Agenda

1) IntelMQ in a nutshell
2) IntelMQ 3.0
3) Interoperability and related tools
4) Q&A

Whois

Sebastian Wagner

project management, software development, etc.

At CERT.at since 2015

Part of nic.at

13 people

GovCERT Austria

AUSTRIAN ENERGY CERT

In a nutshell

CERT.at

A **Toolbox**

based on **stream** processing

of **IoCs**

Goal: **Automate TI data processing as far as possible → focus time on complex cases**

Core Concepts

- **ETL** (Extract Transform Load)
- Freely **composable** tools (“bots”)
- Messaging **broker**
- **Stateless**
- **interoperability** with other tools
- Focus on **CERT**s’ and SOCs’ needs

A community project

- Collaboration
- Relying on contributions of all kinds
- Architecture Board being funded
  - structure for long term sustainability
- IntelMQ Enhancement Proposals (“IEPs”) for major changes

Thank you!

- Bernhard Herzog & Bernhard Reiter (Intevation funded by CERT-BUND and SUNET)
- Christopher Schappelwein (BMLV.at)
- Edvard Rejthar & Filip Pokorný (CSIRT.CZ)
- Einar Felipe Lanfranco (CERT-UNLP)
- Karl-Johan Karlsson (LIU.SE)
- Marcos Gonzalez (CSIRT-RD)
- Marius Karotkis (KAM.LT)
- Marius Urkis (NRDCS.LT)
- Mikk Margus Möll (CERT.EE)
- Raphaël Vinot (CIRCL)
- Thomas Bellus (SK-CERT)
- Thomas Hungenberg (CERT-BUND)
- Zach Stone (giantswarm.io)

...and many others

CERT.at's role

Main developer and Maintainer role

- Packaging & Release management
- Support

Work funded by CEF and MeliCERTes

Co-financed by the Connecting Europe Facility of the European Union

IntelMQ 3.0

Bots and feeds

- 26 collectors (protocols and APIs)
- 59 parsers
- 36 experts (enrichment, filtering, lookups etc)
- 19 outputs (to other systems, databases etc.)
- 88 *documented* Feeds

  + 73 Shadowserver feeds

https://intelmq.readthedocs.io/

Domain based data

- Domain suffix extraction
- HTTP status and content filtering
- Lookyloo lookup (website analysis and screenshots)
- RDAP lookup (whois on steroids with JSON)
- TI team contacts lookup
- *Tuency* Contact portal lookup
- uwhoisd lookup
- ...

https://intelmq.readthedocs.io/

Configuration changes

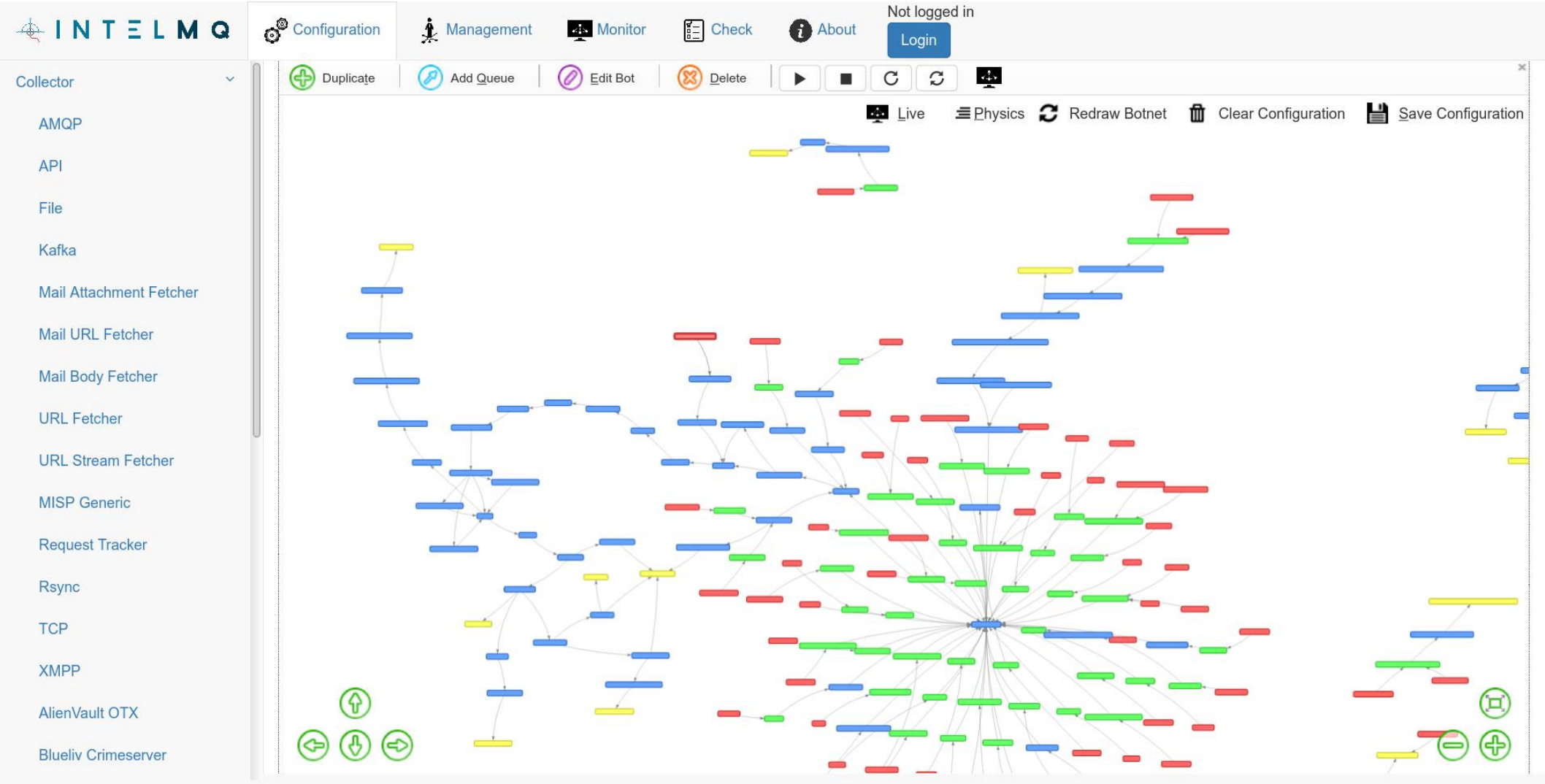
- 3 JSON files merged into one YAML file
  - Much easier syntax
  - Allows inline comments
- Proper default parameter handling in bots
- Official Docker images

API & Manager

- Python-based API
- Replaced PHP-backend of Manager
- Authentication
- Currently covers configuration files
- Call for contribution:

  Adapt Manager frontend (JavaScript)

https://intelmq.readthedocs.io/


INTELMQ
Configuration
Management
Monitor
Check
About
Not logged in
Login
Collector
AMQP
API
File
Kafka
Mail Attachment Fetcher
Mail URL Fetcher
Mail Body Fetcher
URL Fetcher
URL Stream Fetcher
MISP Generic
Request Tracker
Rsync
TCP
XMPP
AlienVault OTX
Blueliv Crimeserver
Duplicate
Add Queue
Edit Bot
Delete
Live
Physics
Redraw Botnet
Clear Configuration
Save Configuration

Docs and tutorial

- New docs home: intelmq.readthedocs.io/
- Tutorial: github.com/certtools/intelmq-tutorial/

tuency Contact Portal

- Auth based on Keycloak
- Self-administration
- Organisation hierarchy
- Netobjects (RIPE-Org, AS, Netblocks, Domains)
  - Claim+approval-process
  - Rules and contact data for automation → IntelMQ

gitlab.com/Intevation/tuency/tuency

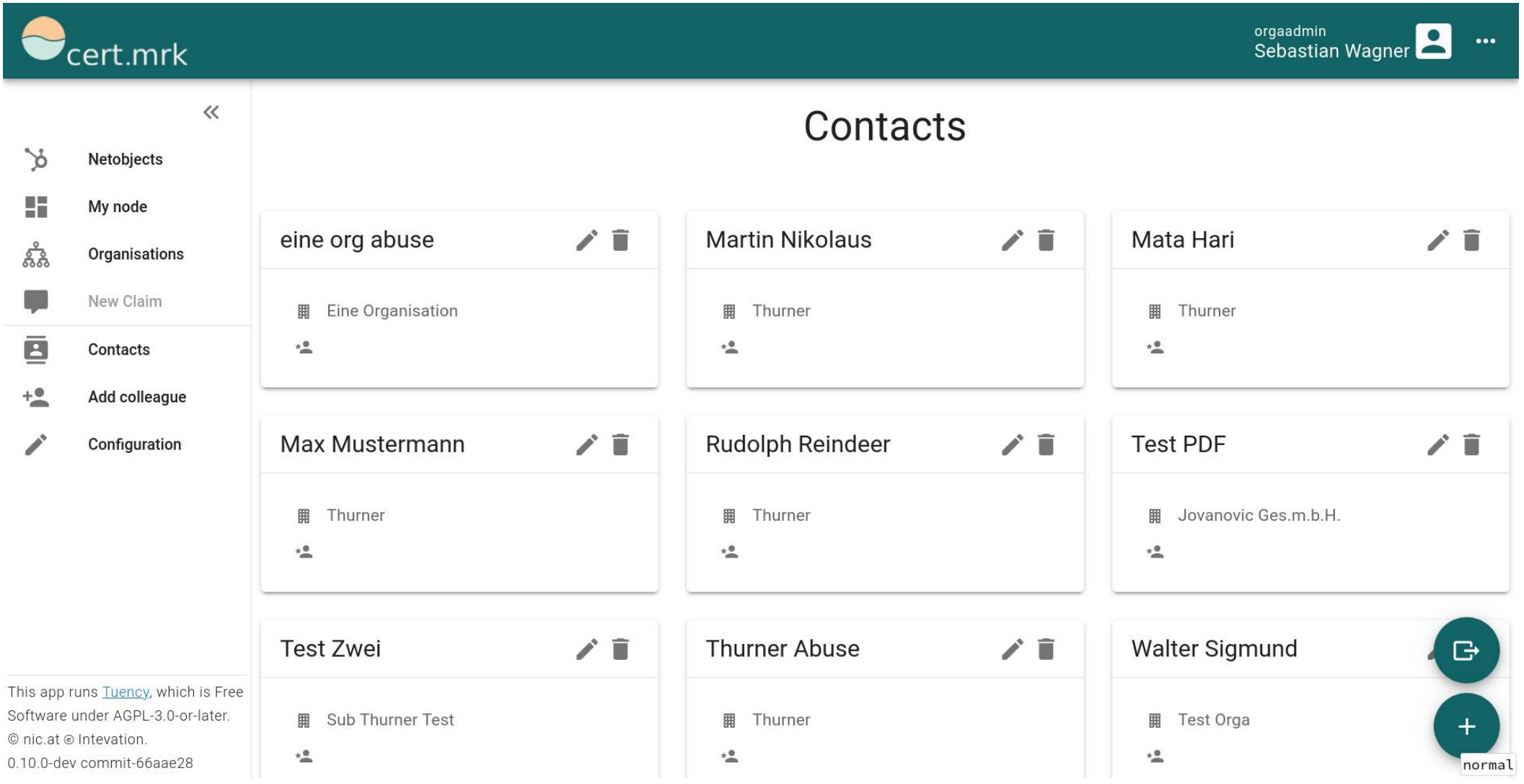
Netobjects
My node
Organisations
New Claim
Contacts
Add colleague
Configuration

Organisations

Name	Constituency	Parent Nodes	Actions
Thurner			
Nagl KEG		Thurner	
Jovanovic Ges.m.b.H.		Thurner	
Sub Thurner Test		Thurner	
Test Orga		Thurner --> Nagl KEG	
Eine Organisation		Thurner --> Nagl KEG --> Test Orga	

NEW ORGANISATION

normal

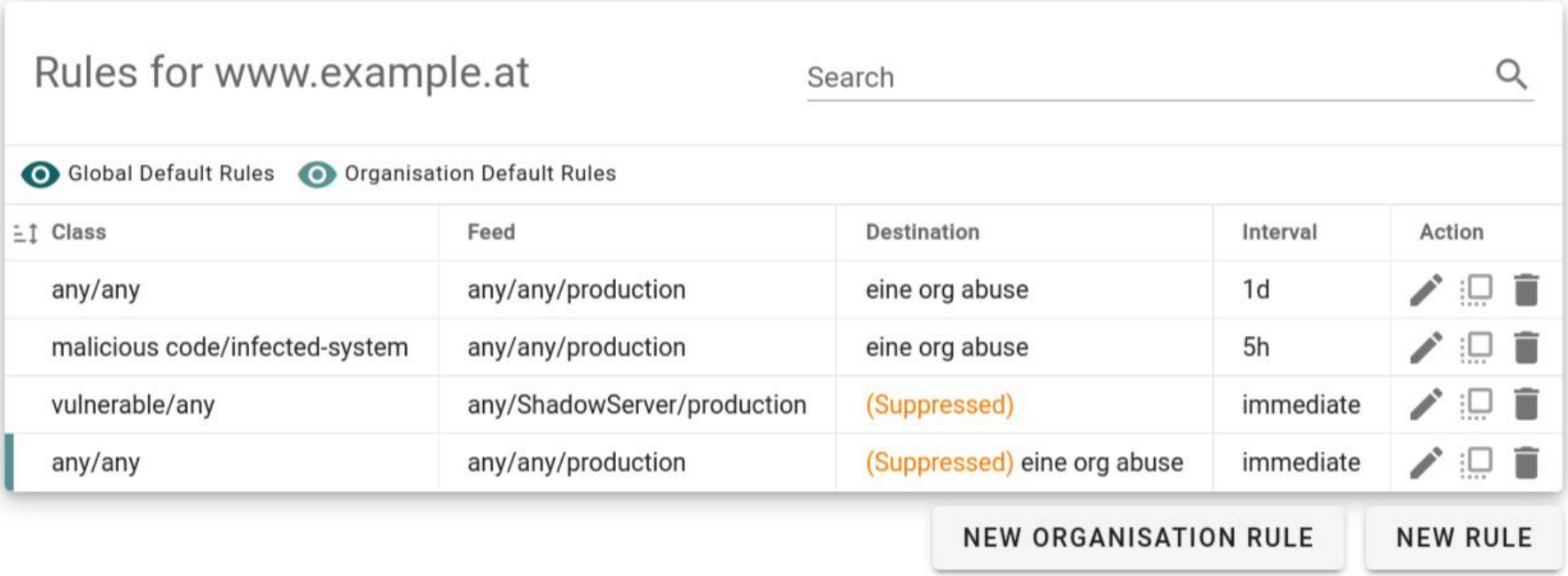

cert.mrk
orgaadmin
Sebastian Wagner
Netobjects
My node
Organisations
New Claim
Contacts
Add colleague
Configuration
Contacts
eine org abuse
Eine Organisation
Martin Nikolaus
Thurner
Mata Hari
Thurner
Max Mustermann
Thurner
Rudolph Reindeer
Thurner
Test PDF
Jovanovic Ges.m.b.H.
Test Zwei
Sub Thurner Test
Thurner Abuse
Thurner
Walter Sigmund
Test Orga
This app runs Tuency, which is Free Software under AGPL-3.0-or-later.
© nic.at ⊛ Intevation.
0.10.0-dev commit-66aae28
normal

Netobjects
My node
Organisations
New Claim
Contacts
Add colleague
Configuration

Manage Netobjects

fizeau.net		Eine Organisation	approved	
sebix.at		Thurner	approved	
www.sebix.at		Eine Organisation	approved	
16.0.0.0/4		Thurner	pending	
123.123.123.0/24		Thurner	approved	
123.123.123.123		Thurner	pending	
192.168.5.0/24		Thurner	pending	
1000:123:123:123:123::/80		Thurner	approved	
1000:123:123:123:123:1111::/96		Thurner	approved	
1000:123:123:123:123:1111:123:123		Thurner	approved	
2001:db8:123:4567:89ab:cdef::/96		Thurner	approved	
Default		Thurner		

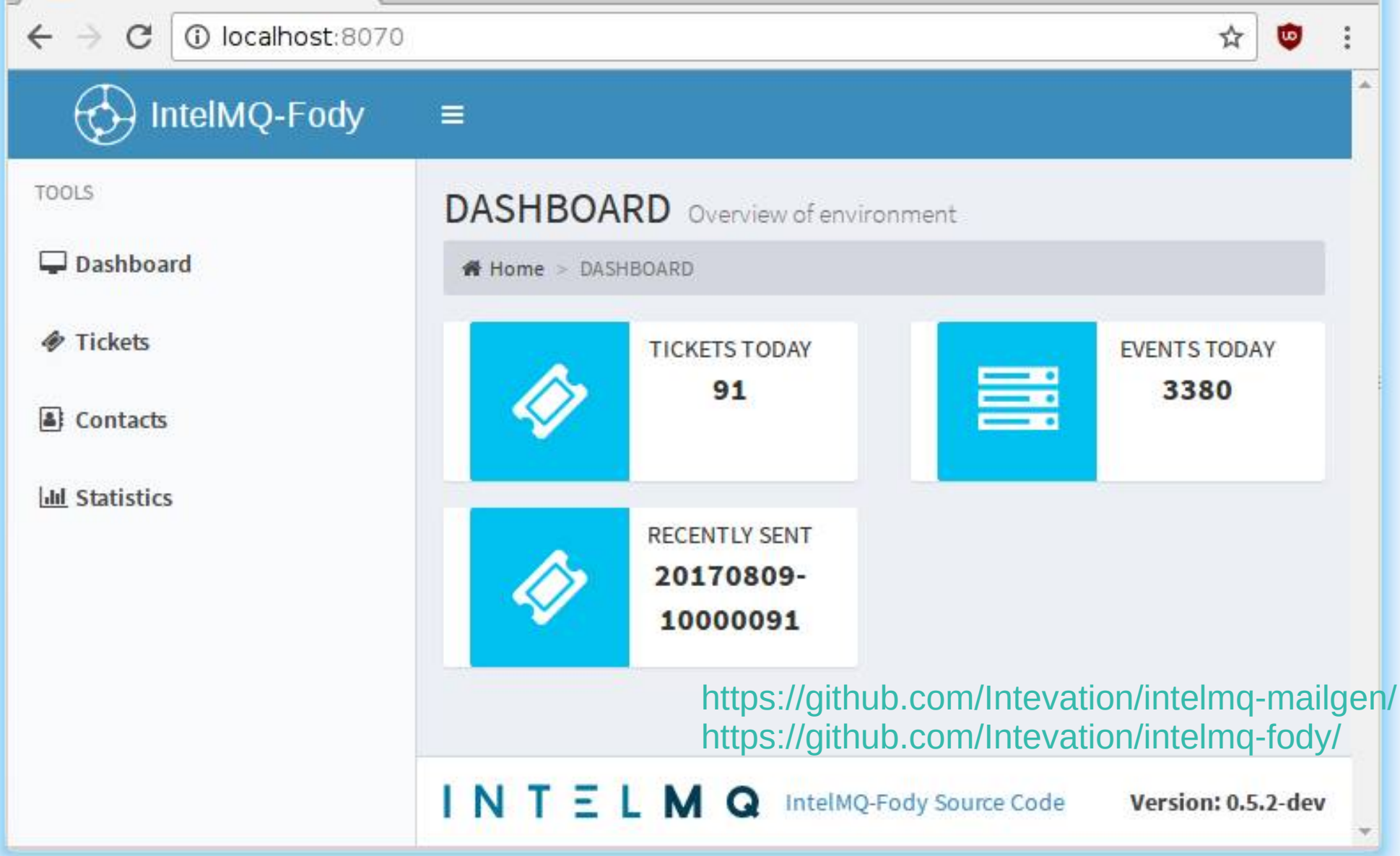
CLAIM RIPE HANDLE CLAIM NETOBJECT

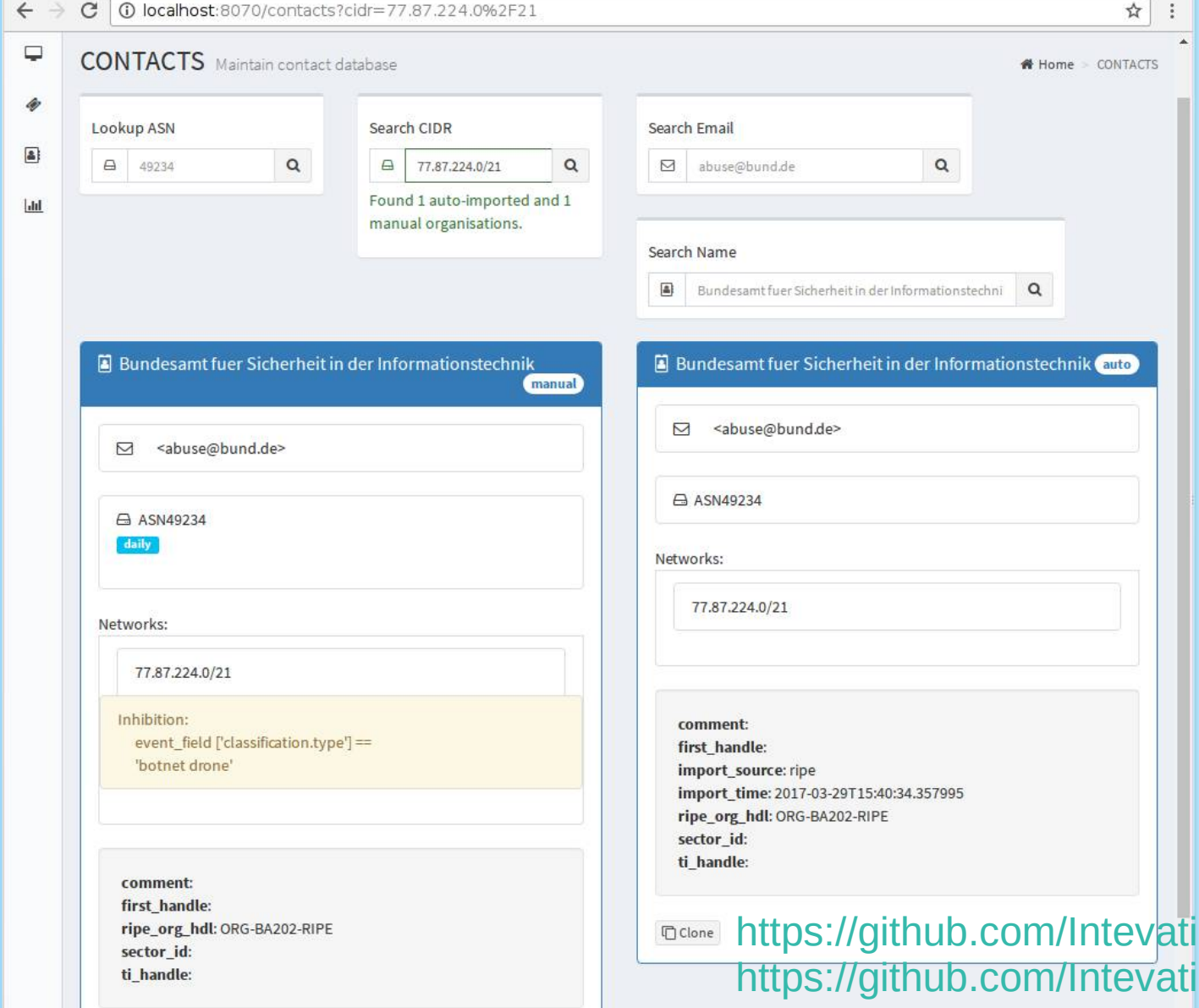

Rules for www.example.at
Search
Global Default Rules
Organisation Default Rules
Class
Feed
Destination
Interval
Action
any/any
any/any/production
eine org abuse
1d
malicious code/infected-system
any/any/production
eine org abuse
5h
vulnerable/any
any/ShadowServer/production
(Suppressed)
immediate
any/any
any/any/production
(Suppressed) eine org abuse
immediate
NEW ORGANISATION RULE
NEW RULE

Intelmq-mailgen / -fody

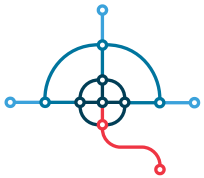
- Sending with SMTP
- Compatible with OTRS
- Rulesets and contacts from intelmq-fody
- Webinterface for tickets, contacts, rules, event database search & stats
- Developed by BSI/Intevation

https://github.com/Intevation/intelmq-mailgen/
https://github.com/Intevation/intelmq-fody/


localhost:8070
IntelMQ-Fody
TOOLS
Dashboard
Tickets
Contacts
Statistics
DASHBOARD
Overview of environment
Home > DASHBOARD
TICKETS TODAY
91
EVENTS TODAY
3380
RECENTLY SENT
20170809-
10000091
https://github.com/Intevation/intelmq-mailgen/
https://github.com/Intevation/intelmq-fody/
INTELMQ
IntelMQ-Fody Source Code
Version: 0.5.2-dev



https://github.com/Intevation/intelmq-mailgen/
https://github.com/Intevation/intelmq-fody/



intelmq-webinput-csv

CERT.at

timezone

+00:00

dry run

Constant fields (fallback):

classification type

malware configuration

Taxonomy: malicious code

feed.code

oneshot

classification.identifier

test

time.source	source.ip	destination.ip	
timestamp	ip	protocol	po
2018-12-09 02:53:18	85.126.145.244	tcp	548
2018-12-09 02:53:18	77.119.237.121	tcp	548
2018-12-09 02:53:18	77.119.229.227	tcp	548
2018-12-09 02:53:21	178.18.164.3	tcp	548
2018-12-09 02:53:21	78.132.127.172	tcp	548
2018-12-09 02:53:49	62.40.138.97	tcp	548
2018-12-09 02:53:49	212.197.156.245	tcp	548

https://github.com/certat/intelmq-webinput-csv/

MISP & IntelMQ

- MISP → IntelMQ (data feed and enrichment)
- IntelMQ → MISP
  - As MISP Feed
  - With MISP API
- Example: Generating RPZ data with IntelMQ

https://intelmq.readthedocs.io/

n6 & IntelMQ

- Interoperability via STOMP protocol
- Format conversions in both directions
- IntelMQ bots can be run inside n6 instances
- Webinput is n6-compatible

https://intelmq.readthedocs.io/

Contribute!

Sharing is caring

Thanks to

Bernhard Herzog & Bernhard Reiter (Intevation funded by CERT-BUND and SUNET), Christopher Schappelwein (BMLV.at), Edvard Rejthar & Filip Pokorný (CSIRT.CZ), Einar Felipe Lanfranco (CERT-UNLP), Karl-Johan Karlsson (LIU.SE), Marcos Gonzalez (CSIRT-RD), Marius Karotkis (KAM.LT), Marius Urkis (NRDCS.LT), Mikk Margus Möll (CERT.EE), Raphaël Vinot (CIRCL), Thomas Bellus (SK-CERT), Thomas Hungenberg (CERT-BUND), Zach Stone (giantswarm.io)

#threatintel on TI chat

github.com/certtools/intelmq/

https://intelmq.readthedocs.io/