MozDef Documentation

Release 0.0.1

Jeff Bryner, Anthony Verez

January 11, 2016

Contents

CHAPTER 1

Overview

1.1 Why?

The inspiration for MozDef comes from the large arsenal of tools available to attackers. Suites like metasploit, armitage, lair, dradis and others are readily available to help attackers coordinate, share intelligence and finely tune their attacks in real time. Defenders are usually limited to wikis, ticketing systems and manual tracking databases attached to the end of a Security Information Event Management (SIEM) system.

The Mozilla Defense Platform (MozDef) seeks to automate the security incident handling process and facilitate the real-time activities of incident handlers.

1.2 Goals

1.2.1 High level

- Provide a platform for use by defenders to rapidly discover and respond to security incidents.
- Automate interfaces to other systems like MIG, flowspec, load balancers, etc
- Provide metrics for security events and incidents
- Facilitate real-time collaboration amongst incident handlers
- Facilitate repeatable, predictable processes for incident handling
- Go beyond traditional SIEM systems in automating incident handling, information sharing, workflow, metrics and response automation

1.2.2 Technical

- Replace a Security Information and Event Management (SIEM)
- Scalable, should be able to handle thousands of events per second, provide fast searching, alerting, correlation and handle interactions between teams of incident handlers.

MozDef aims to provide traditional SIEM functionality including:

- Accepting events/logs from a variety of systems
- Storing events/logs
- Facilitating searches

- Facilitating alerting
- Facilitating log management (archiving,restoration)

It is non-traditional in that it:

- Accepts only JSON input
- Provides you open access to your data
- Integrates with a variety of log shippers including heka, logstash, beaver, nxlog and any shipper that can send JSON to either rabbit-mq or an HTTP endpoint.
- Provides easy python plugins to manipulate your data in transit
- Provides realtime access to teams of incident responders to allow each other to see their work simultaneously

1.3 Architecture

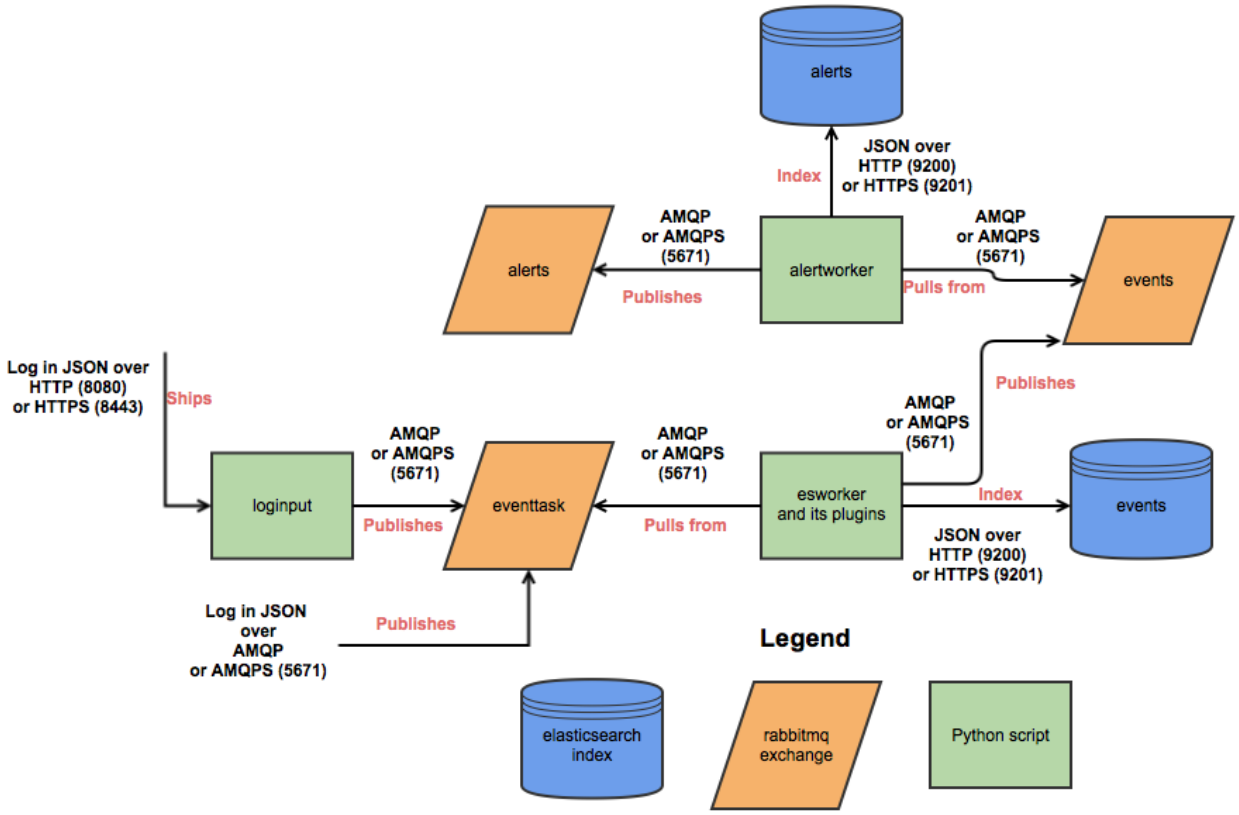
MozDef is based on open source technologies including:

- Nginx (http(s)-based log input)
- RabbitMQ (message queue and amqp(s)-based log input)
- uWSGI (supervisory control of python-based workers)
- bottle.py (simple python interface for web request handling)
- elasticsearch (scalable indexing and searching of JSON documents)
- Meteor (responsive framework for Node.js enabling real-time data sharing)
- MongoDB (scalable data store, tightly integrated to Meteor)
- VERIS from verizon (open source taxonomy of security incident categorizations)
- d3 (javascript library for data driven documents)
- dc.js (javascript wrapper for d3 providing common charts, graphs)
- three.js (javascript library for 3d visualizations)
- Firefox (a snappy little web browser)

1.3.1 Frontend processing

Frontend processing for MozDef consists of receiving an event/log (in json) over HTTP(S) or AMQP(S), doing data transformation including normalization, adding metadata, etc. and pushing the data to elasticsearch.

Internally MozDef uses RabbitMQ to queue events that are still to be processed. The diagram below shows the interactions between the python scripts (controlled by uWSGI), the RabbitMQ exchanges and elasticsearch indices.



1.4 Status

MozDef is in production at Mozilla where we are using it to process over 300 million events per day.

1.5 Roadmap

Initial Release:

- Facilitate replacing base SIEM functionality including log input, event management, search, alerts, basic correlations
- Enhance the incident workflow UI to enable realtime collaboration
- Enable basic plug-ins to the event input stream for meta data, additional parsing, categorization and basic machine learning
- Support as many common event/log shippers as possible with repeatable recipies
- 3D visualizations of threat actors

Mid term:

- Repeatable installation guides
- Ready-made AMIs/downloadable ISOs
- Correlation through machine learning, AI

- Base integration into Mozilla's defense mechanisms for automation
- Fine tuning of interactions between meteor, mongo, dc.js
- Support a variety of authentication/authorization schemes/technologies
- Plain text version of attackers
- Enhanced search for alerts, events, attackers within the MozDef UI

Long term:

- Integration into common defense mechanisms used outside Mozilla
- Enhanced visualizations and interactions including alternative interfaces (myo, omnidirectional treadmills, oculus rift)

CHAPTER 2

Introduction

2.1 Concept of operations

2.1.1 Event Management

From an event management point of view MozDef relies on Elastic Search for:

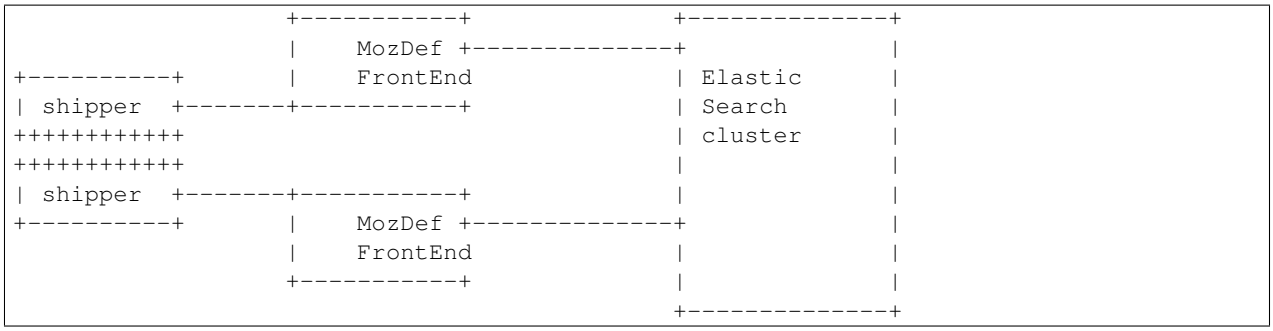
- event storage
- event archiving
- event indexing
- event searching

This means if you use MozDef for your log management you can use the features of Elastic Search to store millions of events, archive them to Amazon if needed, index the fields of your events, and search them using highly capable interfaces like Kibana.

MozDef differs from other log management solutions that use Elastic Search in that it does not allow your log shippers direct contact with Elastic Search itself. In order to provide advanced functionality like event correlation, aggregation and machine learning, MozDef inserts itself as a shim between your log shippers (rsyslog, syslog-ng, beaver, nxlog, heka, logstash) and Elastic Search. This means your log shippers interact with MozDef directly and MozDef handles translating their events as they make they're way to Elastic Search.

2.1.2 Event Pipeline

The logical flow of events is:



Choose a shipper (logstash, nxlog, beaver, heka, rsyslog, etc) that can send JSON over http(s). MozDef uses nginx to provide http(s) endpoints that accept JSON posted over http. Each front end contains a Rabbit-MQ message queue server that accepts the event and sends it for further processing.

You can have as many front ends, shippers and cluster members as you with in any geographic organization that makes sense for your topology. Each front end runs a series of python workers hosted by uwsgi that perform:

- event normalization (i.e. translating between shippers to a common taxonomy of event data types and fields)
- event enrichment
- simple regex-based alerting
- machine learning on the real-time event stream

2.1.3 Event Enrichment

To facilitate event correlation, MozDef allows you to write plugins to populate your event data with consistent meta-data customized for your environment. Through simple python plug-ins this allows you to accomplish a variety of event-related tasks like:

- further parse your events into more details
- geoIP tag your events
- correct fields not properly handled by log shippers
- tag all events involving key staff
- tag all events involving previous attackers or hits on a watchlist
- tap into your event stream for ancilary systems
- maintain 'last-seen' lists for assets, employees, attackers

2.1.4 Event Correlation/Alerting

Correlation/Alerting is currently handled as a series of queries run periodically against the Elastic Search engine. This allows MozDef to make full use of the lucene query engine to group events together into summary alerts and to correlate across any data source accessible to python.

2.1.5 Incident Handling

From an incident handling point of view MozDef offers the realtime responsiveness of Meteor in a web interface. This allows teams of incident responders the ability to see each others actions in realtime, no matter their physical location.

CHAPTER 3

Installation

The installation process has been tested on CentOS 6, RHEL 6 and Ubuntu 14.

3.1 Docker

You can quickly install MozDef with an automated build generation using docker.

3.1.1 Dockerfile

After installing docker, use this to build a new image:

```
cd docker && sudo make build
```

Running the container:

```
sudo make run
```

You're done! Now go to:

- http://localhost:3000 < meteor (main web interface)
- http://localhost:9090 < kibana
- http://localhost:9200 < elasticsearch
- http://localhost:9200/_plugin/marvel < marvel (monitoring for elasticsearch)
- http://localhost:8080 < loginput
- http://localhost:8081 < rest api

3.1.2 Get a terminal in the container

An common problem in Docker is that once you start a container, you cannot enter it as there is no ssh by default.

To solve this, a solution is to use *nsenter* present in the *util-linux* > 2.23 package. Debian and Ubuntu currently provide the 2.20 version so you need to download and compile the source code:

```
cd /tmp
curl https://www.kernel.org/pub/linux/utils/util-linux/v2.24/util-linux-2.24.tar.gz | tar -zxf-
cd util-linux-2.24
./configure --without-ncurses
```

```
make nsenter
cp nsenter /usr/local/bin
```

Now we can create a script for docker (/usr/local/sbin/dkenter):

```
#!/bin/bash

CNAME=$1
CPID=$(docker inspect --format '{{ .State.Pid }}' $CNAME)
nsenter --target $CPID --mount --uts --ipc --net --pid
```

While your MozDef container is running:

```
docker ps # find the container ID, fc4917f00ead in this example
dkenter fc4917f00ead
root@fc4917f00ead:/# ...
root@fc4917f00ead:/# exit
```

3.2 Docker config in AWS

3.2.1 Summary

If you don't want to install MozDef with docker on your own machine because for example it doesn't support docker or you fear you don't have enough memory, AWS supports docker.

1. Create a t2.small instance (enough to test MozDef) with the following details:
   - AMI: Ubuntu LTS-14-04 HVM
   - In "Configure Instance Details", expand the "Advanced Details" section. Under "User data", select "As text". Enter *#include https://get.docker.io* into the instance "User data". It will bootstrap docker in your instance boot.
2. In this instance, clone our github repo
3. Follow our docker config install instructions
4. Configure your security group to open the ports you need. Keep in mind that it's probably a bad idea to have a public facing elasticsearch.

3.2.2 Detailed Steps

Step by Step:

```
Sign into AWS
Choose EC2
Choose Images->AMIs
Find  Public Image ami-a7fdfee2 or a suitable Ubuntu 14.04 LTS(HVM) SSD 64bit server with HVM virtual
Choose Launch
Choose an instance type according to your budget. (at least a t2.small)
Choose next: configure instance details
Choose a network or create a VPC
Choose or create a new subnet
Choose to Assign a public IP
Under advanced details: user data choose 'as text' and enter #include https://get.docker.io
Choose next: add storage and add appropriate storage according to your budget
Choose next and add any tags you may want
```

```
Choose next and select any security group you may want to limit incoming traffic.
Choose launch and select an ssh key-pair or create a new one for ssh access to the instance.

For easy connect instructions, select your instance in the Ec2 dashboard->instances menu and choose c
ssh into your new instance according to the instructions ^^

clone the github repo to get the latest code:
from your home directory (/home/ubuntu if using the AMI instance from above)
    sudo apt-get update
    sudo apt-get install git
    git clone https://github.com/jeffbryner/MozDef.git

change the settings.js file to match your install:
vim /home/ubuntu/MozDef/docker/conf/settings.js
    <change rootURL,rootAPI, kibanaURL from localhost to the FQDN or ip address of your AMI instance

Inbound port notes:
You will need to allow the AWS/docker instance to talk to the FQDN or ip address you specify in setti
or the web ui will likely fail as it tries to contact internal services.
i.e. you may need to setup custom TCP rules in your AWS security group to allow the instance to talk
if you use the public IP on the ports specified in settings.js. (usually 3000 for meteor, 8081 for re

build docker:
    cd MozDef/docker
    sudo apt-get install make
    sudo make build (this will take awhile)
        [ make build-no-cache     (if needed use to disable docker caching routines or rebuild)
        [ at the end you should see a message like: Successfully built e8e075e66d8d ]

starting docker:
    <build dkenter which will allow you to enter the docker container and control services, change se
        sudo apt-get install gcc
        cd /tmp
        curl https://www.kernel.org/pub/linux/utils/util-linux/v2.24/util-linux-2.24.tar.gz | tar -zx
        cd util-linux-2.24
        ./configure --without-ncurses
        make nsenter
        sudo cp nsenter /usr/local/bin

        sudo vim /usr/local/bin/dkenter
            #!/bin/bash

            CNAME=$1
            CPID=$(docker inspect --format '{{ .State.Pid }}' $CNAME)
            nsenter --target $CPID --mount --uts --ipc --net --pid

        sudo chmod +x /usr/local/bin/dkenter

    cd && cd MozDef/docker/
    screen (running docker will not run in background session)
    sudo make run
    Browse to http://youripaddress:3000 for the MozDef UI

Build notes:
************
You can sign in using any Persona-enabled service (i.e. any yahoo or gmail account will work)
supervisor config that starts everything is in /etc/supervisor/conf.d/supervisor.conf
MozDef runs as root in /opt/MozDef
```

```
Logs are in /var/log/mozdef
MozDef will automatically start sending sample events to itself. To turn this off:
    0) get a new screen ( ctrl a c)
    1) sudo docker ps (to get the container id)
    2) sudo dkenter <containerid>
    3) supervisorctl
    4) stop realTimeEvents
```

3.3 Elasticsearch nodes

This section explains the manual installation process for Elasticsearch nodes (search and storage).

3.3.1 ElasticSearch

Installation instructions are available on Elasticsearch website. You should prefer packages over archives if one is available for your distribution.

3.3.2 Marvel plugin

Marvel is a monitoring plugin developed by Elasticsearch (the company).

WARNING: this plugin is NOT open source. At the time of writing, Marvel is free for development but you have to get a license for production.

To install Marvel, on each of your elasticsearch node, from the Elasticsearch home directory:

```
sudo bin/plugin -i elasticsearch/marvel/latest
sudo service elasticsearch restart
```

You should now be able to access to Marvel at http://any-server-in-cluster:9200/_plugin/marvel

3.4 Web and Workers nodes

This section explains the manual installation process for Web and Workers nodes.

3.4.1 Python

Create a mozdef user:

```
adduser mozdef
```

We need to install a python2.7 virtualenv.

On Yum-based systems:

```
sudo yum install make zlib-devel bzip2-devel openssl-devel ncurses-devel sqlite-devel readline-devel
```

On APT-based systems:

```
sudo apt-get install make zlib1g-dev libbz2-dev libssl-dev libncurses5-dev libsqlite3-dev libreadline
```

Then:

```
su - mozdef
wget http://python.org/ftp/python/2.7.6/Python-2.7.6.tgz
tar xvzf Python-2.7.6.tgz
cd Python-2.7.6
./configure --prefix=/home/mozdef/python2.7 --enable-shared
make
make install

wget https://raw.github.com/pypa/pip/master/contrib/get-pip.py
export LD_LIBRARY_PATH=/home/mozdef/python2.7/lib/
./python2.7/bin/python get-pip.py
./python2.7/bin/pip install virtualenv
mkdir ~/envs
cd ~/envs
~/python2.7/bin/virtualenv mozdef
source mozdef/bin/activate
pip install -r MozDef/requirements.txt
```

At this point when you launch python, It should tell you that you're using Python 2.7.6.

Whenever you launch a python script from now on, you should have your mozdef virtualenv actived and your LD_LIBRARY_PATH env variable should include /home/mozdef/python2.7/lib/

3.4.2 RabbitMQ

RabbitMQ is used on workers to have queues of events waiting to be inserted into the Elasticsearch cluster (storage).

To install it, first make sure you enabled EPEL repos. Then you need to install an Erlang environment. On Yum-based systems:

```
sudo yum install erlang
```

You can then install the rabbitmq server:

```
rpm --import http://www.rabbitmq.com/rabbitmq-signing-key-public.asc
yum install rabbitmq-server-3.2.4-1.noarch.rpm
```

To start rabbitmq at startup:

```
chkconfig rabbitmq-server on
```

On APT-based systems

```
sudo apt-get install rabbitmq-server
sudo invoke-rc.d rabbitmq-server start
```

3.4.3 Meteor

Meteor is a javascript framework used for the realtime aspect of the web interface.

We first need to install Mongodb since it's the DB used by Meteor.

On Yum-based systems:

In /etc/yum.repo.d/mongo, add:

```
[mongodb]
name=MongoDB Repository
baseurl=http://downloads-distro.mongodb.org/repo/redhat/os/x86_64/
gpgcheck=0
enabled=1
```

Then you can install mongodb:

```
sudo yum install mongodb
```

On APT-based systems:

```
sudo apt-get install mongodb-server
```

For meteor, in a terminal:

```
curl https://install.meteor.com/ | sh

wget http://nodejs.org/dist/v0.10.26/node-v0.10.26.tar.gz
tar xvzf node-v0.10.26.tar.gz
cd node-v0.10.26
./configure
make
make install
```

Make sure you have meteorite/mrt:

```
npm install -g meteorite
```

Then from the meteor subdirectory of this git repository run:

```
mrt add iron-router
mrt add accounts-persona
```

You may want to edit the app/lib/settings.js file to properly point to your elastic search server:

```
elasticsearch={
  address:"http://servername:9200/",
  healthurl:"_cluster/health",
  docstatsurl:"_stats/docs"
}
```

Then start meteor with:

```
meteor
```

3.4.4 Node

Alternatively you can run the meteor UI in 'deployment' mode using a native node installation.

First install node:

```
yum install bzip2 gcc gcc-c++ sqlite sqlite-devel
wget http://nodejs.org/dist/v0.10.25/node-v0.10.25.tar.gz
tar xvfz node-v0.10.25.tar.gz
cd node-v0.10.25
python configure
make
make install
```

Then bundle the meteor portion of mozdef:

```
cd <your meteor mozdef directory>
meteor bundle mozdef.tgz
```

You can then deploy the meteor UI for mozdef as necessary:

```
scp mozdef.tgz to your target host
tar -xvzf mozdef.tgz
```

This will create a 'bundle' directory with the entire UI code below that directory.

You will need to update the settings.js file to match your servername/port:

```
vim bundle/programs/server/app/app/lib/settings.js
```

If your development OS is different than your production OS you will also need to update the fibers node module:

```
cd bundle/programs/server/node_modules
rm -rf fibers
sudo npm install fibers@1.0.1
```

Then run the mozdef UI via node:

```
export MONGO_URL=mongodb://mongoservername:3002/meteor
export ROOT_URL=http://meteorUIservername/
export PORT=443
node bundle/main.js
```

3.4.5 Nginx

We use nginx webserver.

You need to install nginx:

```
sudo yum install nginx
```

On apt-get based system:

```
sudo apt-get nginx
```

If you don't have this package in your repos, before installing create */etc/yum.repos.d/nginx.repo* with the following content:

```
[nginx]
name=nginx repo
baseurl=http://nginx.org/packages/centos/6/$basearch/
gpgcheck=0
enabled=1
```

3.4.6 UWSGI

We use uwsgi to interface python and nginx:

```
wget http://projects.unbit.it/downloads/uwsgi-2.0.2.tar.gz
tar zxvf uwsgi-2.0.2.tar.gz
~/python2.7/bin/python uwsgiconfig.py --build
~/python2.7/bin/python uwsgiconfig.py  --plugin plugins/python core
cp python_plugin.so ~/envs/mozdef/bin/
```

```
cp uwsgi ~/envs/mozdef/bin/

cd rest
# modify settings.py
vim settings.py
# modify uwsgi.ini
vim uwsgi.ini
uwsgi --ini uwsgi.ini

cd ../loginput
# modify uwsgi.ini
vim uwsgi.ini
uwsgi --ini uwsgi.ini

sudo cp nginx.conf /etc/nginx
# modify /etc/nginx/nginx.conf
sudo vim /etc/nginx/nginx.conf
sudo service nginx restart
```

3.4.7 Kibana

Kibana is a webapp to visualize and search your Elasticsearch cluster data:

```
wget https://download.elasticsearch.org/kibana/kibana/kibana-3.0.0milestone5.tar.gz
tar xvzf kibana-3.0.0milestone5.tar.gz
mv kibana-3.0.0milestone5 kibana
# configure /etc/nginx/nginx.conf to target this folder
sudo service nginx reload
```

To initialize elasticsearch indices and load some sample data:

```
cd examples/es-docs/
python inject.py
```

CHAPTER 4

Screenshots

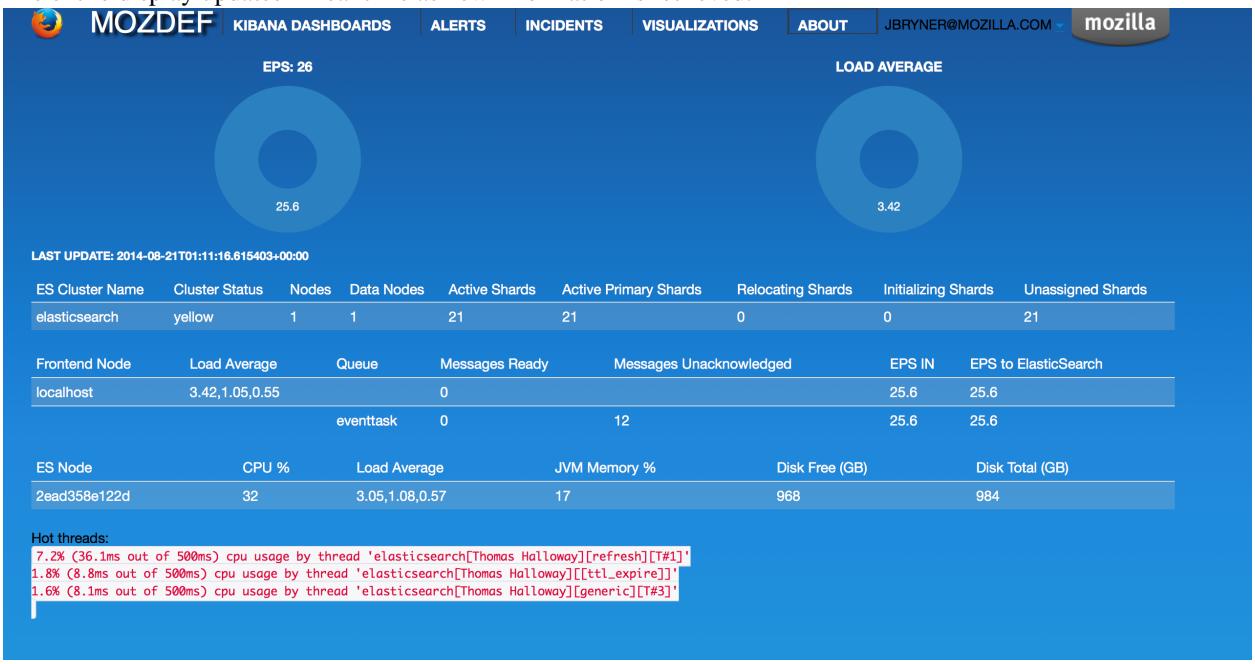
Here are a few screen captures of key portions of the MozDef user interface.

4.1 Health and Status

MozDef includes an integrated health and status screen under the 'about' menu showing key performance indicators like events per second from rabbit-mq and elastic search cluster health.

You can have as many front-end processors running rabbit-mq as you like in whatever geographic distribution makes sense for your environment. The hot threads section shows you what your individual elastic search nodes are up to.

The entire display updates in real time as new information is retrieved.

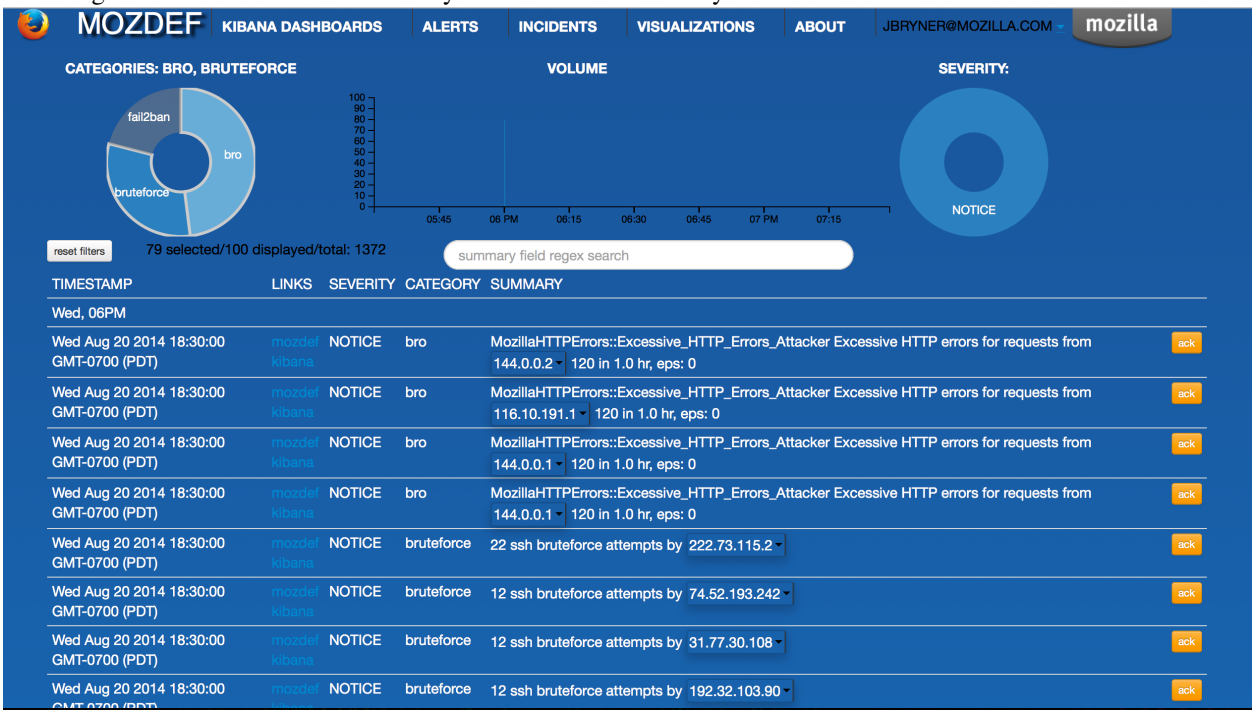


4.2 Alerts

Alerts are simply python jobs run as celery tasks that query elastic search for either individual events, or correlate multiple events into an alert.

The alerts screen shows the latest 100 alerts and allows interactive filtering by category, severity, time frame and free-form regex.

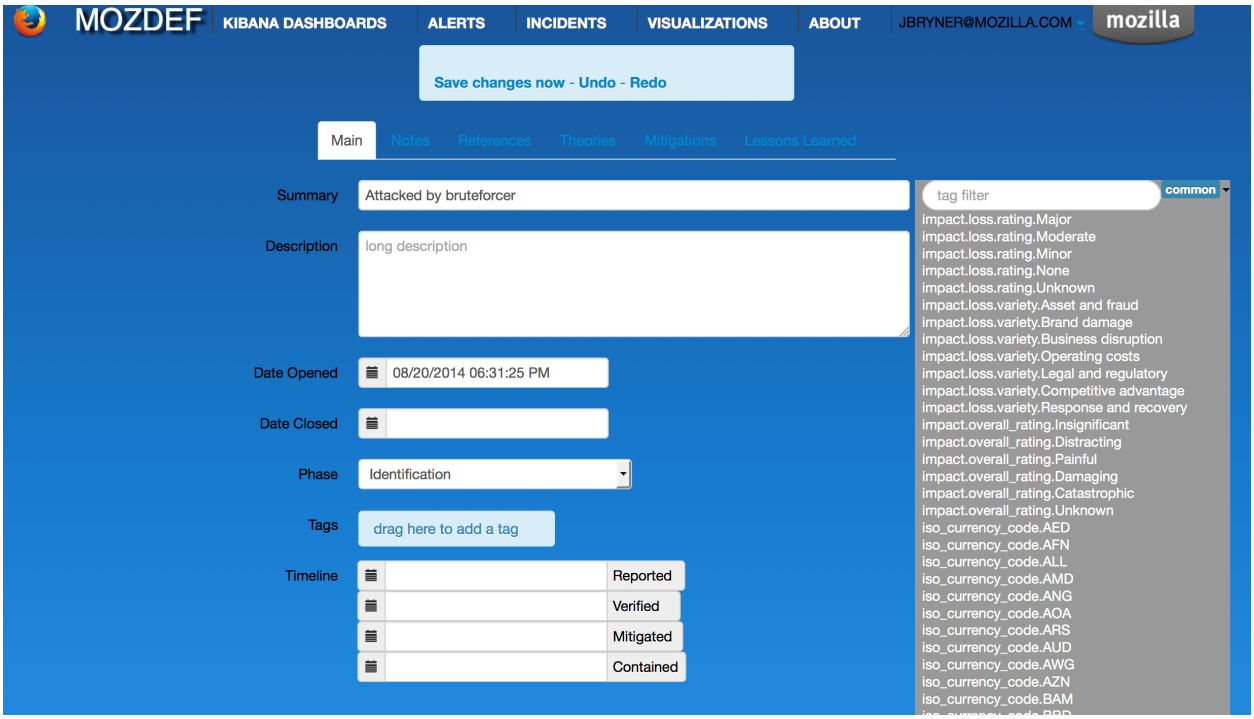
The display updates in real time as new alerts are received and any IP address in an alert is decorated with a menu allowing you to query whois, dshield, CIF, etc to get context on the item. If your facilities include blocking, you can also integrate that into the menu to allow you to block an IP directly from this screen.



4.3 Incident Handling

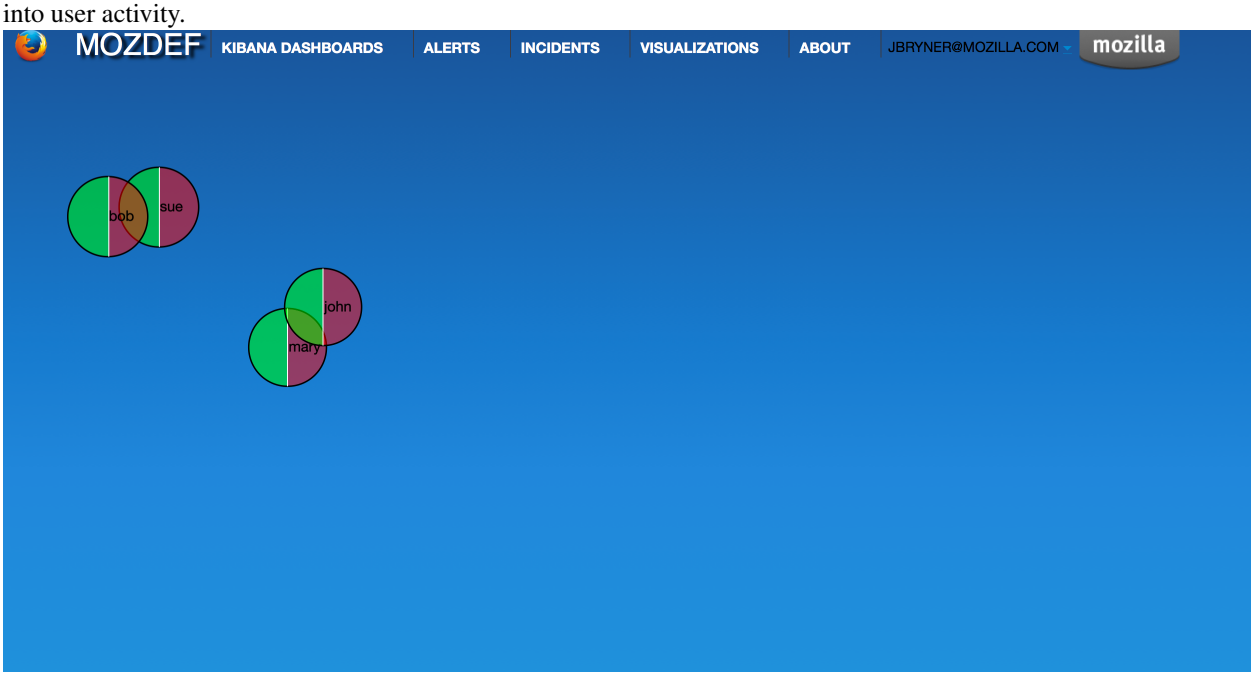
MozDef includes an integrated, real time incident handling facility that allows multiple responders to work collaboratively on a security incident. As they add information to the incident they are able to see each others changes as they happen, in real time.

MozDef includes integration into the VERIS classification system to quickly tag incidents with metadata by dragging tags onto the incident which allows you to aggregate metrics about your incidents.



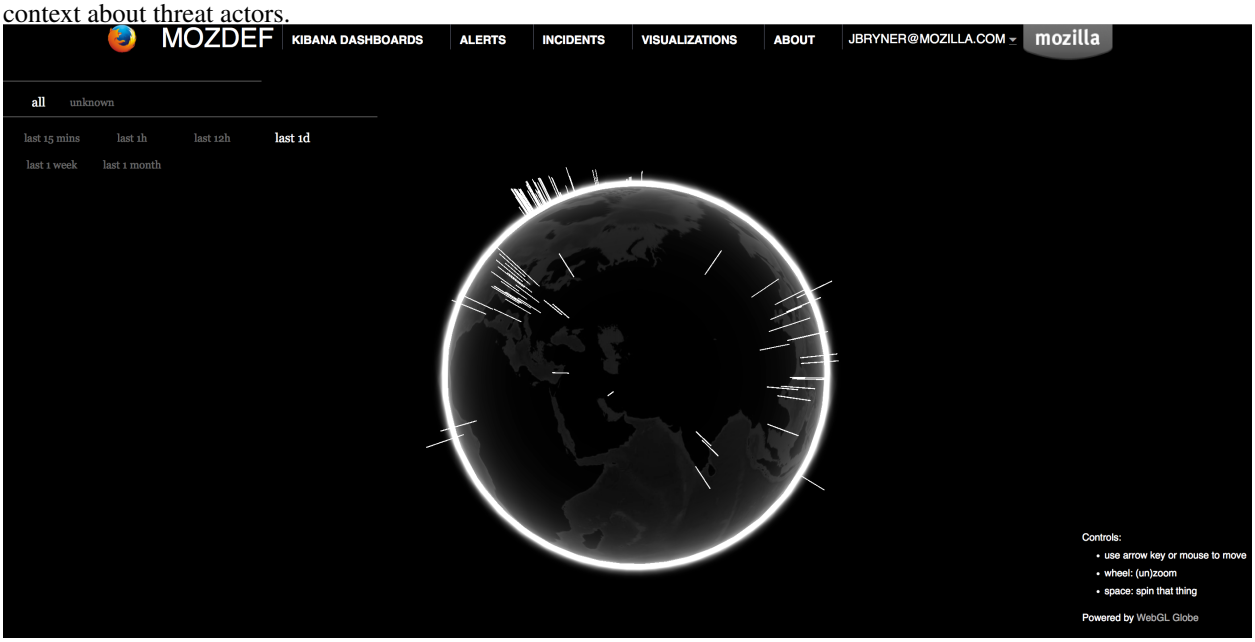
4.4 d3 visualizations

The d3.js library is included in MozDef to allow you custom visualizations of your data. The is a sample visualization of login counts (success vs failed) that you can integrate into your central authentication directory for quick context into user activity.



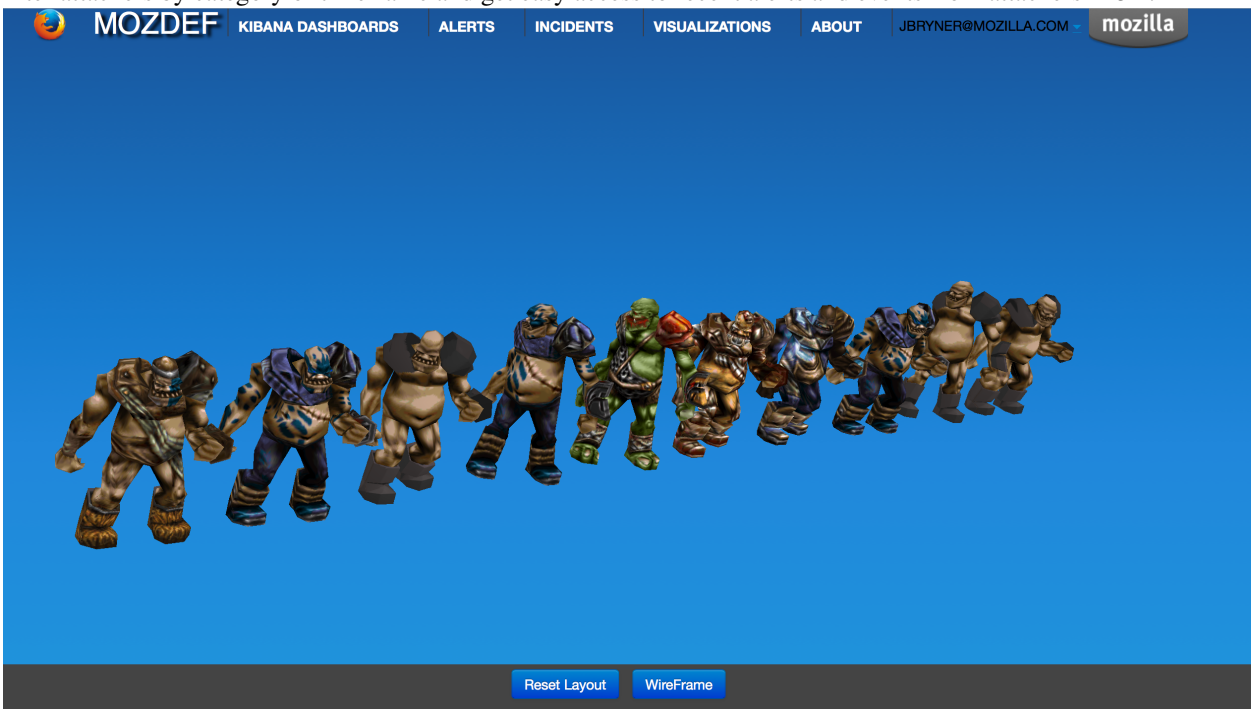
4.5 Geo location of Attackers

MozDef includes the WebGL globe as a three.js visualization that geolocates attackers to give you quick, interactive context about threat actors.



4.6 3D interactive Attacker visualization

MozDef correlates alerts and events into a 3D visual representation of attackers as ogres. You can use this to quickly filter attackers by category or timeframe and get easy access to recent alerts and events from attackers in 3D.



CHAPTER 5

Demo Instance

Mozilla maintains a demo instance of MozDef that you can use try out the UI and get a feel for it in a live environment with test/random data.

Simply browse to http://demo.mozdef.com:3000 and login using any gmail or yahoo email address. No credentials/passwords are sent to the demo instance, though your email will be logged. If you'd prefer you can also use mozdef@mockmyid.com as a userID which will not prompt for any credentials.

CHAPTER 6

Usage

6.1 Web Interface

MozDef uses the Meteor framework for the web interface and bottle.py for the REST API. For authentication, MozDef ships with native support for Persona. Meteor (the underlying UI framework) also supports many authentication options including google, github, twitter, facebook, oath, native accounts, etc.

6.1.1 Events visualizations

Since the backend of MozDef is Elastic Search, you get all the goodness of Kibana with little configuration. The MozDef UI is focused on incident handling and adding security-specific visualizations of SIEM data to help you weed through the noise.

6.1.2 Alerts

Alerts are generally implemented as Elastic Search searches, or realtime examination of the incoming message queues. MozDef provides a plugin interface to allow open access to event data for enrichment, hooks into other systems, etc.

6.1.3 Incident handling

6.2 Sending logs to MozDef

Events/Logs are accepted as json over http(s) with the POST or PUT methods or over rabbit-mq. Most modern log shippers support json output. MozDef is tested with support for:

- heka
- beaver
- nxlog
- logstash
- native python code
- AWS cloudtrail (via native python)

We have some configuration snippets

6.2.1 What should I log?

If your program doesn't log anything it doesn't exist. If it logs everything that happens it becomes like the proverbial boy who cried wolf. There is a fine line between logging too little and too much but here is some guidance on key events that should be logged and in what detail.

Event	Example	Rationale
Authentication Events	Failed/Success logins	Authentication is always an important event to log as it establishes traceability for later events and allows correlation of user actions across systems.
Authorization Events	Failed attempts to insert/update/delete a record or access a section of an application.	Once a user is authenticated they usually obtain certain permissions. Logging when a user's permissions do not allow them to perform a function helps troubleshooting and can also be helpful when investigating security events.
Account Lifecycle	Account creation/deletion/update	Adding, removing or changing accounts are often the first steps an attacker performs when entering a system.
Password/Key Events	Password changed, expired, reset. Key expired, changed, reset.	If your application takes on the responsibility of storing a user's password (instead of using centralized LDAP/persona) it is important to note changes to a users credentials or crypto keys.
Account Activations	Account lock, unlock, disable, enable	If your application locks out users after failed login attempts or allows for accounts to be inactivated, logging these events can assist in troubleshooting access issues.
Application Exceptions	Invalid input, fatal errors, known bad things	If your application catches errors like invalid input attempts on web forms, failures of key components, etc creating a log record when these events occur can help in troubleshooting and tracking security patterns across applications. Full stack traces should be avoided however as the signal to noise ratio is often overwhelming. It is also preferable to send a single event rather than a multitude of events if it is possible for your application to correlate a significant exception. For example, some systems are notorious for sending a connection event with source IP, then sending an authentication event with a session ID then later sending an event for invalid input that doesn't include source IP or session ID or username. Correctly correlating these events across time is much more difficult than just logging all pieces of information if it is available.

6.3 JSON format

This section describes the structure JSON objects to be sent to MozDef. Using this standard ensures developers, admins, etc are configuring their application or system to be easily integrated into MozDef.

6.3.1 Background

Mozilla used CEF as a logging standard for compatibility with Arcsight and for standardization across systems. While CEF is an admirable standard, MozDef prefers JSON logging for the following reasons:

- Every development language can create a JSON structure
- JSON is easily parsed by computers/programs which are the primary consumer of logs

- CEF is primarily used by Arcsight and rarely seen outside that platform and doesn't offer the extensibility of JSON
- A wide variety of log shippers (heka, logstash, fluentd, nxlog, beaver) are readily available to meet almost any need to transport logs as JSON.
- JSON is already the standard for cloud platforms like amazon's cloudtrail logging

6.3.2 Description

As there is no common RFC-style standard for json logs, we prefer the following structure adapted from a combination of the graylog GELF and logstash specifications.

Note all fields are lowercase to avoid one program sending sourceIP, another sending sourceIp, another sending SourceIPAddress, etc. Since the backend for MozDef is elasticsearch and fields are case-sensitive this will allow for easy compatibility and reduce potential confusion for those attempting to use the data. MozDef will perform some translation of fields to a common schema but this is intended to allow the use of heka, nxlog, beaver and retain compatible logs.

6.3.3 Mandatory Fields

Field	Purpose	Sample Value
category	General category/type of event matching the 'what should I log' section below	Authentication, Authorization, Account Creation, Shutdown, Startup, Account Deletion, Account Unlock, brointel, bronotice
details	Additional, event-specific fields that you would like included with the event. Please completely spell out a field rather an abbreviate: i.e. sourceipaddress instead of srcip.	"dn": "john@example.com,o=com, dc=example", "facility": "daemon"
hostname	The fully qualified domain name of the host sending the message	server1.example.com
processid	The PID of the process sending the log	1234
processname	The name of the process sending the log	myprogram.py
severity	RFC5424 severity level of the event in all caps: DEBUG, INFO, NOTICE, WARNING, ERROR, CRITICAL, ALERT, EMERGENCY	INFO
source	Source of the event (file name, system name, component name)	/var/log/syslog/2014.01.02.log
summary	Short human-readable version of the event suitable for IRC, SMS, etc.	john login attempts over threshold, account locked
tags	An array or list of any tags you would like applied to the event	vpn, audit nsm,bro,intel
timestamp	Full date plus time timestamp of the event in ISO format including the timezone offset	2014-01-30T19:24:43+00:00

6.3.4 Details substructure (optional fields)

Field	Purpose	Used In	Sample Value
destination-ipaddress	Destination IP of a network flow	NSM/Bro/Intel	8.8.8.8
destination-port	Destination port of a network flow	NSM/Bro/Intel	80
dn	Distinguished Name in LDAP, mean unique ID in the ldap hierarchy	event/ldap	john@example.org,o=org, dc=example
filedesc		NSM/Bro/Intel	
filemime-type		NSM/Bro/Intel	
fuid		NSM/Bro/Intel	
result	Result of an event, success or failure	event/ldap	LDAP_SUCCESS
seenindicator	Intel indicator that matched as seen by our system	NSM/Bro/Intel	evil.com/setup.exe
seenindicator_type	Type of intel indicator	NSM/Bro/Intel	HTTP::IN_URL
seenwhere	Where the intel indicator matched (which protocol, which field)	NSM/Bro/Intel	Intel::URL
source	Source of the connection	event/ldap	Mar 19 15:36:25 ldap1 slapd[31031]: conn=6633594 fd=49 ACCEPT from IP=10.54.70.109:23957 (IP=0.0.0.0:389) Mar 19 15:36:25 ldap1 slapd[31031]: conn=6633594 op=0 BIND
sourceipaddress	Source IP of a network flow	NSM/Bro/Intel event/ldap	8.8.8.8
source-port	Source port of a network flow	NSM/Bro/Intel	42297
sources	Source feed	NSM/Bro/Intel	CIF - need-to-know
success	Auth success	event/ldap	True
uid	Bro connection uid	NSM/Bro/Intel	CZqhEs40odso1tFNx3

6.3.5 Examples

```
{
    "timestamp": "2014-02-14T11:48:19.035762739-05:00",
    "hostname": "fedbox",
    "processname": "/tmp/go-build278925522/command-line-arguments/_obj/exe/log_json",
    "processid": 3380,
    "severity": "INFO",
    "summary": "joe login failed",
    "category": "authentication",
    "source": "",
    "tags": [
```

```
        "MySystem",
        "Authentication"
    ],
    "details": {
        "user": "joe",
        "task": "access to admin page /admin_secret_radioactiv",
        "result": "10 authentication failures in a row"
    }
}
```

6.4 BanHammer

MozDef integrates BanHammer in its web interface to easily ban attackers from your network. To enable this feature, in `meteor/app/lib/settings`, change the `enableBanhammer` option to `true`, and modify set your BanHammer DB parameters in `rest/index.conf`:

```
banhammerenable=True
banhammerdbhost="localhost"
banhammerdbuser="root"
banhammerdbpasswd=""
banhammerdbdb="banhammer"
```

6.5 Writing alerts

Alerts allow you to create notifications based on events stored in elasticsearch. You would usually try to aggregate and correlate events that are the most severe and on which you have response capability. Alerts are stored in the alerts folder.

There are two types of alerts:

- simple alerts that consider events on at a time. For example you may want to get an alert everytime a single LDAP modification is detected.
- aggregation alerts allow you to aggregate events on the field of your choice. For example you may want to alert when more than 3 login attempts failed for the same username.

To narrow the events your alert sees, you need to specify filters. You can either use pyes to do that or load them from a Kibana dashboard.

You'll find documented examples in the alerts folder.

Once you've written your alert, you need to configure it in celery to be launched periodically. If you have a `AlertBruteforceSsh` class in a `alerts/bruteforce_ssh.py` file for example, in `alerts/lib/config` you can configure the task to run every minute:

```
ALERTS = {
        'bruteforce_ssh.AlertBruteforceSsh': crontab(minute='*/1'),
}
```

CHAPTER 7

Advanced Settings

7.1 Using local accounts

MozDef ships with support for persona which is Mozilla's open source, browser-based authentication system. You should be to use any gmail or yahoo account to login to get started.

To change authentication to something less public like local accounts here are the steps:

Assuming Meteor 9.1 (current as of this writing) which uses it's own package manager:

1. From the mozdef meteor directory run '$ meteor remove mrt:accounts-persona'
2. 'meteor add accounts-password'
3. Alter app/server/mozdef.js Accounts.config section to: forbidClientAccountCreation: false,
4. Restart Meteor

This will allow people to create accounts using almost any combination of username/password. To add restrictions, limit domains, etc please see: http://docs.meteor.com/#accounts_api

CHAPTER 8

Code

8.1 Plugins

The front-end event processing portion of MozDef supports python plugins to allow customization of the input chain. Plugins are simple python modules than can register for events with a priority, so they only see events with certain dictionary items/values and will get them in a predefined order.

To create a plugin, make a python class that presents a registration dictionary and a priority as follows:

```
class message(object):
    def __init__(self):
        '''register our criteria for being passed a message
           as a list of lower case strings or values to match with an event's dictionary of keys or v
           set the priority if you have a preference for order of plugins to run.
           0 goes first, 100 is assumed/default if not sent
        '''
        self.registration = ['sourceipaddress', 'destinationipaddress']
        self.priority = 20
```

8.1.1 Message Processing

To process a message, define an onMessage function within your class as follows:

```
def onMessage(self, message, metadata):
    #do something interesting with the message or metadata
    return (message, metadata)
```

The plugin will receive a copy of the incoming event as a python dictionary in the 'message' variable. The plugin can do whatever it wants with this dictionary and return it to MozDef. Plugins will be called in priority order 0 to 100 if the incoming event matches their registration criteria. i.e. If you register for sourceipaddress you will only get events containing the sourceipaddress field.

If you return the message as None (i.e. message=None) the message will be dropped and not be processed any further. If you modify the metadata the new values will be used when the message is posted to elastic search. You can use this to assign custom document types, set static document _id values, etc.

8.1.2 Plugin Registration

Simply place the .py file in the plugins directory where the esworker.py is located, restart the esworker.py process and it will recognize the plugin and pass it events as it sees them.

CHAPTER 9

Benchmarking

Performance is important for a SIEM because it's where you want to store, search and analyze all your security events.

You will want it to handle a significant number of new events per second, be able to search quickly and perform fast correlation. Therefore, we provide some benchmarking scripts for MozDef to help you determine the performance of your setup. Performance tuning of elastic search can be complex and we highly recommend spending time tuning your environment.

9.1 Elasticsearch

Elasticsearch is the main backend component of MozDef. We strongly recommend you to have a 3+ nodes cluster to allow recovery and load balancing. During our tests, Elasticsearch recovered well after being pushed to the limits of hardware, loosing and regaining nodes, and a variety of valid/invalid data. We provide the following scripts for you to use to test your own implementation.

The scripts for Elasticsearch benchmarking are in *benchmarking/es/*. They use nodejs to allow asynchronous HTTP requests.

9.1.1 insert_simple.js

insert_simple.js sends indexing requests with 1 log/request.

Usage: *node ./insert_simple.js <processes> <totalInserts> <host1> [host2] [host3] [...]*

- *processes*: Number of processes to spawn
- *totalInserts*: Number of inserts to perform, please note after a certain number node will slow down. You want to have a lower number if you are in this case.
- *host1*, *host2*, *host3*, etc: Elasticsearch hosts to which you want to send the HTTP requests

9.1.2 insert_bulk.js

insert_bulk.js sends bulk indexing requests (several logs/request).

Usage: *node ./insert_bulk.js <processes> <insertsPerQuery> <totalInserts> <host1> [host2] [host3] [...]*

- *processes*: Number of processes to spawn
- *insertsPerQuery*: Number of logs per request

- *totalInserts*: Number of inserts to perform, please note after a certain number node will slow down. You want to have a lower number if you are in this case.
- *host1*, *host2*, *host3*, etc: Elasticsearch hosts to which you want to send the HTTP requests

9.1.3 search_all_fulltext.js

search_all_fulltext.js performs search on all indices, all fields in fulltext. It's very stupid.

Usage: *node ./search_all_fulltext.js <processes> <totalSearches> <host1> [host2] [host3] [...]*

- *processes*: Number of processes to spawn
- *totalSearches*: Number of search requests to perform, please note after a certain number node will slow down. You want to have a lower number if you are in this case.
- *host1*, *host2*, *host3*, etc: Elasticsearch hosts to which you want to send the HTTP requests

CHAPTER 10

Contributors

Here is the list of the awesome contributors helping us or that have helped us in the past:

- Yohann Lepage (@2xyo) yohann INSERTAT lepage INSERTDOT info (docker configuration)
- Björn Arnelid bjorn.arnelid INSERTAT gmail INSERTDOT com

CHAPTER 11

Indices and tables

- genindex
- modindex
- search

CHAPTER 12

License

license

CHAPTER 13

Contact

- opsec+mozdef INSERTAT mozilla.com
- Jeff Bryner, jbryner INSERTAT mozilla.com @0x7eff
- Anthony Verez, @netantho
- https://lists.mozilla.org/listinfo/dev-mozdef