MENTAT: the SIEM system for the CSIRT team

Jan Mach, Radomír Orkáč, Pavel Kácha, Andrea Kropáčová
E-mail: mach@cesnet.cz, orkac@cesnet.cz, ph@cesnet.cz, andrea@cesnet.cz
CESNET, a.l.e., Prague, Czech Republic

Abstract: Mentat is a distributed modular SIEM (Security Information Management System) designed to help monitoring NREN-size networks. Its architecture enables accepting, storing, analyzing and reacting on vast amounts of arbitrary security events from various sources - e.g. honeypots, network probes, log analyzers and external third party detection/clearinghouse/blacklist services (ShadowServer). Mentat is an open source project.

Keywords: CSIRT, security incident, network anomaly, SIEM, IDS

1 Introduction

Most network operators care about their network and perform some kind of network monitoring. In order to keep their network under control and more secure, they usually apply some combination of various passive and proactive methods (IDS, IPS, honeypots, probes). In addition they usually have a CSIRT/CERT or some other type of a security team to watch over the network and deal with any issues.

CESNET is in the same position. CESNET operates a large high-speed network, called CESNET2, with rich international connectivity and approximately 400th users. The CESNET2 network is carefully and systematically monitored by means of many tools, technologies and services. These generate a great deal of warnings – network anomalies, security events and incidents etc. Besides that, we receive the alerts about the problems in our network from third party services such as ShadowServer. On top of that, we have a CSIRT team the members of which use the OTRS ticket tracking system to handle any incidents. To look for relevant information in multiple places manually is rather time consuming. Thus, our biggest motivation to develop the Mentat system is to consolidate event sources, event persistent storage and event processing.

2 What is Mentat

The Mentat project is a platform enabling to unify gathering and subsequent processing and managing of various detected security events coming from a wide range of different detection systems. Prior to developing our own custom solution we tested the existing open source SIEM systems (e.g. Prelude IDS). However we ended up implementing our own solution to best fit our needs.

3 Architecture

Mentat is designed as a distributed modular system with the emphasis on security, extendability and scalability. The core of the system is implemented similarly to the Postfix MTA. It consists of many simple modules/daemons, each of which concentrates on performing a single task. This approach enables smooth parallelization and extendability. All modules use the same core service framework, which makes implementing new modules an easy task. Currently, the whole system including the web interface is implemented in Perl and uses document oriented MongoDB database as persistent data storage. The system uses the IDEA data model, which is based on JSON. It was specifically designed to describe and contain a wide range of different security events and with further extendability in mind.

4 Conclusion

Currently, a working prototype of the Mentat system is being successfully operated. It accepts events from several internal and external IDS, IPS and detection systems. The system is processing circa 1 million events a day. The reporting module distributes the security reports directly to the responsible administrators within the CESNET2 network. We are still developing the system further. Currently we focus on improving the reporting capabilities and on event correlations.

5 ACKNOWLEDGMENTS

This work has been supported by the CESNET association within its “Large Infrastructure“ (LM2010005) research programme.

6 REFERENCES

[1] Mach, J., Expert system Mentat, Technical Report 04/2013, Prague: CESNET, 2014