Product Information

Key Features

- Built on a minimized and hardened Rocky Linux 8 platform
- Integration of Wazuh for automatic log analysis
- Log management and analysis in ELK
- Role-based user concept enforced by SELinux
- Cryptographic signatures on exported log files
- Smartcard login optional (supports OpenSC-compatible smartcards out-of-the-box)
- Integration with third party authentication (such as KrAPI) optional
- External security alarm function via relay
- Supports unidirectional connection for logging from multiple information security domains
- Supports reliable log transfer via the RELP-protocol
- Optional NIDS with Snort Open Source NIDS-engine
- Optional continuous network traffic recording in conjunction with NIDS option
- Integrity monitoring software for client computers
- Optional network backup/mirroring of logs to a Linux/Windows server

Description

ODIN Security Log is a product based on Open Source products and custom developed software. It consists of an installation bundle based on Rocky Linux 8 with integrated Wazuh (http://wazuh.com) HIDS system for intrusion detection and automatic log analysis. It also features a powerful log analysis tool, ELK which is short for Elasticsearch, Logstash, Kibana (http://www.elastic.co). ELK provides search and filter functions as well as a very customizable web based graphical user interface for viewing logs, statistics, traffic profiles, etc.

ODIN can also be purchased with an optional NIDS which is based on the Open Source (GPLv2) NIDS engine Snort. ODIN has custom GUI-based tools for easy management of Snort engine and rules. Note however that NO rules are included in the option since rules are licensed under a proprietary license.

Enguild Log Solutions AB
Ögonmåttsgatan 1, 421 72 Västra Frölunda, Sweden
URL: www.enguildlogsolutions.com, email: info@enguild.com
Reg. no: 559390-6604

Apart from the bundled functions, configurations for standard Rocky/RHEL functions such as syslogd, logrotate, auditd and SELinux is part of ODIN Security Log. It also comes bundled with some programs developed by Enguild AB for easy management and compliance with requirements found in most sensitive IT-systems. It integrates out-of-the-box with all syslog-compliant units. Log transfer from Windows-platforms use an Enguild proprietary agent which is easily integrated in any Windows version. For systems where unidirectional links to the log server are required in conjunction with high assurance requirements that logs are not lost in transmission, another product, ODIN Log Concentrator may be used to seamlessly integrate ODIN into almost any environment. ODIN also comes with separate client software for encryption of traffic over unidirectional links, client supervision software, a powerful log distribution software that performs Windows Event-logs to syslog conversion without loss of log entries as well as advanced integrity monitoring of files and Windows registry entries that alerts instantly when an entry is modified.

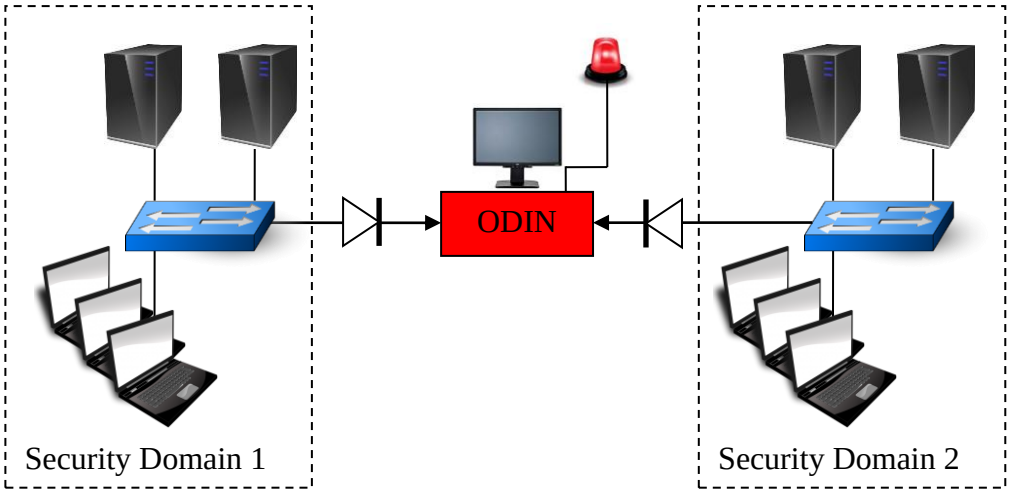
When the automatic analysis identifies potential threats using the rules configured in Wazuh, a security alarm is issued. This alarm is visible on the user Desktop but it is also possible to signal to an external alarm using a USB-relay if your ODIN Security Log is connected via a unidirectional link or using standard email or SNMP traps if your log server is connected via a bidirectional standard Ethernet connection. The alarm function has two levels for which separate relays can be used. For example, a critical system may want to connect the criticial alarm relay to a master system switch to automatically disable the system in case of a detected breach.

When using ODIN Security Log, Enguild Log Solutions AB can offer support with all configurations needed for specific log formats used by your system as well as education both in how to manage the log server and configure it yourself as well as basic log analysis techniques.

Optionally for use in Swedish military systems, it is possible to integrate KrAPI for authentication using TAK/TEID and cryptographic signatures on files. KrAPI is GFE and must be provided by the project using ODIN Security Log.

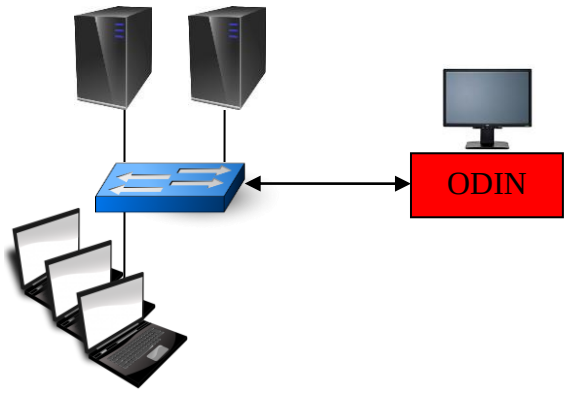
Typical Configurations

The pictures below show some typical ODIN Security Log Server setups depending on the specific needs for the customer and system it is integrated into. Note that these are just examples, ODIN can be deployed in several other ways also.



High assurance ODIN connection from two different security domains

The connection example above uses network diodes to enforce unidirectional connections to avoid data leakage between the two security domains. Typically used in multi-level security military systems. This configuration may use the ODIN log concentrator to fully utilize all security functions provided by Wazuh and ODIN software in conjunction with the network diodes.



This connection example is a typical office installment where alarm via email/SNMP is preferable and no high assurance security domain separation is needed.

ODIN in one security domain, alert via email or SNMP

Standard Packages

- Complete package including all software and hardware known to work with ODIN but custom specified to your needs.
- Package including software bundle and some of the specific hardware if you already have hardware dedicated for running a security log server.
- Software Bundle containing only the installation kit and all bundled software which can be installed on most standard hardware
- Streamlined installation kit with configuration parameters of your choice for fully automatic installation.

Options

- Optional Snort NIDS integration with custom tools for easy management. NOTE: Rules are NOT included since these require a proprietary license which must be obtained by the customer.
- Optional network traffic recording (only in conjunction with NIDS option)
- Optional integration with GFE-products such as KrAPI
- Help with configuration of your equipment to support unidirectional connections
- Configuration of your systems to integrate with the log server (syslog, Wazuh, Logstash, etc.)
- Adaption to custom log formats (many standard formats are supported out-of-the-box)
- Different educational packages

Licensing and Price

Wazuh, ELK and all packages from Rocky Linux in the bundle are licensed under GNU General Public License (version 2) as published by the FSF – Free Software Foundation, BSD with advertising or the Apache License Version 2.0. Please refer to the individual included products for information of which of these licenses that are applicable for the specific product. Software included and developed by Enguild AB or its subsidiaries are licensed under Enguild license which is closed source and NOT redistributable without written permission from Enguild AB. The base license is per system and not customer which means that a system using ODIN may be transferred to a third party without permission but it is NOT allowed to redistribute the ODIN instance separately without the system.

NOTE: The bundle contains the cryptographic packages from OpenSSL which may be subject to export control regulations.

The price of the bundle with the different options regarding support and education depends on the customer's specific needs. For more information, please contact:

Enguild Log Solutions AB
Phone: +46 708 233 933
Email: info@enguild.com
URL: http://www.odinsecuritylog.com