
WISE
With Intelligence See Everything
Andy Wick

What is it

- **Moloch SPI data enhancer**
  - Can match on host/domains, md5, url, ip, ja3, email or almost any field
  - Can set almost any field in SPI data
  - Can add menu options (called right clicks still)
- **Supported data sources**
  - Simple Files
  - Commercial Services: OpenDNS, Emerging Threats Pro, Threatstream, ...
  - Elasticsearch/Redis
  - Splunk
- **Multilayer caching**
  - Capture
  - WISE Memory
  - Redis

verizon media

Sessions Example #1 - Subnets Database

Moloch uses WISE to query every single IP in a subnets database. Any matches creates new fields in sessions

verizon media

Sessions Example #2 - Threatstream

Moloch uses WISE to query every single IP, domain, md5 in Threatstream. Matches add fields to sessions

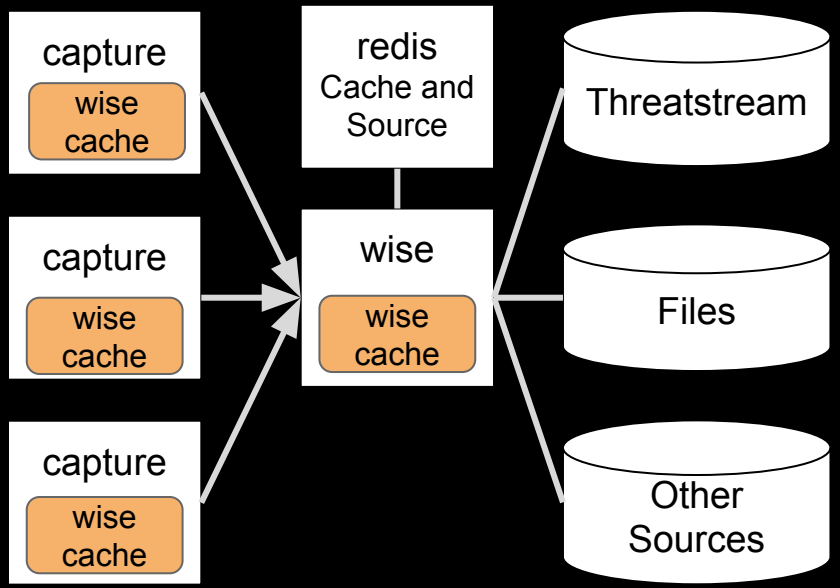
verizon media

SPI View Example #3 - Threatstream

SPI View allows you to see all the unique values for each field with counts

verizon media

Architecture

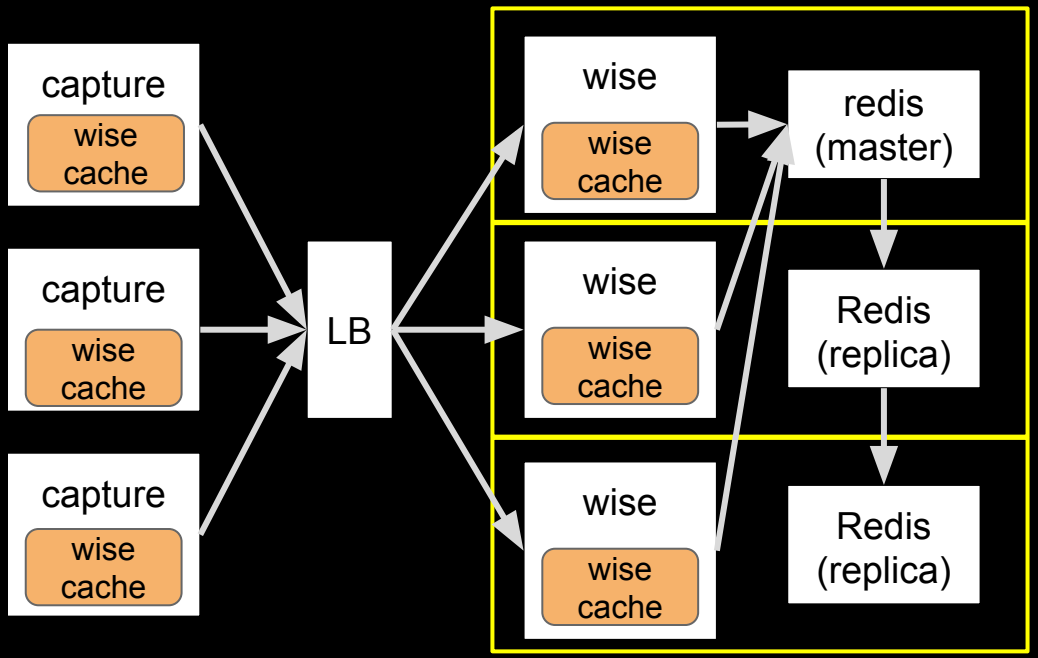


For performance reasons lookups are cached at multiple layers.

1) Check wise cache in capture (ALWAYS)
2) Check wiseService cache (for some sources)
3) Check redis cache (if configured)
4) Query the data source for information

verizon media

Architecture - Caching with multiple wise



verizon media

Capture & Viewer Configuration

Set in [default] and/or for each capture node
wiseHost=wisehost.example.com

Semicolon ';' separated list of viewer plugins to load and the order to load in
viewerPlugins=wise.js

Semicolon ';' separated list of capture plugins to load and the order to load in
plugins=wise.so

verizon media

Data source configuration

- **Like capture/viewer, everything in an ini file**
- **Each data source has its own section**
  - Some sections are unique like [threatstream]
  - Some sections have prefixes like [file:filename] and [url:urlname]
- **Most feeds just require simple configuration with defaults being good enough**
- **All WISE sources implement some common options**
  - cacheAgeMin - For those that cache
  - excludeDomains, excludeEmails, excludeURLs - don't lookup matching items
  - excludeEmails, excludeURLs - support wildcards
  - excludeIPs - CIDR
- **See WISE settings page for configuration options**

verizon media

Sample WISE Configuration

```
# wiseService contains global settings and global excludes
[wiseService]
excludeDomains=*.zen.spamhaus.org;*.in-addr.arpa;*.dnsbl.sorbs.net;*.ip6.arp
a

[reversedns]
ips=192.168.0.0/16;10.0.0.0/8;172.20.0.0/21
field=asset

[file:badbadbad.ip]
file=/data/moloch/wisefiles/badbadbad.ip
tags=badbadbad
type=ip
format=tagger
```

verizon media

Tagger Format - badbadbad.ip

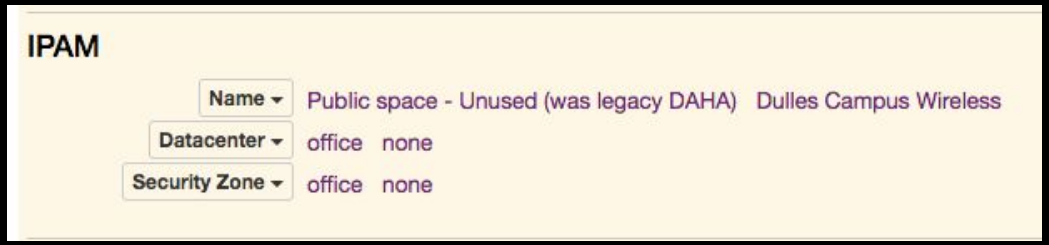
#field:whatever.str;kind:lotermfield;count:true;friendly:A String;db:whatever.str-term;help:Help for String;shortcut:0

#field:tags;shortcut:1

10.0.0.1;0=this is really bad;1=reallyBadTag
10.0.0.2;tags=anotherRealBadTag
10.0.0.3

verizon media

IPAM Example



verizon media

JSON Format - IPAM

[url:ipam]
type = ip
format = json
url = https://exampl.com/getipam.json
reload = 60
keyColumn = CIDR
fields=field:ipam.datacenter;kind:termfield;count:false;friendly:DataCenter;db:ipam.dc-term;help:DataCenter;shortcut:DataCenter\nfield:ipam.zone;kind:termfield;count:true;friendly:Security Zone;db:ipam.zone-term;help:Security Zone;shortcut:SecurityZone

verizon media

JSON Sample Data

```
[
    {"DataCenter": "none",
    "SecurityZone": "none",
    "CIDR": "10.0.0.0/8"},

    {"DataCenter": "none",
    "SecurityZone": "office",
    "CIDR": "10.66.0.0/16"}
]
```

verizon media

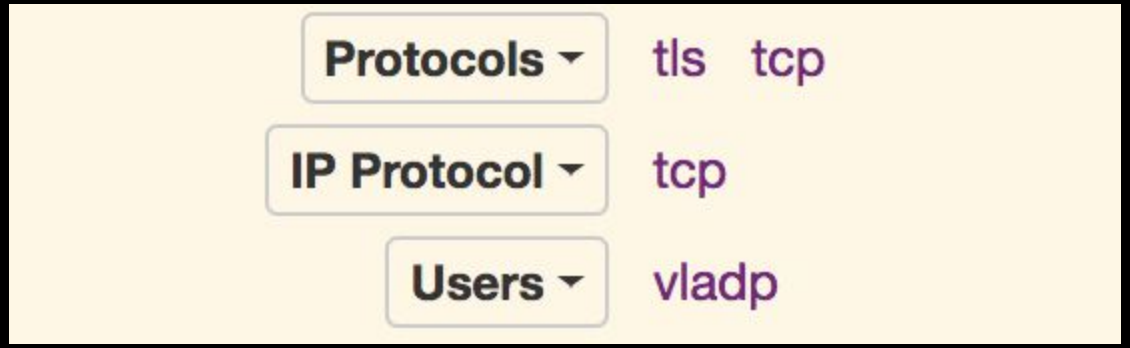
Elasticsearch Source - Get username from panos

```
[elasticsearch:user]
type=ip
onlyIPs=10.10.0.0/16                          = Our VPN space
elasticsearch=https://elk.example.com:9200
esIndex=panos-*                               = index to search against
esTimestampField=@timestamp                   = what field has the timestamps
esQueryField=sourceIP                         = field to check against
esMaxTimeMS=86400000                          = range of data to search around
esResultField=sourceUserName                  = what json field must exist in results
fields=field:user;shortcut:sourceUserName     = what SPI data fields to set

{"sourceIP" : "10.10.10.10",
"sourceUserName" : "andywick",
"@timestamp" : "2014-11-13T00:13:32.000Z", ...}
```

verizon media

Example Users Display



verizon media

Splunk - Table Query

```
type = ip
format = json
host = splunk.host.example.com
port=5500
username={{wise.splunk.user}}
password={{wise.splunk.password}}
periodic=60
query=search index="vpnlog" sourcetype="vpn" assigned earliest=-24h | rex
"User <(?<user>[^>]+)>.*IPv4 Address <(?<vpn_ip>[^>]+)>" | dedup vpn_ip |
table user, vpn_ip
keyColumn=vpn_ip
fields=field:user;shortcut:user
```

verizon media

Right clicks

```
[right-click]
VTIP=url:https://www.virustotal.com/en/ip-address/%TEXT%/information/;name:Virus Total
IP;category:ip
VTHOST=url:https://www.virustotal.com/en/domain/%HOST%/information/;name:Virus Total
Host;category:host
VTURL=url:https://www.virustotal.com/latest-scan/%URL%;name:Virus Total URL;category:url
PTHOST=url:https://passivetotal.org/search/%TEXT%;name:Passivetotal Host;category:host
PTIP=url:https://passivetotal.org/search/%TEXT%;name:Passivetotal IP;category:ip
PTEMAIL=url:https://passivetotal.org/search/%TEXT%;name:Passivetotal User;category:user
```

(should be renamed “Field Actions”)

verizon media

Creating Views - Old way

```
this.api.addView("threatstream",
    "if (session.threatstream)\n" +
    "  div.sessionDetailMeta.bold Threatstream\n" +
    "  dl.sessionDetailMeta\n" +
    "    +arrayList(session.threatstream, 'severity-term', 'Severity',
'threatstream.severity')\n" +
    "    +arrayList(session.threatstream, 'confidence', 'Confidence',
'threatstream.confidence')\n" +
    "    +arrayList(session.threatstream, 'id', 'Id', 'threatstream.id')\n" +
    "    +arrayList(session.threatstream, 'importId', 'Import Id',
'threatstream.importId')\n" +
    "    +arrayList(session.threatstream, 'type-term', 'Type', 'threatstream.type')\n" +
    "    +arrayList(session.threatstream, 'maltype-term', 'Malware Type',
'threatstream.maltype')\n" +
    "    +arrayList(session.threatstream, 'source-term', 'Source', 'threatstream.source')\n”
)
```

verizon media

Creating Views - New way

```
require:threatstream;title:Threatstream;fields:threatstream
.severity,threatstream.confidence,threatstream.id,threatstr
eam.importId,threatstream.type,threatstream.maltype,threats
tream.source
```

verizon media

Wise Types

You can now add fields to already created wise types, or create new wise types

This examples add a new “mac” type and adds to the md5 type a new field “blahblah.md5”

```
[wise-types]
mac=db:srcMac;mac.dst
md5=db:http.md5;db:email.md5;db:blahblah.md5
```

verizon media

Todo

- Make creating new sources easier
- Add UI to see wise state and configuration
- Support multiple WISE servers on one machine better
- Include more examples with the release

verizon media


QUESTIONS?