OPEN SOURCE TOOLS FOR BLUE TEAMS

INTELLIGENCE

Actionable threat intelligence that is relevant, current & useful.

- ATT&CK attack.mitre.org
- MISP github.com/MISP/MISP
- Sigma github.com/SigmaHQ/sigma

ATTACK SURFACE

Know the network footprint, open services and vulnerabilities.

- Nmap nmap.org
- OpenVAS openvas.org
- DNS/IP Mapping & OSINT

ENDPOINT VISIBILITY

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

- OSquery osquery.org
- OSSEC ossec.net
- Velociraptor velocidex.com

NETWORK VISIBILITY

Real time & full PCAP archiving for analysis and detection.

- Snort or Suricata snort.org
- Zeek zeek.org
- Arkime arkime.com

TRAINING & SIMULATION

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

- DetectionLab github.com/clong/DetectionLab
- Atomic Red Team github.com/redcanaryco/atomic-red-team

MALWARE

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

- ClamAV clamav.net
- Yara virustotal.github.io/yara/
- Cuckoo cuckoosandbox.org
- Ghidra ghidra-sre.org

HONEYPOT

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

- Opencanary github.com/thinkst/opencanary
- canarytokens.org
- github.com/cowrie/cowrie

HACKER TARGET

See more at hackertarget.com
Specialists in Attack Surface Mapping
& Open Source Security Solutions