

# PROTEJA SUAS APLICAÇÕES DEBIAN COM O SIEM WAZUH

## CASOS PRÁTICOS E ATAQUES REAIS

**Moisés Santos Farias**

<https://github.com/moisesmsf>

[moisesmsf@proton.me](mailto:moisesmsf@proton.me)

<https://www.linkedin.com/in/moisesmsf>



# ABOUT ME

Piaçabuçu – AL

**Moisés Santos Farias**

<https://github.com/moisessmsf>

[moisessmsf@proton.me](mailto:moisessmsf@proton.me)

<https://moisessmsf.github.io>

Privacy + Anonymity + Cybersecurity

Monero + Anti-forensics

Moisés Santos Farias | <https://github.com/moisessmsf>



<https://moisesmsf.github.io/hdcb>



# WAZUH - DEFINITION (?)

OPEN SOURCE SECURITY PLATFORM (?)

XDR + SIEM FOR ENDPOINTS AND CLOUD WORKLOADS (?)

# WAZUH - COMPONENTS

WAZUH INDEXER (OPENSEARCH)

WAZUH SERVER (FILEBEAT)

WAZUH DASHBOARD (OPENSEARCH)

WAZUH AGENT

# WAZUH - DEPLOYMENT

PACKAGE

SOURCES

OVA - AMI

DOCKER - KUBERNETES

ANSIBLE - PUPPET

CLOUD

ALL-IN-ONE

CLUSTER

ARCHIVE

Moisés Santos Farias | <https://github.com/moisesmsf>



# WAZUH - CAPABILITIES

AGENTLESS MONITORING

MALWARE DETECTION

SYSTEM INVENTORY

ACTIVE RESPONSE

VULNERABILITY DETECTION

LOG DATA COLLECTION

COMMAND MONITORING

CONTAINER SECURITY

FIM

SCA

# WAZUH – CAPABILITIES – CLOUD

AWS MONITORING

AZURE MONITORING

OFFICE 365 MONITORING

GOOGLE CLOUD MONITORING

GITHUB MONITORING

Moisés Santos Farias | <https://github.com/moisesmsf>





# WAZUH – COMMUNITY

GITHUB

DISCORD

REDDIT

MAILING LIST

SLACK

TELEGRAM:  
WAZUH\_BR

Moisés Santos Farias | <https://github.com/moisesmsf>



# WAZUH – INTEGRATIONS

VIRUS TOTAL  
OSQUERY  
YARA

MALTIVERSE  
SHUFFLE  
CUSTOM  
OTHERS

# WAZUH – NOTIFICATIONS

EMAIL

SLACK

DISCORD

TELEGRAM

CUSTOM

Moisés Santos Farias | <https://github.com/moisesmsf>



# WAZUH – PAIN POINTS 01

- NO SIGMA RULES SUPPORT
- NO LOCAL PERSISTENCE OF LOGS
- RELOADING RULES, DECODERS AND CONFIG REQUIRES A RESTART

# WAZUH – PAIN POINTS 02

- NO LOAD BALANCING BUILT-IN
- NO MULTI-MASTER CLUSTERING
- POOR CHANGE MANAGEMENT AND SELF AUDITING

# WAZUH – HANDS-ON

[HTTPS://WWW.ELASTIC.CO/SECURITY-LABS/OUTLAW-LINUX-MALWARE](https://www.elastic.co/security-labs/outlaw-linux-malware)

[HTTPS://NSFOCUSGLOBAL.COM/ALERT-XORBOT-COMES-BACK-WITH-ENHANCED-TACTICS/](https://nsfocusglobal.com/alert-xorbot-comes-back-with-enhanced-tactics/)

# THANKS!

**Moisés Santos Farias**

<https://github.com/moisesmsf>

[moisesmsf@proton.me](mailto:moisesmsf@proton.me)

<https://www.linkedin.com/in/moisesmsf>

