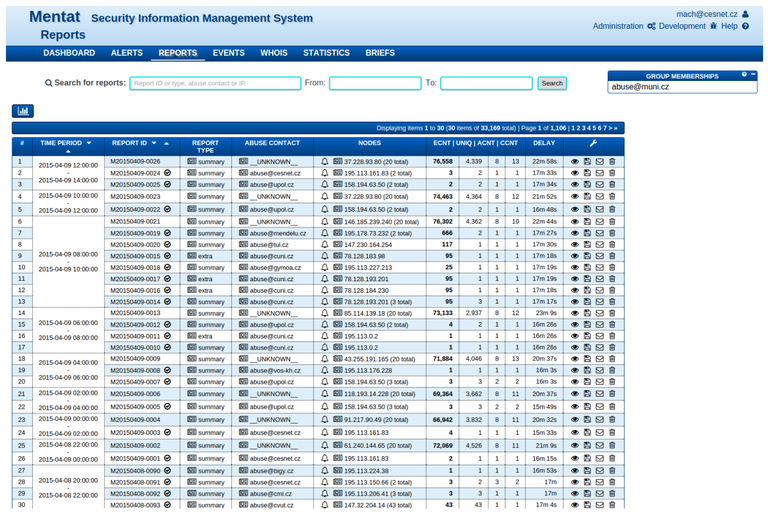
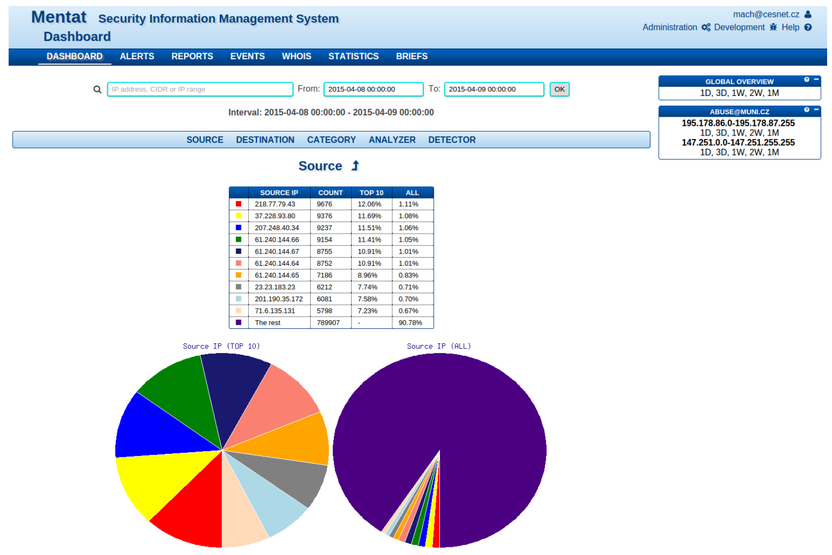
# Mentat

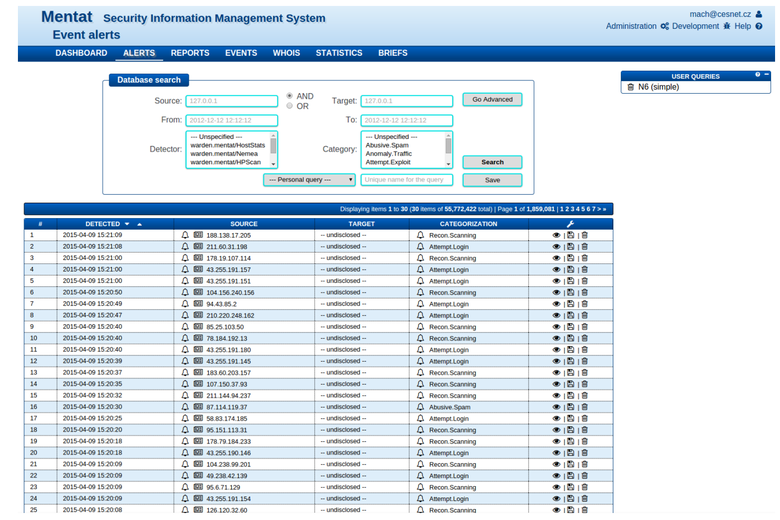
**http://csirt.cesnet.cz/cs/services/mentat**

Jan Mach <jan.mach@cesnet.cz>
Radomír Orkáč <radomir.orkac@cesnet.cz>
Pavel Kácha <pavel.kacha@cesnet.cz>
Andrea Kropáčová <andrea.kropacova@cesnet.cz>

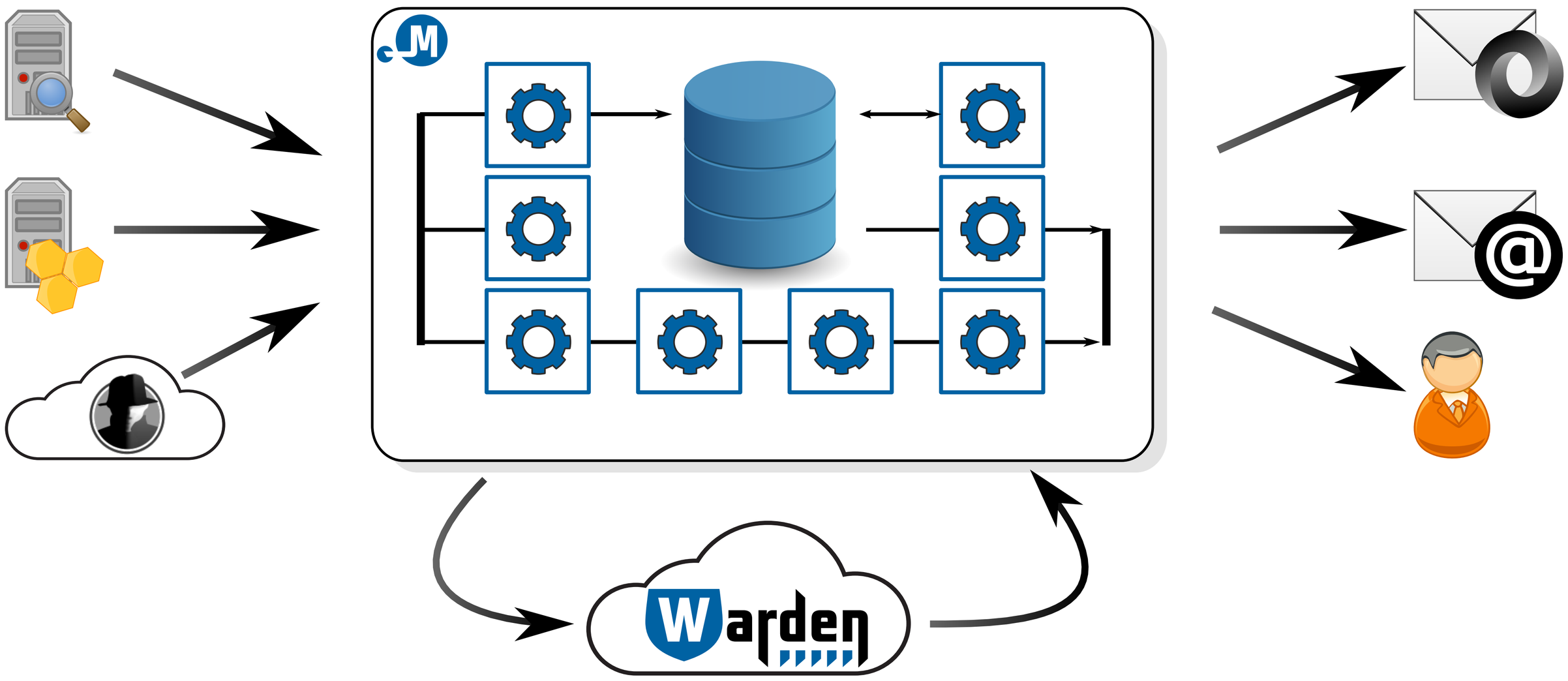
Mentat is a distributed modular SIEM (Security Information Management System) designed to help monitoring NREN-size networks. Its architecture enables accepting, storing, analyzing and reacting on vast amounts of arbitrary security events from various sources - e.g. honeypots, network probes, log analyzers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




## *System overview and architecture*




## *Key Features*

- Distributed architecture
- Real-time processing
- Offline (post) processing
- Structured IDEA data model
- Extentable modular design
- Persistent event repository
- Indexed and searchable storage
- Web user interface
- Data enrichment (RIPE)
- Automated event reporting

## *Applications*

- Consolidation of various feeds
- Platform for development and testing of new correlation and statistical methods
- CSIRT incident handling aid
- Network health overview and monitoring
- Trend observation

## *Future work*

- Event correlations
- Advanced statistical analysis
- Heuristical analysis
- (r)DNS, Passive DNS, GeoIP

...

(How big is **your** imagination?)

CESNET, a.l.e.
Zikova 4, 160 00 Prague 6, Czech Republic
National Research and Educational Network for Czech Republic
http://www.cesnet.cz

See also: CESNET-CERTS <https://csirt.cesnet.cz> | IDEA <https://csirt.cesnet.cz/IDEA> | Project Warden <https://wardenw.cesnet.cz>