

Managing Suricata Rule Sets with Cron



Matt Glass
CISSP, MCSE

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



Overview



Cron overview

Automating tasks with Cron

Using Cron to sequence Suricata updates

Demo

Course Summary



Cron Overview



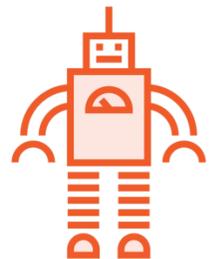
What Is Cron?



Task scheduler for Unix and Linux systems



Uses a cron table (crontab) to determine the schedule and commands



Enables the automation of routine tasks and commands



Schedule Suricata rules updates to occur regularly



Using Cron to Automate Tasks

```
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
[ output removed ]
#
# m h  dom mon dow   command

28 12 * * * /usr/local/bin/suricata-update >> /var/log/suricata/suricata-cron.log 2>&1
```



Sequencing Updates with Cron



**Schedule Suricata
rules updates**



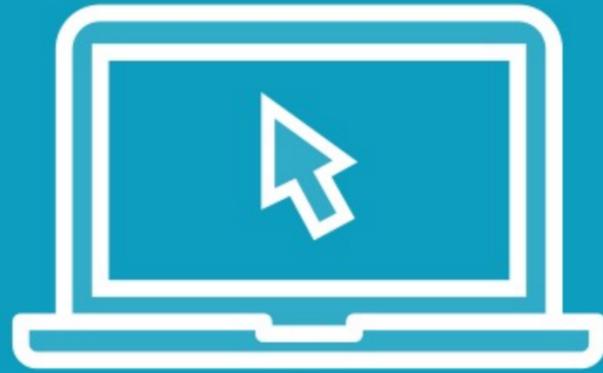
**Ensure rules are
updated frequently**



**Use reload commands
to minimize impact**



Demo



Use cron to schedule regular updates

Globomantics Goals:

- Automate the update process
- Schedule updates using an automated tool



Wrapping Up



Summary



Rule sets and sources in Suricata

Evaluated potential rule sets and sources

Leveraged suricata-update

Evaluated rule sets to detect specific threats

Tested threat detection using PCAP replay to evaluate rule sets

Automated updates using cron



Globomantics IDS/IPS Progress



Added new rule sources to our Suricata server



Obtained new rule sets from the sources



Tested new rule sets against traffic using PCAP replay



Used Cron to schedule regular rules updates



Next Steps

Continue experimenting with rule sources

Modify rules to target specific traffic in your environment

Learn to write your own custom rules and test in a lab

Continue the Enterprise Security Monitoring with Suricata path

