

# OPEN SOURCE TOOLS FOR BLUE TEAMS

## INTELLIGENCE

Actionable threat intelligence that is relevant, current & useful.

- ATT&CK [attack.mitre.org](https://attack.mitre.org)
- MISP [github.com/MISP/MISP](https://github.com/MISP/MISP)
- Sigma [github.com/SigmaHQ/sigma](https://github.com/SigmaHQ/sigma)

## ATTACK SURFACE

Know the network footprint, open services and vulnerabilities.

- Nmap [nmap.org](https://nmap.org)
- OpenVAS [openvas.org](https://openvas.org)
- DNS/IP Mapping & OSINT

## ENDPOINT VISIBILITY

Real time & historical monitoring for detection, DFIR and hunting.

- OSquery [osquery.org](https://osquery.org)
- OSSEC [ossec.net](https://ossec.net)
- Velociraptor [velocidex.com](https://velocidex.com)

## NETWORK VISIBILITY

Real time & full PCAP archiving for analysis and detection.

- Snort or Suricata [snort.org](https://snort.org)
- Zeek [zeek.org](https://zeek.org)
- Arkime [arkime.com](https://arkime.com)

## TRAINING & SIMULATION

Test detection, try attack tools.  
Play, Learn, Build.

- DetectionLab [github.com/clong/DetectionLab](https://github.com/clong/DetectionLab)
- Atomic Red Team [github.com/redcanaryco/atomic-red-team](https://github.com/redcanaryco/atomic-red-team)

## MALWARE

Malware Analysis is a deep rabbit hole; from detection to RE.

- ClamAV [clamav.net](https://clamav.net)
- Yara [virustotal.github.io/yara/](https://virustotal.github.io/yara/)
- Cuckoo [cuckoosandbox.org](https://cuckoosandbox.org)
- Ghidra [ghidra-sre.org](https://ghidra-sre.org)

## HONEYPOT

An easy to manage honeypot is the key to successful operational deployment.

- Opencanary [github.com/thinkst/opencanary](https://github.com/thinkst/opencanary)
- canarytokens.org
- [github.com/cowrie/cowrie](https://github.com/cowrie/cowrie)

## HACKER TARGET



See more at [hackertarget.com](https://hackertarget.com)  
Specialists in Attack Surface Mapping  
& Open Source Security Solutions