

Top 25 Open Source cyber security tools

1. Zeek: <https://zeek.org/>
Network Security Monitoring
2. ClamAV: <https://www.clamav.net/>
Antivirus
3. OpenVAS: <https://www.openvas.org/>
Vulnerability Scanner
4. TheHive: <https://lnkd.in/e7aVCRUZ>
Incident Response
5. PFSense: <https://www.pfsense.org/>
Security appliance (firewall/VPN/router)
6. Elastic: <https://www.elastic.co/de/>
Analytics
7. Osquery: <https://www.osquery.io/>
Endpoint visibility
8. Arkime: <https://arkime.com/>
Packet capture and search
9. Wazuh: <https://wazuh.com/>
XDR and SIEM
10. Alien Vault Ossim: <https://lnkd.in/eShQt29h>
SIEM
11. Velociraptor: <https://lnkd.in/eYehEaNa>
Forensic and IR
12. MISP project: <https://lnkd.in/emaSrT57>
Information sharing and Threat Intelligence

13. Kali: <https://www.kali.org/>
Security OS
14. Parrot: <https://www.parrotsec.org/>
Security OS
15. OpenIAM: <https://www.openiam.com/>
IAM
16. Yara: <https://lnkd.in/eEJegEak>
Patterns
17. Wireguard: <https://www.wireguard.com/>
VPN
18. OSSEC: <https://www.ossec.net/>
HIDS
19. Suricata: <https://suricata.io/>
IDS/IPS
20. Shuffler: <https://shuffler.io/>
SOAR
21. Phish Report: <https://phish.report/>
Anti Phishing
22. Graylog: <https://lnkd.in/eAFuUmuw>
Logmanagement
23. Trivy: <https://lnkd.in/e7JxXStY>
DevOps/IaC Scanning
24. OpenEDR: <https://openedr.com/>
EDR
25. Metasploit: <https://lnkd.in/e4ECX-py>
Pentest
26. NMAP: <https://nmap.org/>
Old but gold