Mentat System

Jan Mach

Webinar 2017-02-24

Before we begin

Language

- Event ≈ Alert ≈ Message
  a data entity flowing through the system
- Component ≈ Module ≈ Deamon
  a part of the Mentat system
- Source ≈ Connector ≈ Security tool
  a source of primary data emitting events

Agenda

Agenda

Motivation

Key ideas

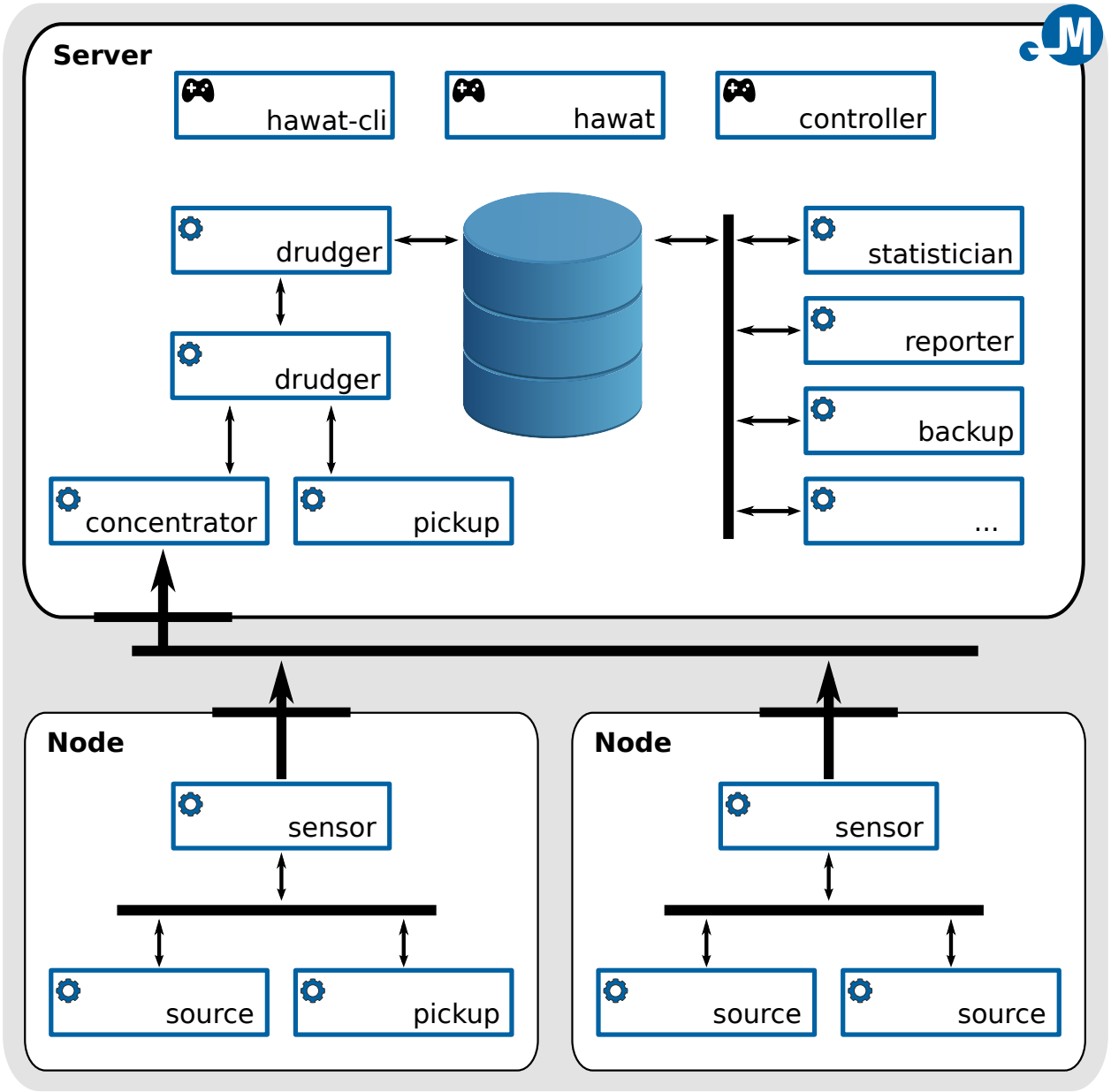
- Aid for CESNET-CERTS security team
- Resource consolidation

Main features

- Gathering/receiving information from various sources
- Long term searchable persistent information storage
- Real-time and back information processing with various methods
- Fully automatic processing, enable performing of automatic actions on specific conditions

Agenda

History: prototype design



History: prototype features

- Implementation language: Perl
- Data model: IDMEF (RFC 4765)
- Data storage: MongoDB
- Design inspired by Prelude SIEM and Postfix MTA
- Hierarchical structure of sensors sending data over network to one or more concentrators
- Hierarchical message source structure below sensors (on single host)
- Real-time message processing pipeline on server
- Message post processing modules on server
- Custom bidirectional protocol for message exchange (BSD sockets)
- Framework for module development

History: prototype drawbacks

- IDMEF
  - XML based format, bulk and chatty, deep structucture
  - Hard to serialize to DB
  - Bad design for automatic processing, possible infinite recursion
  - Obsolete datatypes and structures
  - Challenging extendability
- Perl
  - Really challenging to write robust applications
  - CPAN module hell
  - Obsolete web application development frameworks
- Warden
  - Popularity and simplicity of Warden deprecated many components including the communication protocol

History: lessons learned

Lesson learned

Focus on the server and data processing, there is already enough good client libraries.

Lesson learned

MISS = Make it simple, stupid!

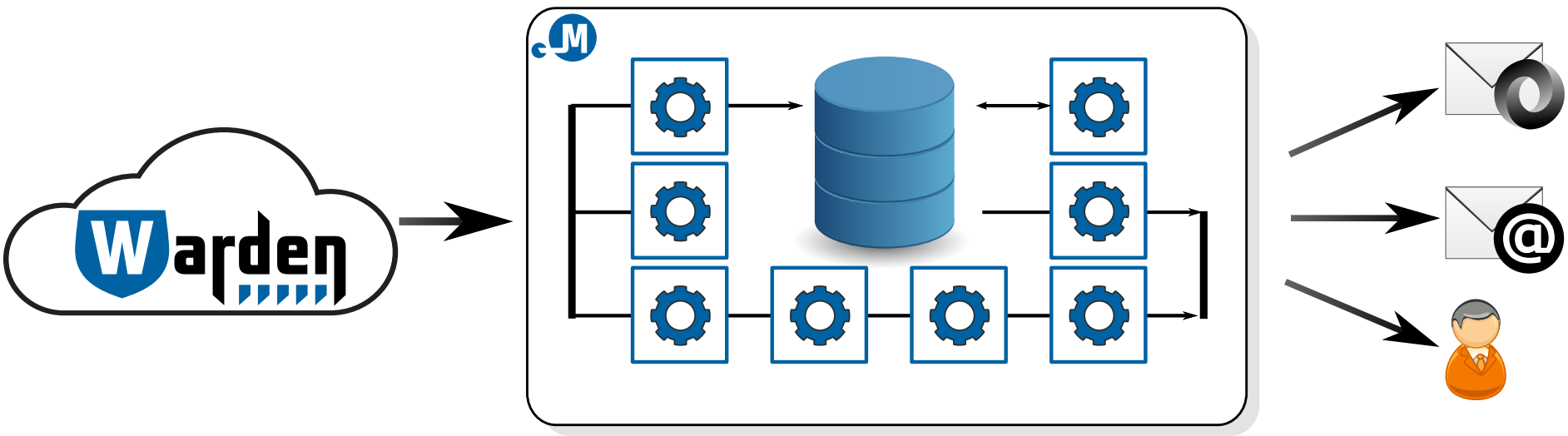
and then

KISS = Keep it simple, stupid!

Let‘s try it better, shall we...

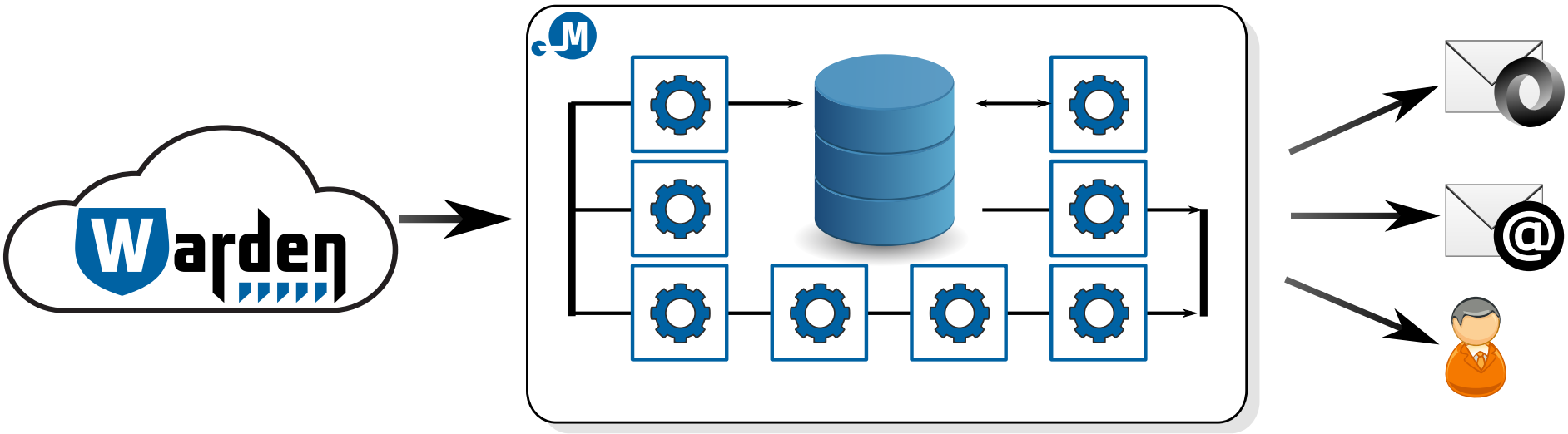
Agenda

System overview



- Implementation language: Python
- Data model: IDEA
- Data storage: MongoDB
- Removed all communication protocol related components and the protocol itself
- Warden used as a network communication protocol

System features



- Design inspired by Postfix MTA
  - Hierarchical structure of many small one task daemons
  - Filesystem directory message queues
  - Easy paralelization
- Better internal module design and framework for module development

Current status

- The project is still evolving
- In the process of migration to Python (40% done)
- Lack of documentation, but preparations made for Sphinx
- Git repository with Python code and software packages are not yet public

Agenda

Agenda

Warden

`https://warden.cesnet.cz/en/index`

- A system for efficient sharing information about detected events (threats)
- Simple client-server architecture
- Sending and receiving clients
- Based on HTTPS protocol with bidirectional certificate authentication
- Communication possible with any HTTPS capable library
- Python client library and simple filer daemon in distribution
- Community approach in data sharing

Data model: IDEA

`https://idea.cesnet.cz/en/index`

- Intrusion Detection Extensible Alert
- JSON based format (NoSQL friendly)
- Shallow structure, strong typed (SQL friendly)
- Easily extendable and customizable
- Possibility to mark anonymised, inaccurate, incomplete or forged data
- Support for aggregated, correlated events
- Support for various data attachments
- Dictionaries for description of various event attributes (Category, Source/Target type, etc.)

IDEA: Example message

- Example Botnet C&C report event


```
{
    "Format": "IDEA0",
    "ID": "cca3325c-a989-4f8c-998f-5b0e971f6ef0",
    "DetectTime": "2014-03-05T15:52:22Z",
    "Category": ["Intrusion.Botnet"],
    "Description": "Botnet Command and Control",
    "Source": [
        {
            "Type": ["Botnet", "CC"],
            "IP4": ["93.184.216.119"],
            "Proto": ["tcp", "ircu"],
            "Port": [6667]
        }
    ]
}
```

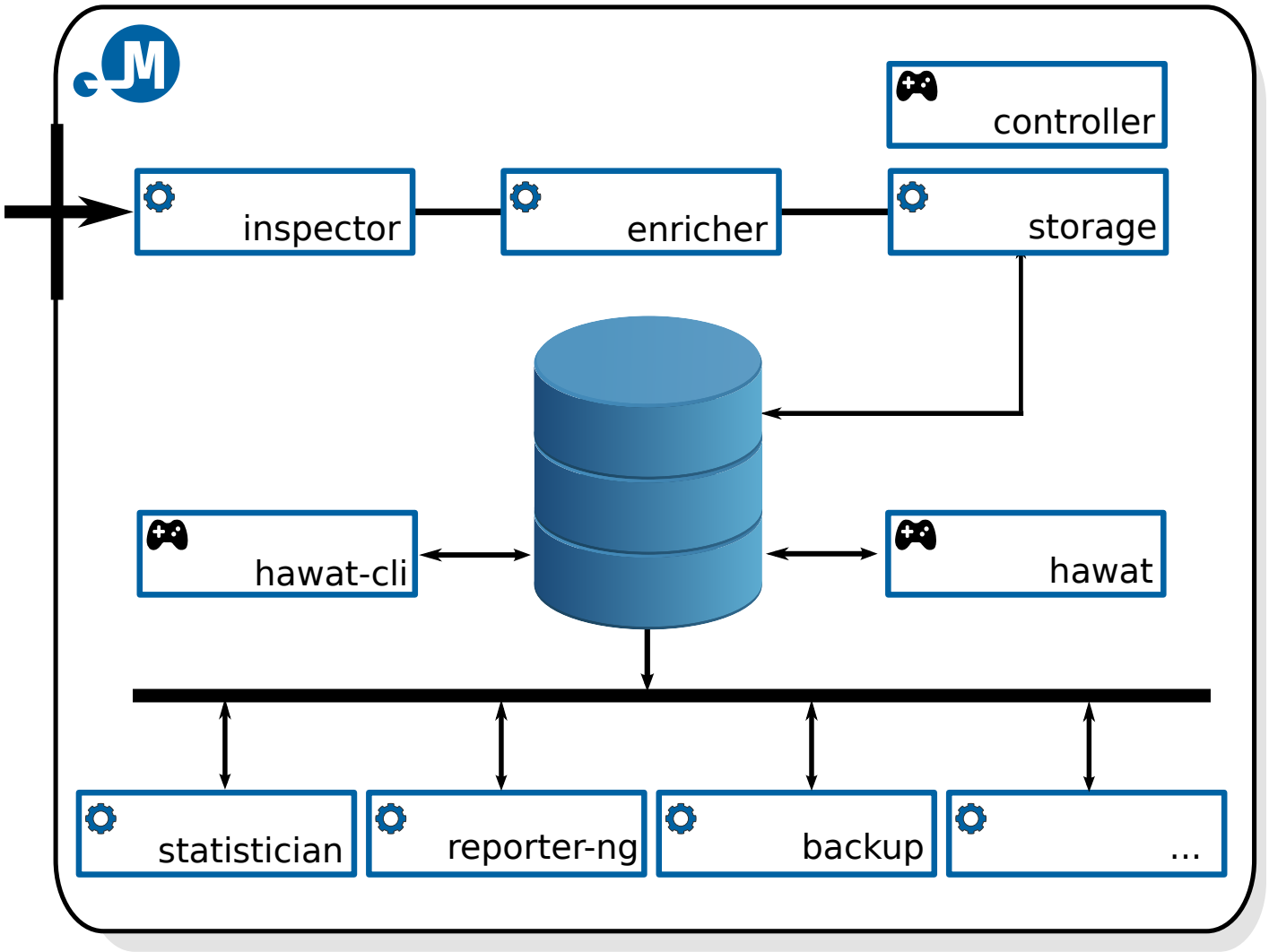
Database storage: MongoDB

`https://www.mongodb.com/`

- Single database instance
- Statistics
  - ~96,000,000 events in total
  - Receiving about 3,000,000 new events daily
  - Database size is ~100 GB
  - Average object size in DB is 1.7 KB
  - Record TTL is 6 months for interesting events, 4 weeks otherwise
  - Keeping infinite history of statistical summaries
  - Optimized indices for most common searches

Agenda

System architecture



System modules

- Real-time event processing modules
  - mentat-inspector
  - mentat-enricher
  - mentat-storage
- Event post processing modules (via database)
  - mentat-reporter-ng
  - mentat-statistician
  - (management scripts)
- Control modules and user interfaces
  - mentat-controller
  - hawat-cli
  - hawat

Module design

- Design inspired by Postfix MTA
  - Hierarchical structure of many small one task daemons
  - Filesystem directory message queues
- Process paralelization support, more instances can work with the same queue
- Framework for module development
  - Configuration loading, validation and merging (JSON)
  - Deamonisation
  - Log initialisation
  - Database abstract layer
  - IDEA message abstract layer
  - Filtering library
  - Statistical data processing library
  - WHOIS library, DNS resolving library
  - Report formatting and distribution library

Agenda

mentat-inspector

Description

- real-time event processing module
- perform various actions based on given rules

Available actions

- tag - tag event with given string
- set - set event attribute with given expression
- report - send report to email
- duplicate - copy event to queue
- dispatch - move event to another queue
- drop - filter out the event

mentat-enricher

Description

- real-time event processing module
- enrich events with additional data

Enriched data

- Problem source abuse resolving
- Hostname resolving (TBD)
- GeoIP resolving (TBD)

- Enriching events too much makes them bigger and duplicates information in database
- Project NERD: Network Entity Reputation Database

mentat-storage

Description

- real-time event processing module
- convert events into appropriate format and store them to database

mentat-reporter-ng

Description

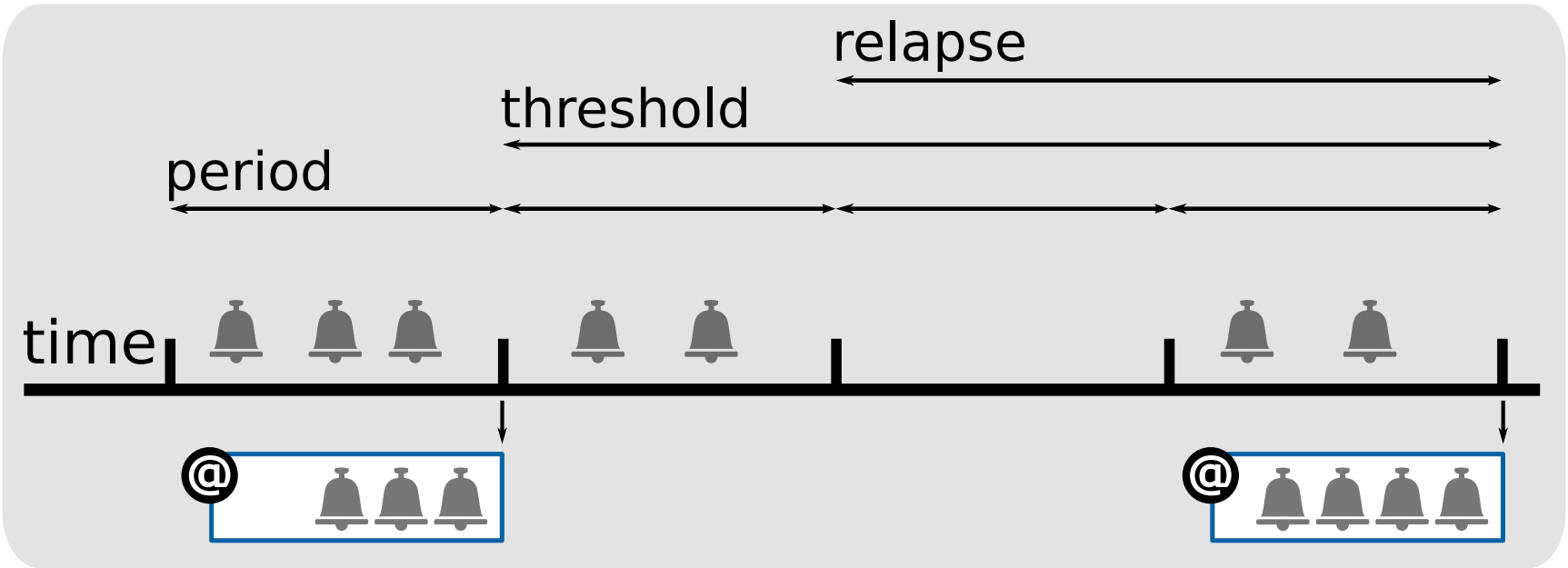
- event post-processing module
- generate periodical email reports and send them to appropriate abuse contacts

Key features

- Withhold reporting of already reported problems for certain time period
- Highly configurable reporting algorithm
- Processing based on event severity (feedback from network administrators)
- Compromise between high aggregation and reporting delay

Reporting algorithm

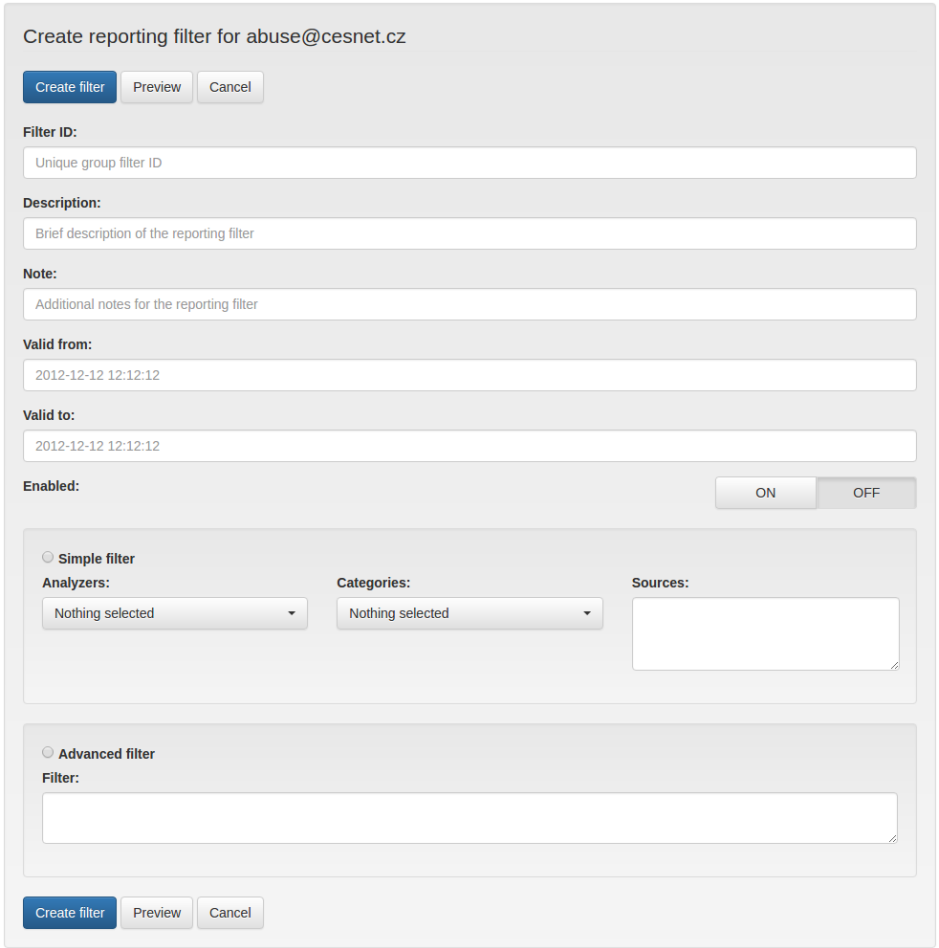
- Separate processing of events with different severities



- period - reporting interval for given severity
- threshold - report witholding interval
- relapse - ”problem solved” detection heuristics

Reporting configuration

- Global or per abuse group
- Pre-reporting filters
- Customizable pe-riod/threshold/relapse
- Email settings
  - Email redirection
  - Report type (summary, extra, both)
  - Attachment type (JSON, CSV, both)
  - Attachment compression



mentat-controller

Description

- configurable control script responsible for starting/stopping/restarting appropriate system modules

Key features

- Configuration file contains list of modules
- Administrator is able to start/stop/restart all/some of the modules

Hawat

- Security tool for CESNER-CERTS security team
- Authorization and data access is based on abuse groups
- Customized for backbone network operator security team

Hawat - Alerts

Search alerts

Go to clean search form

Alert database search

Source: 127.0.0.1

Target: 127.0.0.1

OR AND

From: 2017-02-14 01:00:00

To: 2012-12-12 12:12:12

Detector: Nothing selected

Category: Nothing selected

Search

Go Advanced

If you use certain queries often, you might consider saving them:

--- Personal query ---

Unique name for the query

Save

User queries

- N6 (simple)
- Test (simple)
- Test2 (simple)

Displaying items **1** to **30** (**30** items) | Page **1**

Next

#	Detected	Source	Target	Categorization	
1	2017-02-21 13:42:54	[redacted]1.194.57	[redacted]165.128/25	Attempt.Login	
2	2017-02-21 13:42:54	[redacted]1.194.57	[redacted]165.128/25	Attempt.Login	
3	2017-02-21 13:42:54	[redacted]1.194.57	[redacted]165.128/25	Attempt.Login	
4	2017-02-21 13:42:54	[redacted]1.194.57	[redacted]165.128/25	Attempt.Login	

Hawat - Group dashboard

Group dashboard for abuse@cesnet.cz

From: 2017-02-07 01:00:00 **To:** YYYY-MM-DD HH:MM:SS View

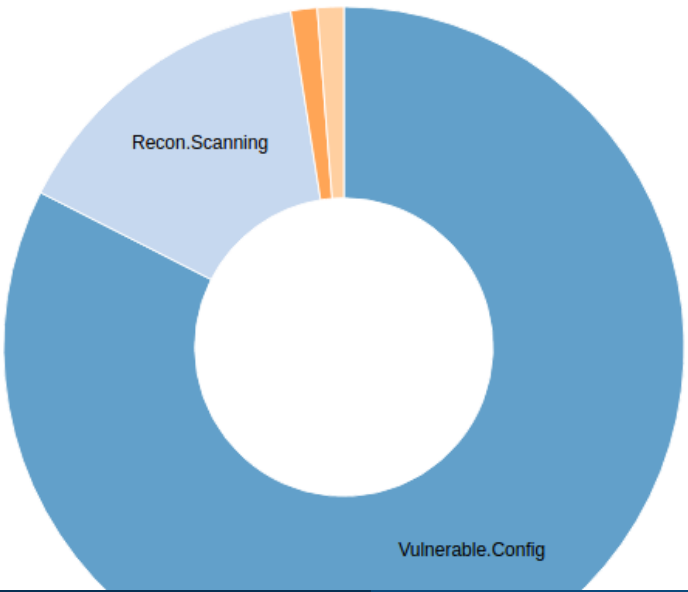
View the related reports (37)

Reporting statistics

Actual data period: 2017-02-07 09:00:00 - 2017-02-21 09:00:00 (14d)

per report | # per detector | **# per category set** | # per analyzer | # per category | # per IP

per category set



Search:

	Name	#	%
1	Vulnerable.Config	66	82.5
2	Recon.Scanning	12	15
3	Attempt.Exploit	1	1.25
4	Anomaly.Traffic	1	1.25
	Sum	**80**	**100**

Showing 1 to 4 of 4 entries

Min	1
Max	66
Sum	80
Cnt	4
Avg	20

Hawat - Report database

Reports

Report ID or type, abuse contact or IP | From: YYYY-MM-DD HH:MM:SS | To: YYYY-MM-DD HH:MM:SS | Search

Displaying items **1** to **30** (**30** items of **28,457** total) | Page **1** of **949**

1 2 3 4 5 6 7 › »

#	?	Time period	Report ID	Abuse contact	Node	ECNT | UNIQ | ACNT | CCNT	Delay
1	M	2017-02-21 09:00:00 -	M20170221SM-Egwd8	abuse@o2.cz	4.11 (3 total)	**14** 3 1 1	36m 48s
2	M	2017-02-21 11:00:00	M20170221SM-anDTH	abuse@cdt.cz	215.221 (2 total)	**12** 2 1 1	36m 47s
3	M		M20170221EM-LIDxm	abuse@vutbr.cz	9.201.173	**2** 1 1 1	25m 34s
4	M		M20170221SM-XIHpN	abuse@vutbr.cz	9.201.173	**2** 1 1 1	25m 34s
5	M		M20170221SM-OX4tG	abuse@o2.cz	148.163 (17 total)	**48** 17 1 1	25m 34s
6	M		M20170221SM-tlY1Z	abuse@cdt.cz	195.7 (4 total)	**7** 4 1 1	25m 33s
7	H	2017-02-21 09:40:00 -	M20170221SH-qH1i8	abuse@jcu.cz	7.6.91	**1** 1 1 1	25m 54s
8	H	2017-02-21 10:10:00	M20170221SH-0Poz5	abuse@sks.cz	3.78.212 (3 total)	**3** 3 1 1	25m 54s
9	H		M20170221SH-Yuqd5	abuse@cmi.cz	3.206.44 (4 total)	**4** 4 1 1	25m 54s
10	H		M20170221SH-BkssQ	abuse@upol.cz	4.22.14 (9 total)	**9** 9 1 1	25m 54s
11	M	2017-02-21 07:00:00 -	M20170221EM-lycuA	abuse@vse.cz	2.231.138	**2** 1 1 1	37m 15s
12	M	2017-02-21 09:00:00	M20170221SM-kQ92B	abuse@vse.cz	2.231.138	**2** 1 1 1	37m 15s
13	M		M20170221SM-KEpty	abuse@pilsedu.cz	3.181.196	**1** 1 1 1	37m 15s

Agenda

Plans for the future

Priorities

- finish migration to Python
- project documentation
- publish Git repository and software packages

- Better reporting capabilities
- Closer Warden server integration/cooperation
- Database performance evaluation/change

Plans for the future

Future goal

Warden and Mentat are developed with a goal to maximize the volume of automation in our data handling processess.

- Better data classification
- Better data prioritization
- Better data evaluation

Related projects

Following projects are related to Mentat and will somehow improve its capabilities. Either they will be integrated as optional modules and distributed separately, or Mentat will use them as a service:

- Project SABU
  - connect additional data sources
  - advanced data analysis and correlation
- Project NERD
  - additional event metadata related to IP address or hostname
  - IP address or hostname reputation

Agenda

Resources

- Project Mentat: official website
- Project Warden: official website
- IDEA: official website
- Project NERD: official website
- Project SABU: official website
- MongoDB: official website
- Sphinx: official website
- Prelude SIEM: official website
- RFC 4765: The Intrusion Detection Message Exchange Format (IDMEF)

What is Warden for us

Key concepts

- tool for automatic message exchange
- intentionally without more complex features

What is Mentat for us

Key concepts

- tool for automatic message processing
- framework for processing module development
- aid for members of CESNET-CERTS team
- aid for system administrators in our subnetworks

Example workflows

- Warden is out channel for distributing security incident data
- Organization has enough manpower
  - Use Warden directly, gather data and process them
- Mentat is our processing tool
  - to aid members of CESNET-CERTS team in incident handling
  - to aid system administrators in our subnetworks

Aid for CESNET-CERTS

- search for additional information
  - additional possible compromised hosts
  - when was the problem first reported
  - change the incident severity
- search history of particular IP
  - administrator failed to resolve issue multiple times, possible incident escalation to higher authorities

Aid for system admins

- use interactive reports instead of email version
- use dasboard to concentrate effort on biggest source of problems
- use web interface to adjust reporting filters

Thank you for your attention

Jan Mach
Jan.Mach@cesnet.cz