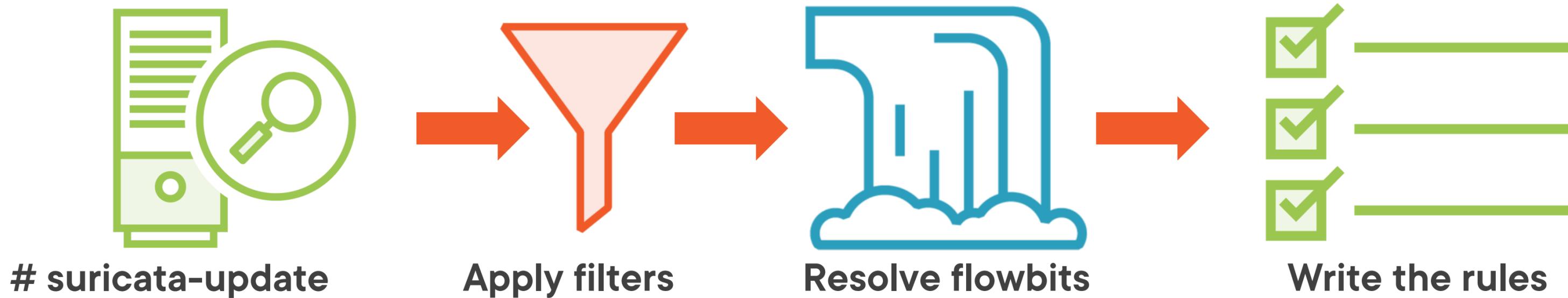
Managing Sources with Suricata-update



Suricata-update Process



Suricata-update Process



Managing Rules with Suricata-update



Adjust the rule sources within suricata-update



Manage rule sets configured on the server



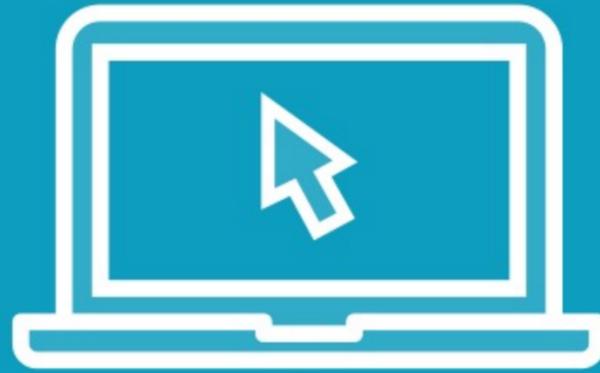
Enable and disable rules using different techniques in conf files



Modify rule behavior or change rules to drop traffic



Demo



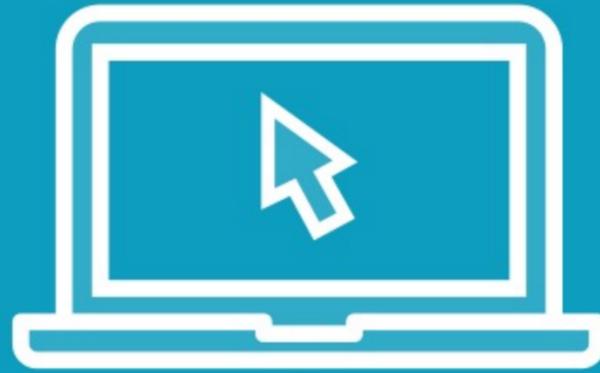
Implement appropriate rule sources

Globomantics Goals:

- Evaluate available rule sources
- Detect the use of popular hacking tools
- Detect internal attempts to access unauthorized external sites
- Select appropriate additional sources



Demo



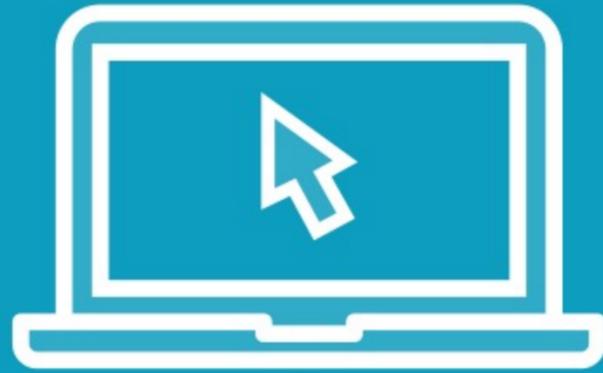
Enable and disable rules sources

Globomantics Goals:

- Obtain new rules sets
- Use `suricata-update` to obtain new rules from new sources
- Verify that new rules were downloaded after the change



Demo



Add a custom rule source

Use suricata-update to obtain rules from the custom source



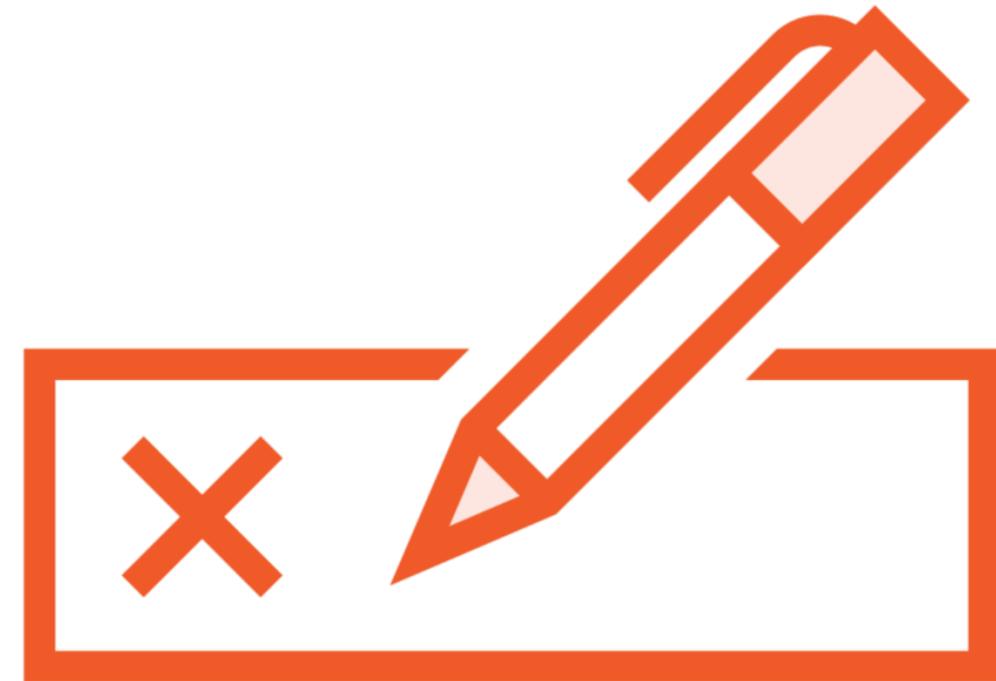
Managing Rules with Surciata-update



Enabling and Disabling Rules



Enable and disable rules by adjusting `enable.conf` and `disable.conf`



Manage rules by signature ID, regular expressions, or group name



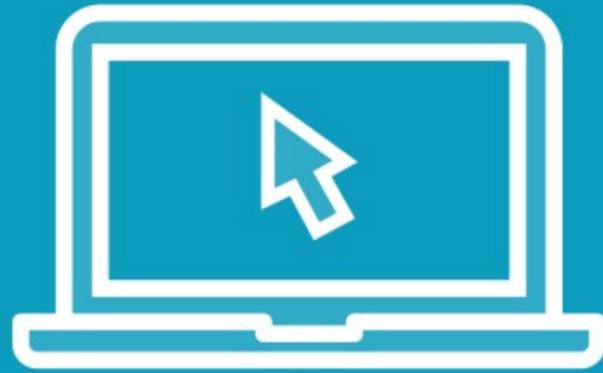
Modifying Rule Behavior

Use `modify.conf` to adjust rule configuration for pre-written rules

Use signature ID, regular expressions, and groups to drop matched traffic



Demo

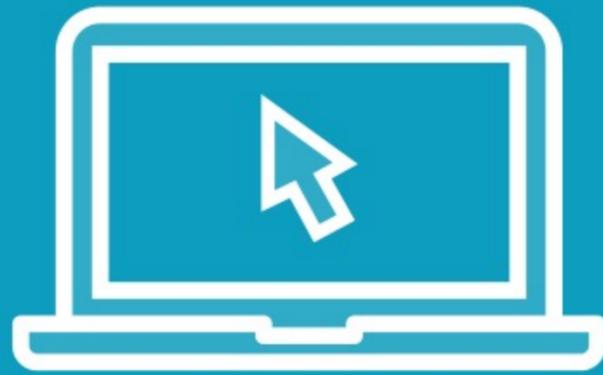


Enable and disable rules using 3 different techniques

- Signature ID
- Regular Expressions
- Group



Demo



Modify rule behavior within `modify.conf`

Use `drop.conf` to configure drop rules



Summary



Summary



Leveraged suricata-update to obtain rules from new sources

Selected appropriate sources

Managed rule sources in suricata-update

Added a custom rule source

Enabled and disabled rules

Adjusted rule behavior

