# Sicherheit und Zuverlässigkeit – Security Onion

## Hauptfunktionen

Siehe github - <https://github.com/Security-Onion-Solutions/security-onion/wiki/IntroductionToSecurityOnion>

### Full packet capture

* durch netsniff-ng implementiert, ähnlich wie wireshark

<https://help.ubuntu.com/community/Netsniff-NG>

### NIDS und HIDS

<https://www.lan-monitor.de/network-intrusion-detection-mit-security-onion/>

### Analyse-Tools

* Sguil - <http://bammv.github.io/sguil/index.html>
  + Analysieren der durch das IDS gesammelten Informationen
  + Grafische Darstellung
* Squert (<http://www.squertproject.org/>)
* Enterprise Log Search and Archive (ELSA <https://code.google.com/p/enterprise-log-search-and-archive/>)
  + Durchsuchen des Syslog

## Sonstiges

Hacking mit Security Onion - <https://drive.google.com/open?id=1_FKhFCQOhYKXxDH1nZFn_3eGNLAS-Tbz>

Idee: Ossec-Netzwerk aufbauen - <https://ossec.github.io/docs/manual/installation/index.html>

SecOnion als Server, Windows-Maschine Client mit OSSEC-Agent

OSSEC = HIDS (Host Intrusion Detection System)