Prelude-SIEM Documentation

Release 4.0

Thomas Andrejak

Nov 15, 2017

Contents

CHAPTER 1

Prelude-SIEM Overview

Prelude is an agentless, universal, and hybrid security information and event management (SIEM) system. Prelude collects, normalizes, sorts, aggregates, correlates and reports all security-related events independently of the product brand or license. Security events are normalized to an IDMEF format, allowing native support with almost all security related event from an IT equipment.

While a malicious user (or software) may be able to evade the detection of a single IDS (NIDS, HIDS, etc.), it becomes exponentially more difficult to get around the defenses when there are multiple protection mechanisms. Prelude comes with a large set of sensors, each of them monitoring different kind of events. Prelude permits alert collection to WAN scale, whether its scope covers a city, a country, a continent or the world.

Prelude claims that it is a SIEM system capable of inter-operating with all the systems available on the market.[3] It is natively compatible with: AuditD, Nepenthes, NuFW, OSSEC, Pam, Samhain, Sancp, Snort, and Suricata but anyone can write its own sensors or utilize some of the 3rd party sensors that are available, given Prelude's opened APIs and librairies.

CHAPTER 2

Prelude SIEM Wiki

CHAPTER 3

Prelude SIEM modules

3.1 Prewikka

3.1.1 Overview

Originally written by Markus Alkio and Miika Keskinen, re-written and maintained by Nicolas Delon with the help of Yoann Vandoorselaere and Audrey Girard, on behalf of PreludeIDS Technologies, it was rapidly adopted as the new Prelude frontend.

Prewikka is a professional looking application providing advanced features like contextual filtering, aggregation, etc.

3.1.2 Github

Project : https://github.com/Prelude-SIEM/prewikka

3.2 Prelude-Correlator

3.2.1 Overview

Prelude-Correlator allows conducting multistream correlations thanks to a powerful programming language for writing correlation rules. With any type of alert able to be correlated, event analysis becomes simpler, quicker and more incisive.

3.2.2 Github

Project : https://github.com/Prelude-SIEM/prelude-correlator

3.3 Prelude-LML

3.3.1 Overview

This is the Prelude-LML log analyzer, collecting events from log files and/or syslog UDP messages.

3.3.2 Github

Project : https://github.com/Prelude-SIEM/prelude-lml

3.4 Prelude-LML-Rules

3.4.1 Overview

Ruleset for pcre LML plugin.

3.4.2 Github

Project : https://github.com/Prelude-SIEM/prelude-lml-rules

3.5 Prelude-Manager

3.5.1 Overview

Prelude-Manager server is the Prelude events collector.

Prelude-Manager is a high availability server that accepts secured connections from distributed sensors or other managers and saves received events to a media specified by the user (database, logfile, mail, etc).

The server is a high availability server capable of handling large number of connections, and processing large amounts of events. It uses a per client scheduling queues in order to process events by severity fairly accross clients.

3.5.2 Github

Project : https://github.com/Prelude-SIEM/prelude-manager

3.6 LibPrelude

3.6.1 Overview

The Prelude Library is used to make sensor developers' life better by providing features used by every sensor:

- Manager(s) Connection management (with fallback in case all configured Managers are down, and automatic reconnection).
- Interface to communicate with the Prelude Manager.

- Asynchronous Message interface (allowing sensor to emit message without blocking, even if there is latency on the wire).
- Asynchronous timer interface.
- Generic configuration API, providing a generic abstraction for command-line, configuration file option, and wide option support.
- Wide option managment allowing sensor-exported options to be directly accessible from the Manager administrative console.
- Generic plugin API.

3.6.2 Github

Project : https://github.com/Prelude-SIEM/libprelude

3.7 LibPreludeDB

3.7.1 Overview

The PreludeDB Library provides an abstraction layer upon the type and the format of the database used to store IDMEF alerts. It allows developers to use the Prelude IDMEF database easily and efficiently without worrying about SQL, and to access the database independently of the type/format of the database.

3.7.2 Github

Project : https://github.com/Prelude-SIEM/libpreludedb

CHAPTER 4

How to contribute

4.1 IRC

If there's something you just can't find out elsewhere, you want to give feedback directly to the authors or you're just bored, visit #prelude on irc.freenode.net

4.2 Get Support

Prelude-user forums can be accessed at:

- https://www.prelude-siem.org/projects/prelude/boards

Old mailing lists can be accessed at:

- http://premalink.gmane.org/gmane.comp.security.ids.prelude.user

Commercial Support is available through the CS company:

- http//www.prelude-siem.com, contact.prelude@c-s.fr

4.3 Help development

4.3.1 Submitting patches

The Prelude source is constantly changing. If you want to submit a patch, please do so from the most recent GIT source tree, subscribe to the prelude-devel forum and post your patch with a description of functionality. You can also attach patches to bugs on

- https://www.prelude-siem.org

4.3.2 Bugs

If you find any bugs, please report them to:

- https://www.prelude-siem.org

Please make sure that what you're reporting is actually a BUG and not a problem on your side.

4.3.3 Suggestions

Post on prelude-devel board and give us your suggestions.

CHAPTER 5

Indices and tables

- genindex
- modindex
- search