

OSSEC ist ein Open Source Host-basiertes Intrusion Detection System und 8-GRID bietet technische Dienstleistungen rund um OSSEC an.

8-GRID setzt auf ganzheitliche IT-Sicherheit, unser Branchenwissen und die langjährige Erfahrung. Unsere Partner, Kunden und Lieferanten profitieren von unserer Beratung, Know-How, technischen Dienstleistungen und dem umfangreichen Produktportfolio.

OSSEC ist eine Open Source Software, welche auf einem Host-basierten Intrusion Detection System, auch HIDS genannt, beruht. Dieses System hat mehrere Aufgaben und Features, um den User vor Trojanern oder Hijackern zu schützen.

Dazu zählen Logfile-Analyse und das Aufspüren von Rootkits genauso, wie das Durchführen von Integritätsprüfungen. Trifft etwas Ungewöhnliches ein, werden diverse Alarmierungen zur Warnung ausgegeben und der Hostmaster per Mail informiert. Der Administrator hat die Möglichkeit, OSSEC auf verschiedene Arten zu installieren bzw. in unterschiedlichen Modi laufen zu lassen.

Als Server nimmt OSSEC diverse Logging-Informationen der verschiedenen Clients entgegen und nutzt dabei eine verschlüsselte Verbindung. Der Agent hingegen überträgt diese Logging-Informationen an den Server, der die Daten zentral von allen angeschlossenen Agents entgegen nimmt und speichert. Zusätzlich kann OSSEC "local" installiert werden, um so das vorherrschende Client/Server-Modell zu umgehen. Diese Installationsmethode richtet sich allerdings an Einzelsysteme, die ohne Server fungieren.

Mit OSSEC HIDS werden folgende Server-Überwachungen ausgeführt:

- Rootkit Erkennung
- Log Analysen
- zeit-basierte Alarmmeldungen
- Integritätschecks
- Active Response

Mit OSSEC HIDS werden Attacken auf den Server und unsachgemäße Aktivitäten erkannt und der Hostmaster wird per Email darüber informiert.

Folgende Betriebssysteme werden von OSSEC unterstützt:

- OpenBSD 3.5-3.9, 4.0, 4.1 and 4.2
- GNU/Linux
 - Slackware 10.1,10.2,11 and 12
 - Ubuntu 5.04, 5.10, 6.06, 7.04 (32 and 64 bits)
 - RedHat (old) 8.0 and 9.0
 - Red Hat EL 4,5
 - Suse ES 9,10
 - Fedora Core 2,3,4 and 5
 - Debian 3.1 Sarge
- FreeBSD 5.2.1, 4.10-BETA, 5.4-RELEASE, 6.0-STABLE, 6.1-RELEASE
- NetBSD 3.0
- Solaris 2.8, 2.9 (Sparc) and 10 (x86)
- AIX 5.2 ML-07
- HP-UX 11i v2
- MacOSX 10
- Windows 2000, XP and 2003 (agent only)

8-GRID
IT Consulting & Services

Weitere Informationen unter:

8-GRID IT Consulting & Services GmbH
Billrothstrasse 12 Top 22
1190 Wien, Austria
Telefon: +43 (1) 890 14 70
eMail: office@8-grid.com
www.8-grid.com