Jigsaw Security

Threat Intelligence

Platform Version 4.6

Jigsaw Security Enterprise Inc.

2664 Timber Drive Suite 342 Garner NC 27529

(800)447-2150 x6 – Security Operations

Jigsaw Security Proprietary Document

Contents

Introduction 4
Automation of Threat Intelligence 4
Platform Components – Base Configuration 6
Additional Modules – Additional Cost 6
Deployment of the Platform 7
Hardware Requirements for Jigsaw Security Platform 8
Node Profiles for Standard Deployment 8
Third Party Software Versions in our Platform – Open Source 9
Ingest Options and Configurations 9
Logstash 10
Apache NIFI 11
Jigsaw Replicator 11
Jigsaw Platform Installation (Partners and Integrators Only) 12
Configuration File Locations 13
Record Level Security Module 14
Platform Monitoring System 14
Platform Features (A Discussion on X-Pack) 15
Matchstick Analytics 16
A walkthrough of the Jigsaw Analytics Platform 18
Matchstick and DNS Sinkhole Alerting 18
Matchstick and Log File Detection 20
IOC Repository 21
IOC Pattern Monitoring 21
MHN (Modern Honeypot Network) - Integration 23
Jigsaw Compliance Login Module 25
Jigsaw Auditing Lockdown Program 26
Management Tools 26
Index Management 27
Ingestion Monitoring Utility 28
Apache Nifi Integration 29

Time Series Applications 29

Searching for IOC data and reference information 30

About Visualizations and Platform Training 30

About the Jigsaw Honeypot Network 31

Introduction

The Jigsaw Security IOC service provides a method for consuming threat intelligence data for use within your organization. Using an API and automation makes the integration of our threat intelligence feeds easy as we provide output in common formats that can be used natively by most security products. Combined with our Jigsaw Security platform the threat intelligence is a way to identify threats in your network environment quickly and efficiently. In addition to signature based activity monitoring our alerting and time series modules will find things that are not in signatures that may indicate a threat to your end users.

One of the greatest challenge in any threat intelligence implementation is being able to make use of the intelligence data being provided. When we set out to create this service our focus in addition to the collection of threat intelligence was to make that threat intelligence useable in our customer's networks. Our thought was that without providing common formatted data that the intelligence service would be nothing more than a system used to search for attackers after the fact. Our goal is to detect threats in real time and to stop threats not just highlight them after the attack has already occurred. This guide will explain in detail exactly how to incorporate our threat intelligence into your operations and ensure that you have the most relevant and up to date information protecting your network.

If at any time, you have any questions concerning the best ways to use our threat intelligence products please feel free to call our support staff at 800-447-2150 x6 and we will assist you through the process.

Automation of Threat Intelligence

Automation functionality is designed to automatically generate signatures for intrusion detection systems and RPZ files for DNS servers to automatically drop malicious activity. This system is built around our shared Intelligence Malware Information Sharing Platform (Enterprise MISP). To utilize the threat intelligence data, you must have two things: first you must have an account on our MISP service which is provided when you subscribe to our threat intelligence service and you must have an API key (provided in the platform) that allows you access to the data in an automated process.

Once you have your account and API key you will use the online portal access to share intelligence with our subscribers that may be of interest and to suggest changes to our included intelligence information. You can make proposals to other entities events or create your own events. You can also create your very own threat intelligence library just for your organization if you wish. This is an automated method for managing blocking and DNS RPZ sinkhole in your organization without affecting anybody else. What

this means is you can create blocklist in the platform that apply only to your organization that are not visible to other users of our system or if you have information you would like to share with the greater community you can do that as well.

A feature in the platform known as tagging allows you to tag events and create groups of events. When using the API, you can use these tags to only export the data that you are interested in. Users can create an unlimited number of tags in the platform for organize data for their use case.

The following guide should assist you in setting up the appropriate feeds. You will need to log in to the IOC Threat Data user interface at http://ui.slcsecurity.com/ to see the tags currently available in the system as these tags are user generated.

In the next section, we will setup an automated pull using a script of threat intel data.

- NOTE – You should never pull more than 1 day's threat intelligence data at a time. If you need to download the entire list, you can do so in the "Event Actions" by selecting "Export" as the indicators are cached and do not put a load on the API functionality of the platform.

Platform Delivery Methods

At Jigsaw Security, we believe in giving our customers a method to incorporate our solutions into their existing security product matrix. The platform will be provided in one of the following manners.

- Physical Installation
- Virtual VMWare or VirtualBox (preferred) VM Appliance
- Installation within a hosting environment such as Amazon, Rackspace (Preferred for performance reasons and cost)
- Jigsaw Hosted Solution – A dedicated cluster installed in a Jigsaw Security provided network, rack and with Internet connectivity

The best solution for installing the platform is the physical deployment method where we purchase servers, install the platform, and ship the hardware to your location for local installation. This ensures that the platform is installed correctly and is setup with your Jigsaw API key for receiving updates.

Platform Components – Base Configuration

Jigsaw Platform: ELK Stack includes Elasticsearch, Kibana and Logstash with Apache NIFI Ingest pre-configured.

Alerting Module: Pre-Installed time series alerting

Timelion Module: Pre-Installed Charting and Graphing Module

Matchstick IOC Matching Analytics: Jigsaw Security proprietary IOC to ingested data log file, packet, and raw data string matching library

LMI: Leaked Credentials Search Module: Jigsaw Security proprietary leaked credential monitor

Reverse Proxy: Provides authentication to the platform

Apache NIFI – Easily ingest web pages, RSS feeds, FTP, SCP, Twitter, or other data in a drag and drop interface in near real time. This makes ingesting data as easy and creating a Visio Diagram.

Additional Modules – Additional Cost

Apache Hadoop Backup Module – Allows full backups of Elasticsearch data to Apache Hadoop. In addition, we can set this module to work with MapR Hadoop to make your Elasticsearch indexes resident in HDFS removing the need for Elasticsearch replication speeding up the ingest process and allowing HDFS to handle replication allowing for 7x compression which allows much longer storage times and ingest speed increases due to HDFS file configurations. This is the preferred method for very large clusters over for archiving of long term data or for clusters greater than 25 nodes.

Financial Trading Advisor Edition – An edition of the platform useful for financial trading. This service provides financial signals to tell you the best time to enter and exit trades and works with stocks and Forex markets.

Data Center DR Replicator – Data Center to Data Center replication for disaster recovery. For high availability environments, this module will replicate your data from one to one or one to many data centers ensuring that in the event of a catastrophic event that your data will remain available and online.

Threat Feed and Data Replication Module – Receive data at one or many remote locations. This service allows Jigsaw to send data to all sites at one time ensuring that all sites have the most up to date threat intelligence data. This service also provide password monitor to show when your organizational credentials have been stolen and will alert you based on our advanced password disclosure feed.

NLP Aware Law Enforcement and Government Edition – A Jigsaw Security module that will find all facets in documents to include people, places, objects, times and dates, locations, or any set of terms. In addition, this module can be combined with our Matchstick analytics for alerting on targeting information. This is a must have for intelligence agencies and law enforcement. Be alerted when fugitives show up in new locations, contact others via the Internet, social media or through other intelligence collection methods.

Deployment of the Platform

Jigsaw Security strongly recommends purchasing hardware and having the Jigsaw Platform deployed by Jigsaw Certified Engineers at our facility. It takes 3 days to get the hardware, 1 day to load and can be shipped the next day. Testing is performed to ensure that the platform can pass our checkout document. The following items are checked prior to shipping.

1. Elasticsearch, Kibana and Logstash start on boot up
2. Jigsaw Analytics run and process data being ingested as scheduled
3. Authentication works properly
4. All plugins, modules, and test data load during testing
5. Ingest Pipeline is tested to include Logstash and Apache NIFI
6. Replication service is tested and data feeds are configured with API

In addition, by purchasing hardware you receive a free 1 year warranty replacement with all hardware included in the price. If you want to use your own hardware we recommend that it be loaded with Ubuntu 16.04 LTS Server version and ship that hardware to our facility for software load. Typical turnaround for software loading is 1-2 business days.

If you are purchasing your own hardware please make sure you order the correct number of computers that fit the parameters in the next section. The source code for the product is NOT included in the

installation. However authorized resellers and distributors do gain access to our deployment servers and/or Github to deploy the system.

Hardware Requirements for Jigsaw Security Platform

Jigsaw Security will support installing the platform on the following hardware specifications. These are the minimum. We highly suggest utilizing Solid State Storage in our platform if possible.

Number of CPU's: 2 (4 is much better on ingest nodes)

Number of Core's Per CPU: 4

Memory: Minimum of 64GB RAM per node (Recommend 128GB on Analytic Nodes)

Minimum Number of Physical or Virtual Servers: 10 Server per Base Cluster

Minimum Drive Storage per Cluster: 2TB per server (1TB minimum)

A clock speed of 2.4GHz per processor recommended. All servers shipped by Jigsaw will be on HP Hardware and will be supported under the HP warranty. We also believe in keeping cost low so we still support Gen5-Gen9 deployments. Gen 5 and 7 refurbished hardware is available at a substantial discount to our customers and comes with a 1 year warranty included.

Node Profiles for Standard Deployment

Jigsaw Security builds our system by deploying all software on all nodes in the cluster and then only activating the needed components based on the use of that node. We support a 4-node profile typical layout. In some cases, or when configuring systems for very specific customer requirements we may modify the layout to support additional functions in the platform.

ES Storage Node – Elasticsearch Data Node

Ingest Node – Includes all ingest products Logstash, NIFI and Replicator

UI Node – Includes Web UI and Reverse Proxy Authentication

Analytics Node – Includes the Jigsaw Analytics Library – If purchased

The typical layout is as follows:

All nodes are configured with the ES Storage Node Role: This ensures maximum utilization of the storage in the servers for long term index storage. Typically, there are 2 ingest nodes a primary and a backup. In some cases, there may be more required for ingest depending on volume and velocity of data being ingested. Typically, we install a single UI node and a backup UI node. This is an active and standby and requires a configuration change to activate. There are typically 2 analytic nodes installed one active and one backup node. Scheduling analytics in CRON is required to activate the standby analytics server in the event of a failure of the main analytic server.

Third Party Software Versions in our Platform – Open Source

Elasticsearch Version 2.3.4

Note: Jigsaw cannot upgrade to Elasticsearch 5 now due to some very substantial changes in Lucene. We will be shipping Elasticsearch 5 updates in 2017 and our analytics will be modified at that time.

Logstash Version 2.3.4

Kibana 4 – Modified Version

Apache NIFI – Version 1.0.1

Built on Ubuntu 16.04LTS

It should be noted that our platform is built on open source but our configuration files, ingest pipelines and analytics are all proprietary and commercial in nature. We list the versions of the open source components so customers and users of the platform can determine if add-on packages they wish to use will work with the deployed versions of the open source in use in this platform.

It should also be noted that all the open source components are left unchanged in the platform. We do not modify the open source components apart from our sensor product which is a port of several open source projects that have been combined to provide a single solution.

Ingest Options and Configurations

Jigsaw Security provides 3 separate ingest methods for the 4.6 version of our software. The most common option is through logstash which is included and installed on /opt/platform/logstash/ directory. We also include some common configurations in the /opt/platform/logstash/bin/config directory. These

configurations may need to be changed to support your installation of the product depending on your specific use cases.

Logstash

To start logstash you must pass a few parameters. In most cases our platform starts logstash automatically and our monitoring processes ensure that the processes are running and ingesting data. In the example below we will start the MISP ingest file to ingest MISP data. Here are the common directories where we preconfigure for storing information for ingestion and specific configurations.

- Ingest Directory - /var/ingest
- Logstash - /opt/platform/logstash
- Elasticsearch - /opt/platform/elasticsearch
- Analytics - /opt/Analytics

To start the MISP ingestion process you would execute the following:

/opt/platform/logstash/bin/elasticsearch -f ./configs/misp.conf &

With this command we start the process and load the misp.conf file as the configuration and detach the process to allow it to run in the background.

Below is the actual misp.conf logstash configuration that ships with the platform.

MISP Configuration Included

```
input {
      file {
            path => "/var/ingest/misp/*"
            type => "core2"
            start_position => "beginning"
            sincedb_path => "/var/sincedb/misp"
            tags => "THREATFEED"
      }
}
filter {
      csv {
            columns => ["uuid","event_id","category","type","IOC","comment",
"to_ids","rawdate","event_info","event_member_org","event_source_org","event_dis
tribution","threatlevel","eventanalysis","date","tag"]
      separator => ","
   }
geoip {
    source => "IOC"
    }
}
```

```
output {
      elasticsearch {
      action => "index"
      hosts => "127.0.0.1:9220"
      index => "jigsaw-misp"
      }
}
```

Apache NIFI

In version 4.6 of our software we introduced a new ingest method using Apache NIFI. Apache NIFI supports a pipeline directed graph to build easily and quickly new ingest methods for virtually any data source. Apache NIFI is powerful in the fact that it can read data from websites, FTP, SCP, local directories, or other storage methods such as databases and big data platforms such as Hadoop. Using Apache NIFI novice users can continue to add new data sources to the Jigsaw Platform.

The good thing about Apache NIFI is that it can be configured for many different applications to include low latency options. The web based interface while separate from the platform is added to the platform via our tabbed interface allowing you to add sources right in the platform quickly and easily. In addition to NIFI Jigsaw Security also supports MiNiFi a subset of NIFI for those customers wanting an agent collector with a low footprint. NIFI is included in all deployments whereas MiNiFi can be added if requested by the client during the provisioning step of the deployment process.

Jigsaw Replicator

In addition to NIFI and Logstash Jigsaw Security provides a one to many service for shipping data for ingest from one system to a second or literally hundreds of connected platforms. Some customers receive data directly from Jigsaw's Cloud instance in this manner allowing us to replicate feeds such as compromised account data from our system to several customer's instances as we update our platform. This one to many configuration allows us to rapidly share data outside of MISP but makes that data available in our platform for adding additional value.

This same module which is installed but not configured requires a separate license for use if you replicate data from one of your instances to several other Jigsaw Platform installations under your control or purchased at a single organization. This system is designed to download data once and distribute to local systems to save the customer bandwidth.

This is also part of our Disaster Recovery option for those requiring a DR site to be activated ensuring data availability. This system is also compatible with US DOD and IC customers and is developed through a cooperative agreement ensuring data availability for our Government customers. This module is only available on US installed systems and may require an approval prior to activation. This module is covered under ITAR and may not be sold outside the DOD/Government.

Jigsaw Platform Installation (Partners and Integrators Only)

Jigsaw Security provides 2 ways to deploy our 4.6 platform. The following instructions are for our authorized parties that have been granted access to our Github repository or our Jigsaw Software Distribution servers. These methods are used internally for deployment of the platform.

The requirements for installation are as follows:

- A local user "platform" with sudoers access configured
- A Github account to synchronize the current source code repository
- Access to the Jigsaw Security Software Distribution Servers (for updates)
- An Ubuntu 16.04LTS server meeting the previous requirements

Installing the platform is a process that takes approximately 20 minutes. Once the installation is completed the services are edited to ensure that the required ingestion processes start and that the platform itself starts up and runs on reboot.

Login to the new Ubuntu LTS 16.04 server as "platform". SU to root and change to the root of the drive (/). Issue the command to synchronize the repository:

git clone https://github.com/jigsawsecurity/commercial

Login when prompted and the repository will copy to the local system in the /commercial directory. Change directory to /commercial/Install (case sensitive) and execute the install script (install.sh). You will be prompted to accept the Oracle Java license as well as to accept the True Type Font license during the installation that typically takes about 20 minutes. Upon finishing the installation, you will then reboot the server.

NOTE: This is for a single server installation with all software installed on a single server. To deploy the distributed Elasticsearch cluster you will need to add additional Elasticsearch nodes. See the document "How to build the ES Jigsaw Cluster" for additional information on this advanced topic.

Upon rebooting the cluster should come online and you should be able to log in to the system via a web browser by pointing your browser at the IP address of the server.

Configuration File Locations

Jigsaw Security keeps the configuration for the system in various locations. To understand the configuration options, we list out each of the configuration files below and give a description of what each file does on the system.

/etc/rc.local - This is the system startup script that starts the platform. Depending of the role of the server various lines or processes may not be needed on each node.

/opt/platform/elasticsearch/config/elasticsearch.yml - This file controls the binding of Elasticsearch to a specific interface. In normal installations, it should bind ES to localhost only and on port 9220. Direct Elasticsearch access is provided through port 35000 with authentication via NGINX (see below). Exposing Elasticsearch to the Internet will certainly cause your instance to become hacked or at a minimum cause your data to be exfiltrated. We do not support any bindings other than to localhost as this would have negative security implications.

/opt/platform/config/kibi.yml - This file tells the system what port Kibi (a port of Kibana) should listen on. We utilize Kibi to provide our tabbed interface since it's open source but it should be noted that we do not use the siren-join plugin and the use of this plugin will break our system if used because of our analytics (see later note). We only support binding Kibi to localhost for the same reasons as mentioned about for Elasticsearch. Note that Kibi is being phased out in the next version as our newest analytics will not work correctly with our existing use of this Third Party open source product.

/etc/nginx/sites-enabled/default - This file provides the configuration for authentication. We do not protect record levels in the data unless you ingest data into indexes with UUID's enabled. The password file for providing logins to the system is in /etc/nginx/conf.d/platform.htaccess and is maintained with the apache utility htpasswd.

To remove users from the system you can edit the platform.htaccess file and remove the users line allowing their specific login. To add a new user, you need to execute the following command:

```
htpasswd /etc/nginx/conf.d/platform.htaccess {username to add}
```

When you execute the command, you will need to enter the password for the new user.

Record Level Security Module

Jigsaw Security provides 2 levels of security one that is included with our product and the option for customers to purchase Elasticsearch Shield should they wish to go that route.

Our built-in solution supports 3 authentication methods and enforces SSL encryption as well as REST protection so that even if you incorrectly expose your Elasticsearch instance that system will still protect your data. The methods of supported authentication are LDAP, Active Directory, and local authentication. The security module is included in our offering at no additional charge whereas there is an additional charge for Elastic's Shield product.

Features of the Jigsaw Security Modules:

- Authentication via LDAP, Active Directory, or Local Authentication
- Index, Types, and Field record level security
- Document and Field level security auditing
- Complete REST security and transport layer through SSL
- Node Level Security – Only allows trusted nodes to join the cluster
- OpenSSL for improved performance
- Wildcard Filtering and Index Aliases

The configuration of this module is done by command line and typically is setup at the time of installation and should not be modified by the customer. The security module supports Kibana, Logstash and Beats natively.

Platform Monitoring System

Jigsaw Security provides a monitoring Interface that is clustered allowing each node in the cluster to check on every other node to ensure that the nodes configured services are available and operating. In the event of a failure or if a process that is monitored crashes or dies the system (any node in the system) can send a notification via SMS, Pager or Email to the administrators indicating that there is a problem.

Here is a list of items monitored in a typical configuration:

- CPU Utilization
- Drive Space Utilization
- Memory Utilization
- System Ping Response Times
- Local or Remote Service Response – Is the service port active
- File or Process Change – Upgrades or Editing of Files
- Disk Space Consumption Rates
- Free Memory or Allocated Memory

- Firewall Status
- LDAP or AD availability for Platform Authentication
- Load Average Monitoring
- Network Interface Status
- RAID Device Status
- Remote Service HTTP, FTP, Mail, etc checking
- Remote Ping
- SSH or SSL access to the server
- Elasticsearch Status – Online and Joined to Cluster
- Mail Server Status
- Monitoring System Status

Platform Features (A Discussion on X-Pack)

Jigsaw Security is often asked about X-Pack the add on available from Elastic directly. While we support the deployment of X-Pack there is no need for X-Pack on a fully deployed system as our own product provides the same features. Below is a list of all the features provided by X-Pack and what modules in our platform are responsible for each of these feature sets.

Security: The Jigsaw Security Module now provides Security in your cluster. This module provides record level security the same as Elastic's Shield yet is included at no additional cost. In addition, we have an additional feature called the star feature that will black out patterns of information that are sensitive if needed such as PHI and PII tagged data. In Shield the product doesn't return any information indicating that there was additional data so you never know what information we denied by the Shield plugin.

Alerting and Monitoring: There are several methods for alerting in our platform. The first is record keyword match alerts and time series alerts whereas a certain number of events or conditions occur in a period or if a single keyword matches in data you can generate an alert for those conditions as well. In addition to data monitoring we have a full platform monitoring capability that is built in to monitor when alert when any component of the system fails to respond or when performance issues are noted. An additional analytic that is included known as Matchstick provides IOC to log file or data matching and creates alerts in a new index for showing threats in our cyber security edition.

Reporting: The Matchstick analytic as well as an hourly report can be configured using our version of Watcher.

Graph: We support Graph in our IOC repository. It will show relationships between threats and IOC data with other events. It is not the same traditional graph database provided by Elastic. A full-blown implementation of Graph will be released with version 5.

Matchstick Analytics

Jigsaw Security provides an analytic product the takes IOC data from our IOC repository and then searches in other indexes to find matching content. This analytic is included in the Cyber Security Edition of the product but is not included in the stand alone VM we ship for testing.

Data Management – IOC Repository and Index Management through KOPF

Jigsaw Security provides the KOPF utility to manage indexes in our Elasticsearch offering. This plugin allows you to delete old indexes that you no longer need. In addition, it is used to create index pattern mappings and to see the health of the cluster (in addition to other monitoring). This plugin is included in the platform web interface.

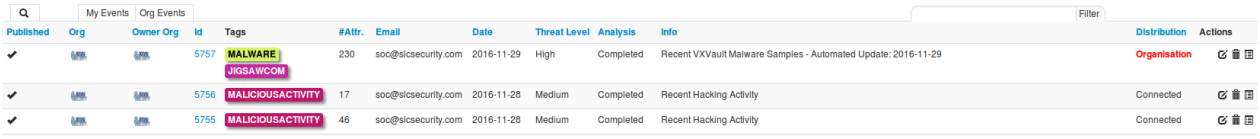
IOC Management – Malware Information Sharing Platform

Jigsaw Security is a user and integrator of the Malware Information Sharing Platform. This system is included in our data solution and allows users to tag data, export and import data and to share information with Jigsaw and our other customers. This is an open source solution and one option for storing this type of information. The following section talks about how we ingest, support and how customers can use this resource to find threats in their environments.

Customers have the option of having MISP installed locally on one of their nodes or can use our Cloud instance. Using our cloud instance is the recommended method as we simply provide the IOC data to your Elasticsearch instance in the form of a feed and then it functions as if the instance were local to you. In some cases, customers, may wish to use this data in unconnected network in which case other methods must be used to keep the IOC information up to date. A landing zone option where a server is never connected to the Internet and your network at the same it is one possible solution for networks that are physically separated from the Internet.

IOC data is pulled from the Jigsaw Security Enterprise MISP server hourly and ingested into each customers Elasticsearch instance. Jigsaw and our partners, customers and contributors share threat details through events. These events show up in the platform as people report these issues to Jigsaws Cloud instance.

Events in MISP



As events are created they are then distributed in near real time to all subscribers of Jigsaw, the MISP network through our connections to CIRCL and Government users of our software. End users can tag events however they see fit and using API calls you can import and export data in any manner you need to while working an incident. For example, if you want to perform a malware search in your forensics software and you want to export data of interest you can select categories such as "Virus", "Malware", "Ransomware", etc through a single API call and import the results directly into Encase, Paraben or a similar forensics software application in which you are conducting your investigation.

You can also pull all data and exclude specific categories such as "Unconfirmed" events as an example. Below is an example of a few API request using the API and wget a common web retrieval utility. You can also use curl or even a web browser to make your request.

Automation functionality is designed to automatically generate signatures for intrusion detection systems. To enable signature generation for a given attribute, Signature field of this attribute must be set to Yes. Note that not all attribute types are applicable for signature generation, currently we only support NIDS signature generation for IP, domains, host names, user agents etc., and hash list generation for MD5/SHA1 values of file artifacts. Support for more attribute types is planned. To make this functionality available for automated tools, your authentication key is used. This makes it easier for your tools to access the data without further form-based-authentication.

Since version 2.2 the usage of the authentication key in the url is deprecated. Instead, pass the auth key in an Authorization header in the request. The legacy option of having the auth key in the url is temporarily still supported but not recommended.

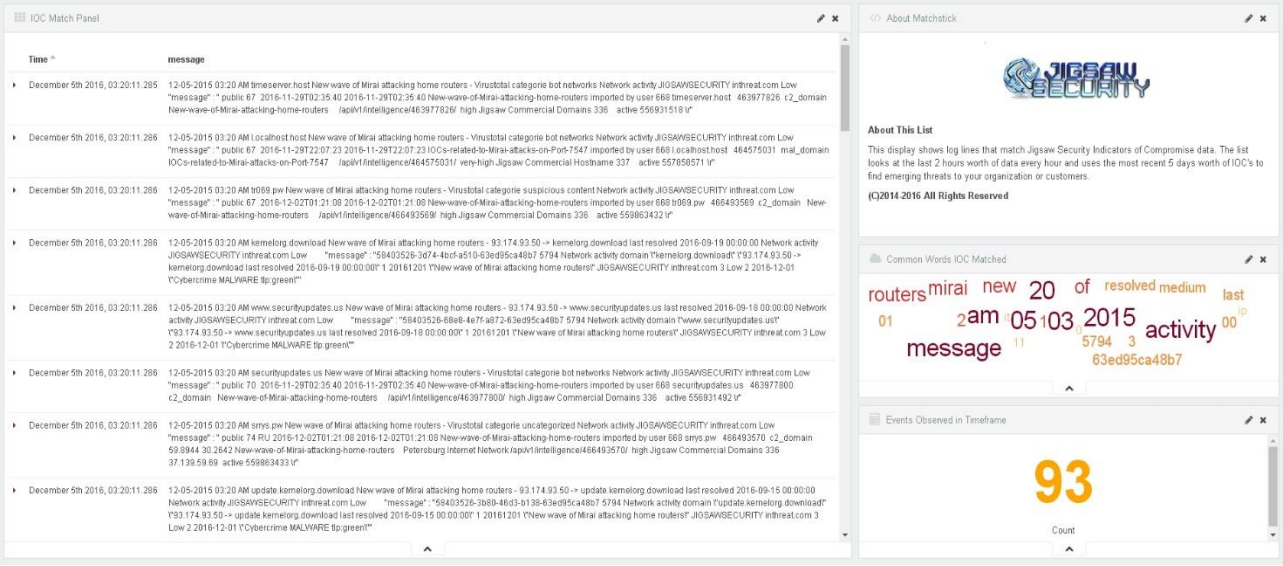
Please use the use the following header:
Authorization: Fb3xhI7MFJOfrZ9kdvvIQwFqh6XUQ79P8cnqUucA

In your request, you must pass a valid API key in the request as indicated above. Please note that this API key is for illustration purposes only and is not valid for use. To obtain a valid API key you can log in to the Jigsaw Security MISP server and select "Global Actions", "My Profile". Your API key will display and you can copy it into your web base utility. Here are some examples of request you may use.

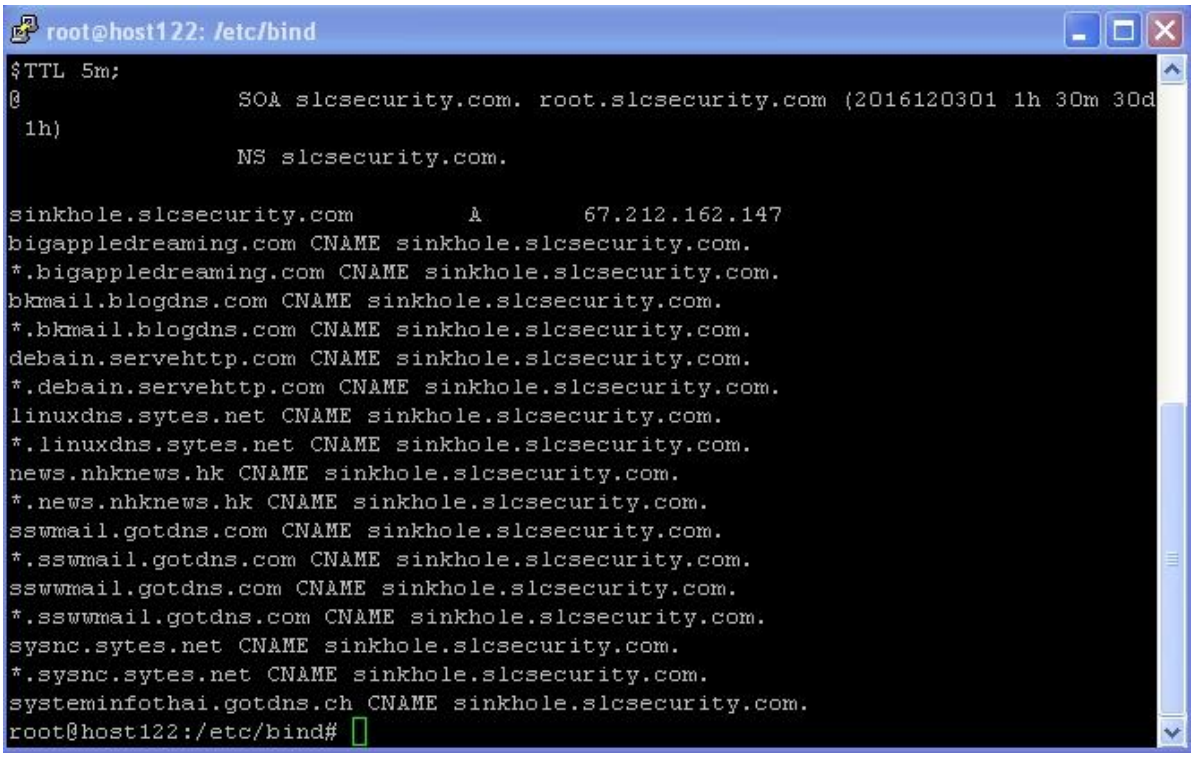
A walkthrough of the Jigsaw Analytics Platform

In order to understand the Jigsaw Analytics Platform features it is best to show you the interface and to describe each of the screens typically (but not always deployed) in our platform.

Matchstick and DNS Sinkhole Alerting



Matchstick Analytic Module: This module runs hourly and matches threat data ingested into the MISP IOC repository and then searches all of the indexes in the Jigsaw platform for items that match the IOC data. This IOC data can be turned on and turned off in the IOC repository using the "For IDS" flag. This same flag controls whether or not the IOC's are exported to your DNS servers for protecting against malware with the Response Policy Zone's generated by the platform. In our typical configuration the IOC data is sent to DNS servers deployed on your network to drop known malware C2 addresses, ads or other categories of data in the environment. When a client such as a workstation request the malware domain the DNS servers reply with a forged record sending the client to a notification window indicating that the domain has malware, logs the attempt and then the Matchstick analytic will detect that request allowing you to clean workstations on your local network. See the notice screen below.



An automated DNS RPZ file – Blocks malware on your local networks

The DNS records above are generated by the Jigsaw Analytics Platform and ensure a higher level of security for your connected workstations and clients.

In the next screen you can see a typical sinkhole response page. When traffic is sinkholed it is an indication that the workstation may be infected with malware. In that case you would want to have your IT team clean the infection.

THE WEBSITE YOU WERE TRYING TO ACCESS HAS BEEN REDIRECTED TO PROTECT YOU FROM A MALWARE OR VIRUS THREAT

You have been redirected to this page to protect you from a virus or malware infection.
If you believe you are receiving this notice in error please contact Jigsaw Security by email (soc@jigsaw-security.com).

Sales and Support 800-447-2150 Ext. 1

Example Screenshot of a Sinkhole Notification – Can be customized in your environment

As you can see using the platform with known bad malware and sites makes it easy to keep a blocklist enforced in your local networks. This is one of the nicest automation features that actually protects your users from malware infections and alerts your IT staff to computers that are infected. The only thing required to make this work is to set your DNS servers to pull the RPZ file from the Jigsaw Cloud Platform (hosted by Jigsaw Security). You can then use the online cloud repository to search threats and find out why a particular site is being blocked or to unblock the site on your network if needed.

Each customer has complete control over what gets blocked on the local client network or networks.

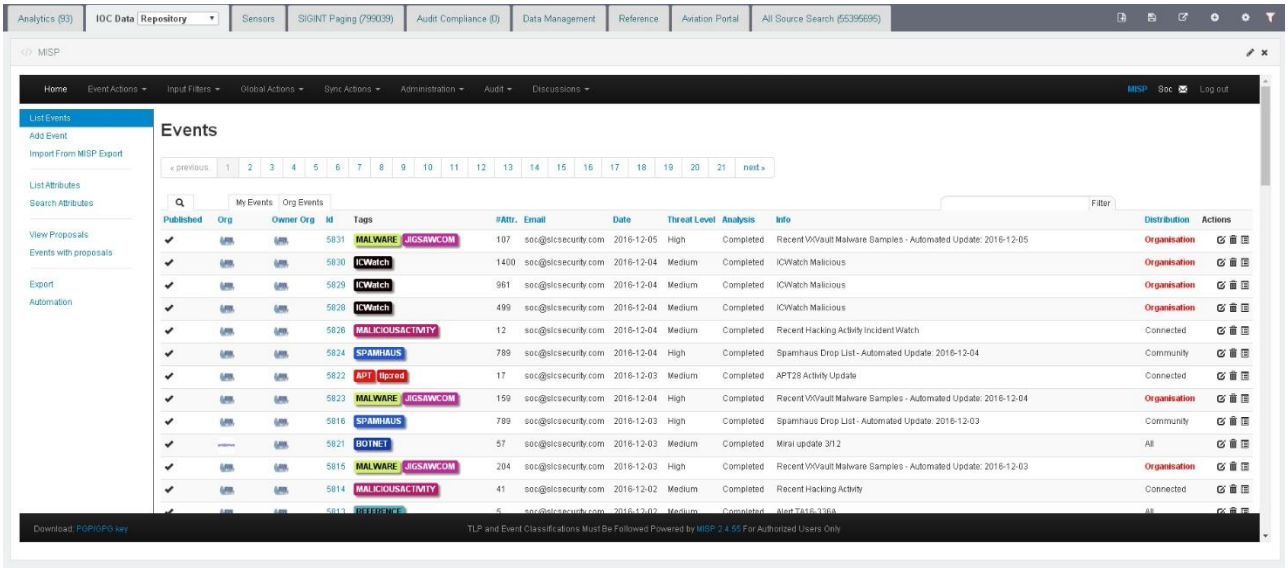
Matchstick and Log File Detection

When a log file is written to the Jigsaw Analytics Platform that is the beginning of processing for that log file. Most products save logs and analyst have to search for bad entries. When you maintain your IOC's or use the Jigsaw Threat Feed you don't need to manually search for threats. The Jigsaw Analytics Platform Matchstick analytic runs IOC data against ingested logs and then outputs matches to the Matchstick analytic panel in the platform (previous page). This allows you to see when an IOC is observed in your environment. If something is triggering false positives you can simply edit the "To IDS" flag and turn off the indicator and it won't trigger in the analytics in the future, will allow access from local networks and will not alerting in any other security devices that utilize the Jigsaw Threat Intelligence.

Product Support:

Jigsaw Analytics Platform works with many firewalls, IDS and IPS products, Host Intrusion Systems and of course DNS. In many cases if you have a SIEM already deployed we can ingest data from your SIEM logs for automatic matching. In many cases we can support virtually any product you already have deployed. We provide integration not a replacement and empower your tools to report into a central management interface for monitoring and management.

IOC Repository

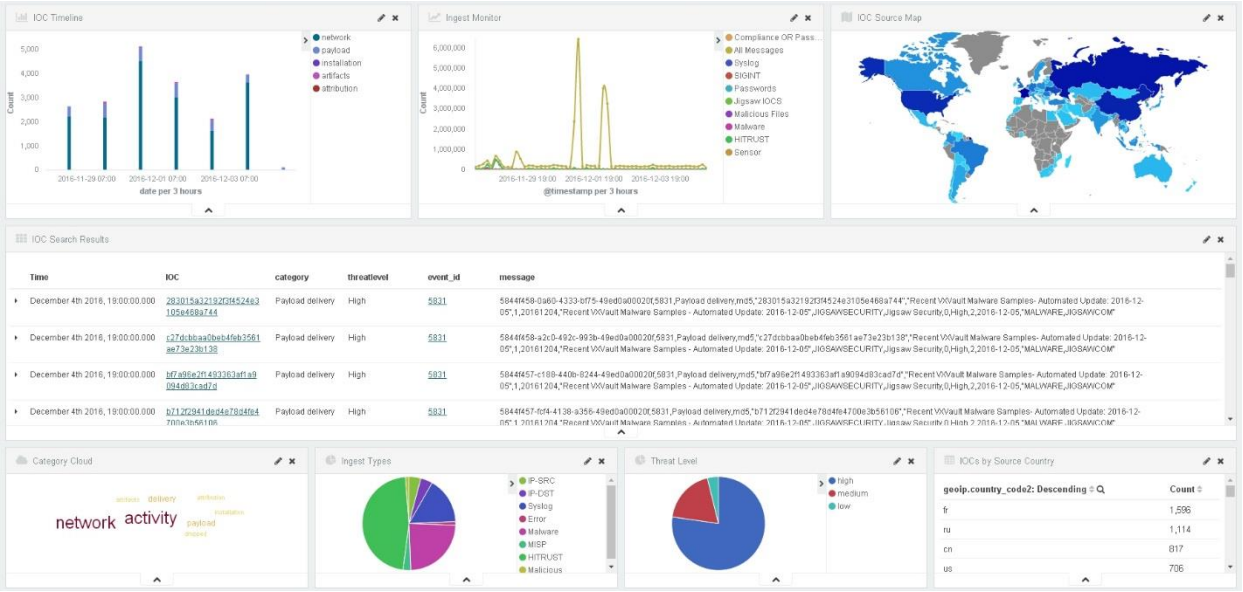


One of the main reasons to use the Jigsaw Platform is to be able to actually make use of threat intelligence data. Many of the products on the market provide methods for searching through IOC data and semi-automated solutions but the Jigsaw Platform is a complete end to end monitoring solution. Regardless of format the Matchstick analytic platform will search through structured and unstructured data ingested into the platform and will alert to matching messages in the system.

Not having a defined schema allows our products to work with any product that can output logs. In fact our system will allow any system that supports syslog to write data directly into the Jigsaw Platform for inspection.

IOC Pattern Monitoring

The Jigsaw Platform provides screens for monitoring ingested IOC data to see the threat levels and risk associated by country, IP block, ASN and other parameters. You can view where threats are coming from and see instantly in the platform what threats are attacking your network infrastructure or other security systems such as door access controls, time reporting, workstation brute force attempts and virtually anything can match and report on patterns occurring in your log file data.

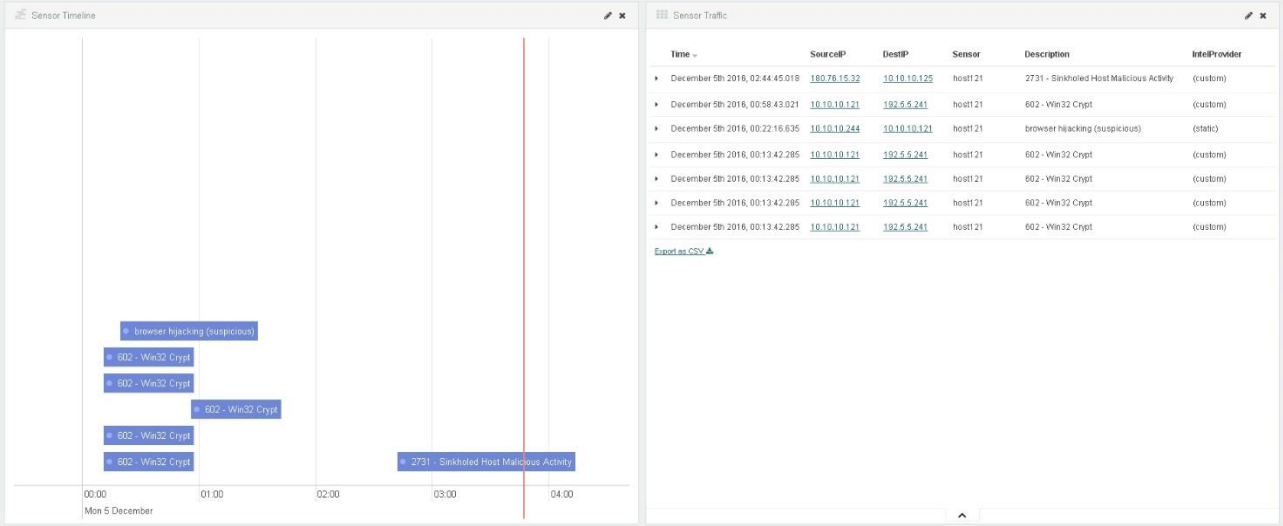


Monitoring the Source and Types of Threats

The Jigsaw Platform provides management dashboards to show the types of threats that are attacking your networks in near real time. This allows you to see things like SMTP brute force attacks, spam campaigns and similar events, DDOS attacks, what sources are the greatest threat and the type of threats being reported by Jigsaw Security customers and users of our Threat Intelligence Feeds.

In addition you can look at individual sensors in the platform and see what signatures are triggering. Keep in mind that Jigsaw Security utilizes time series so we can detect items that are not signature based but are actions that are occurring on your networks.

Time series is included and you can create alerting parameters when there are certain numbers of events or when a particular event that never occurred before is seen for the first time. So remember we detect both signature and non-signature events.



Timelines Events

In the screenshot above you can see events on the timeline as well as anomolies that have not been previously observed.

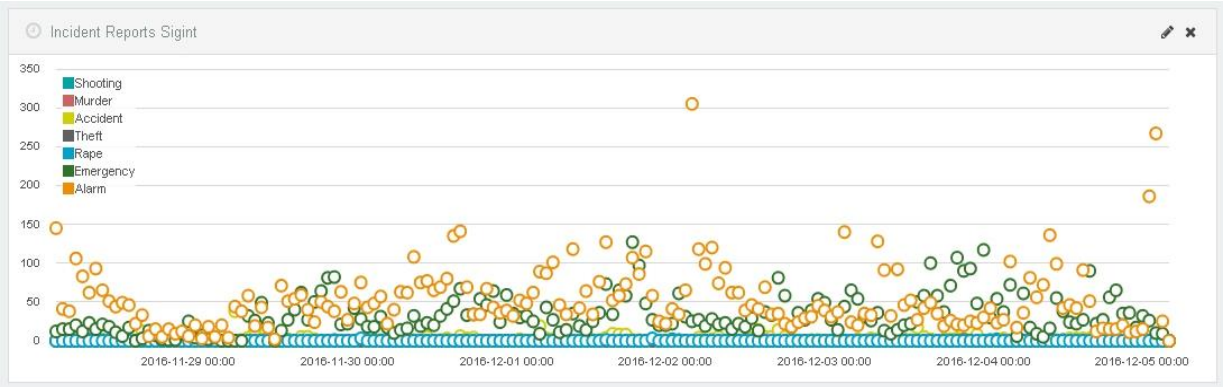
Jigsaw Sensor – A Maltrail Port

The Jigsaw Sensor is automatically updated from the IOC repository and can be deployed to remote networks that may not have the same protections as your corporate network. This sensor product allows a central security team to manage multiple customers, locations and networks regardless of location while ingesting the data into the platform to see what threats are occurring at your customers sites or at remote locations you may manage.

MHN (Modern Honeypot Network) - Integration

One of the features we really like is to utilize honeypot sensors to see who is attempting to break through your border network defenses. Our product works with any honeypot products that have been developed through unstructured data or ingestion of logs into the platform. We can work with any honeypot sensors that output plain text logs.

Modern Honeypot Network – A view of our platform integration with MHN



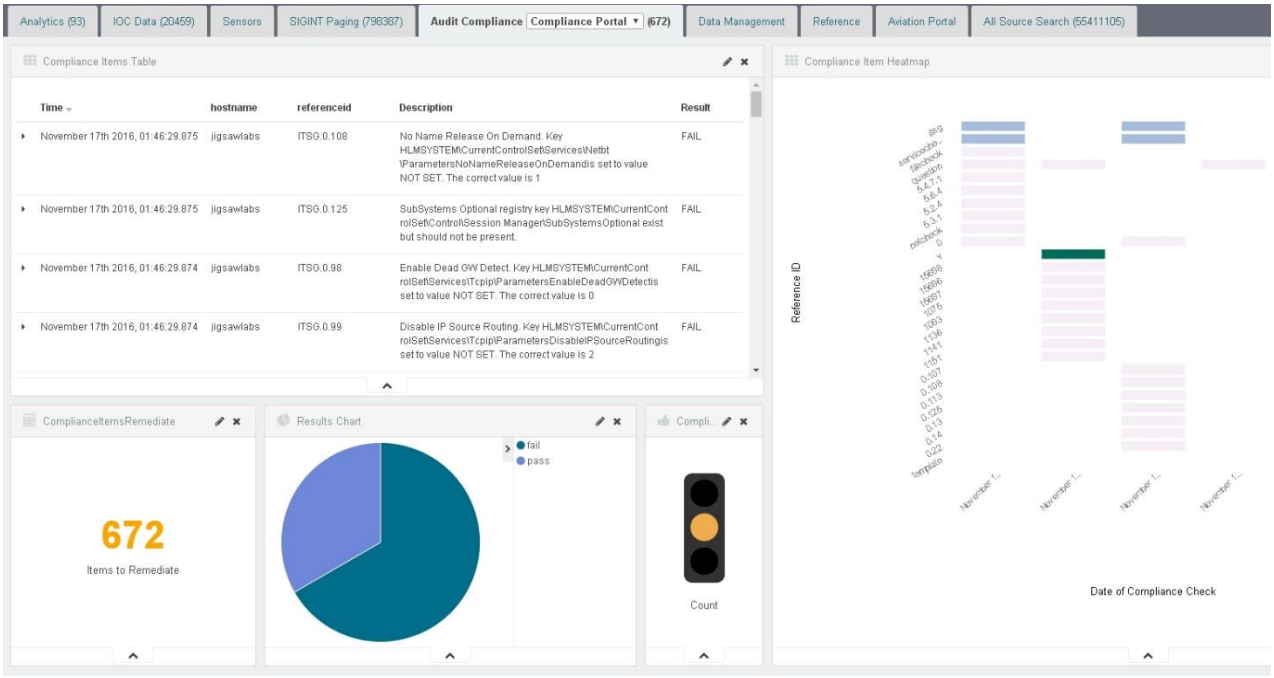
Event and Keyword Timeline

The Jigsaw Security solution provides the ability to parse any data source and log event data. In the example above we are monitoring police and medical dispatch data to see when events are occurring locally that may effect availability of law enforcement or medical personnel. Just because we are a cyber security company does not mean that our analytics can't be purposed for any use case you could come up with.

Jigsaw Workstation and Server Compliance Module

The Jigsaw Security Workstation and Server Compliance module ensures that your workstations are always at a certain compliance level. With templates for ITSG, STIG, HIPPA, PCI, PII and other data restrictions the product instantly tells management the compliance level of all systems, administrators (through the use of automated questioning during server or workstation setup) and processes by requiring management to answer policy questions that need to report reported in auditing. The system generates deviation documents allowing you to effectively document any changes that do not conform

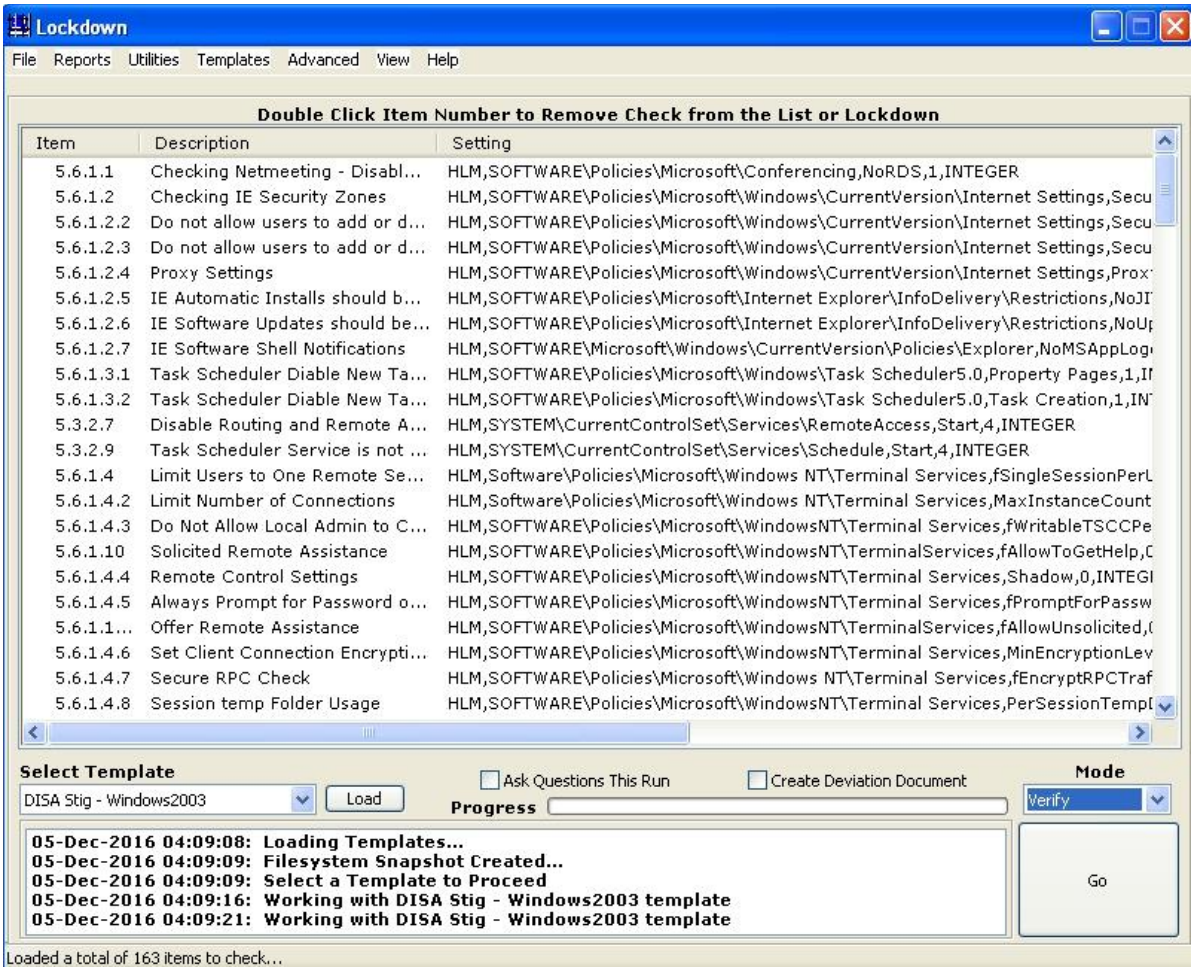
to auditing requirements and generate the paperwork needed to certify to the auditor the reasons why a company has deviated from the compliance standards.



A look at the Jigsaw Compliance Portal

Jigsaw Compliance Login Module

One of the best ways to ensure compliance is to run the auditing script during login to the network. During login the registry, Group Policy Objects and file permissions are checked against the policy daily giving you a view of your compliance teams progress while working toward upcoming audits.

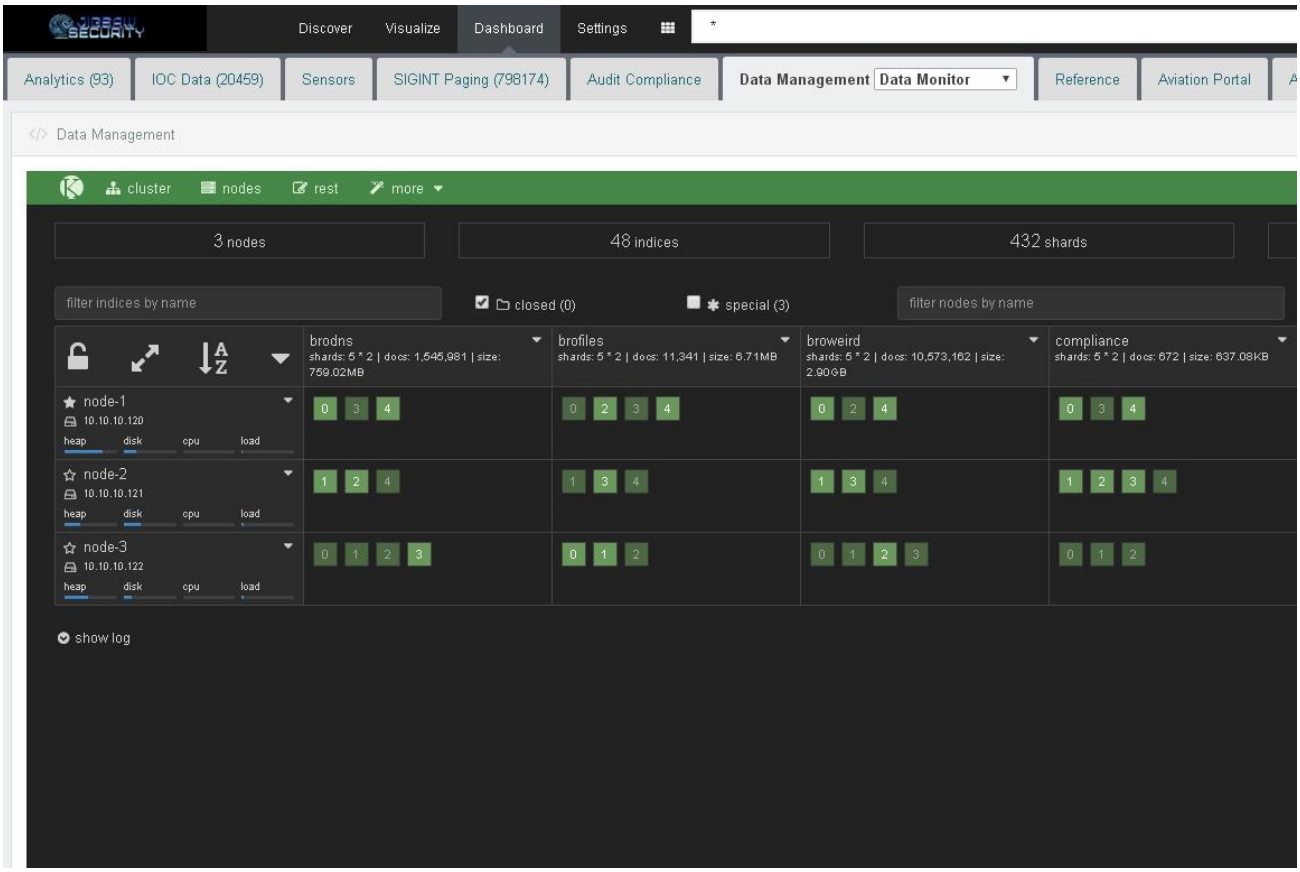


Jigsaw Auditing Lockdown Program

In addition we have a complete auditing framework (pictured above) to allow administrators to lockdown systems in an automated fashion, and ensure all compliance items and requirements are set properly on workstations and servers.

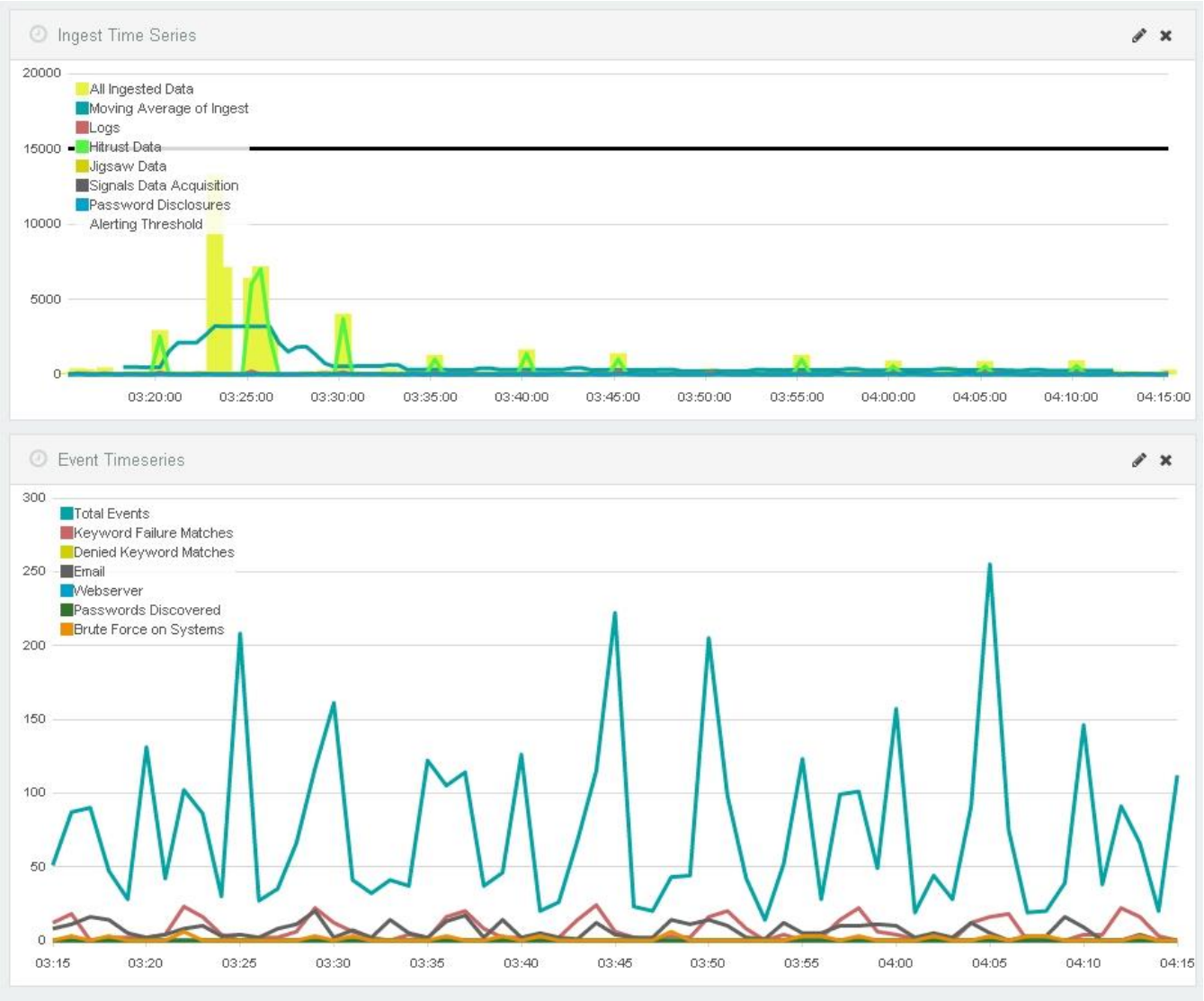
Management Tools

In addition the platform provides index management for administrators to maintain the system. The utilities provide an easy interface for administrators to manage data and to ensure the system is functioning properly. Here are some of the utilities includes in the platform.



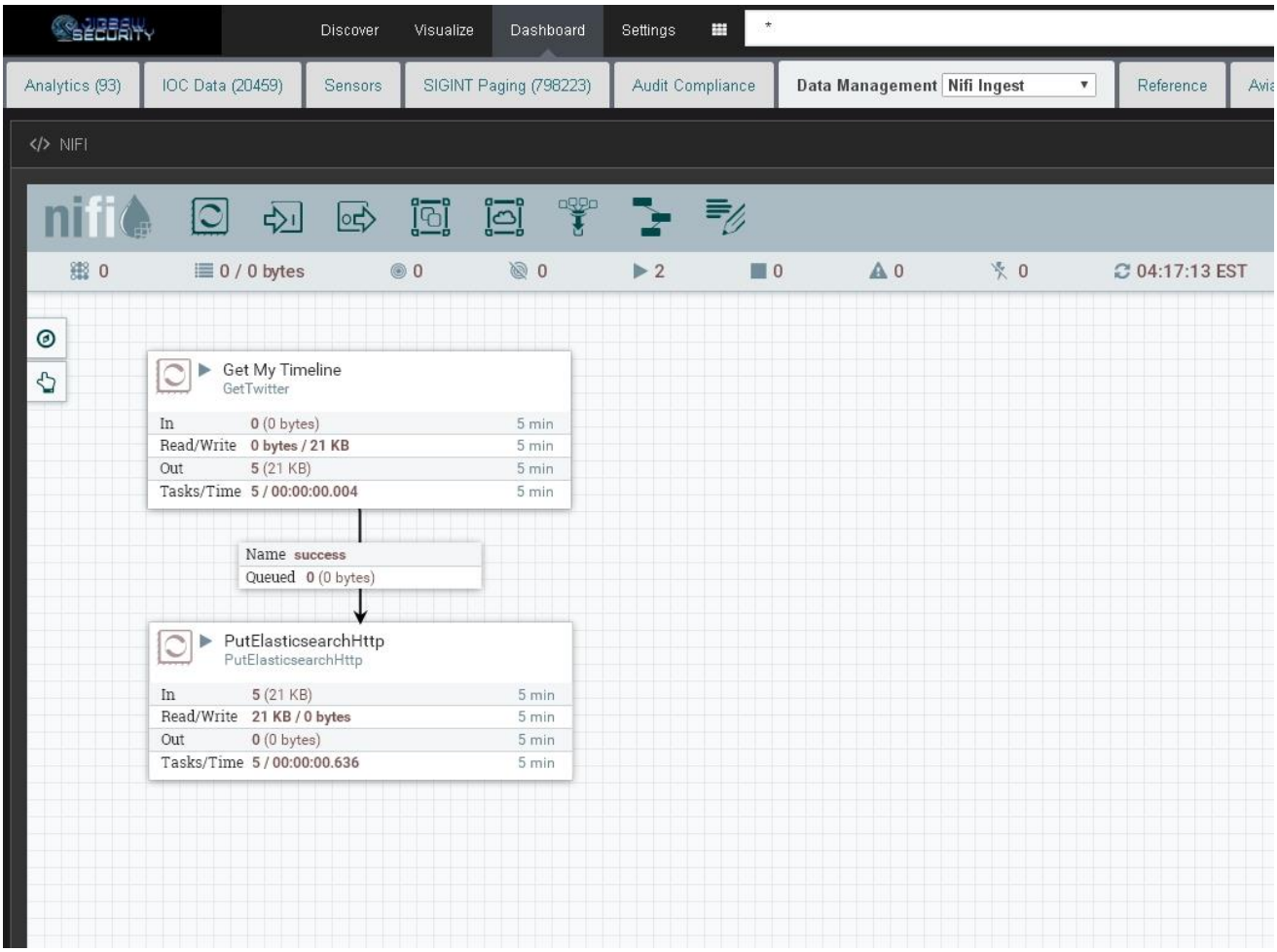
Index Management

Using the index management utility you can delete data no longer needed, create new data collections and archive older data that you wish to keep but store offline for archival purposes but no longer need to access for your day to day operations. Data is easily restored to an active state as needed.



Ingestion Monitoring Utility

The platform allows users and administrators to monitor data being written into the platform. Because we utilize Nifi and Logstash we can easily add new data sources to the platform in either structured or unstructured formats.

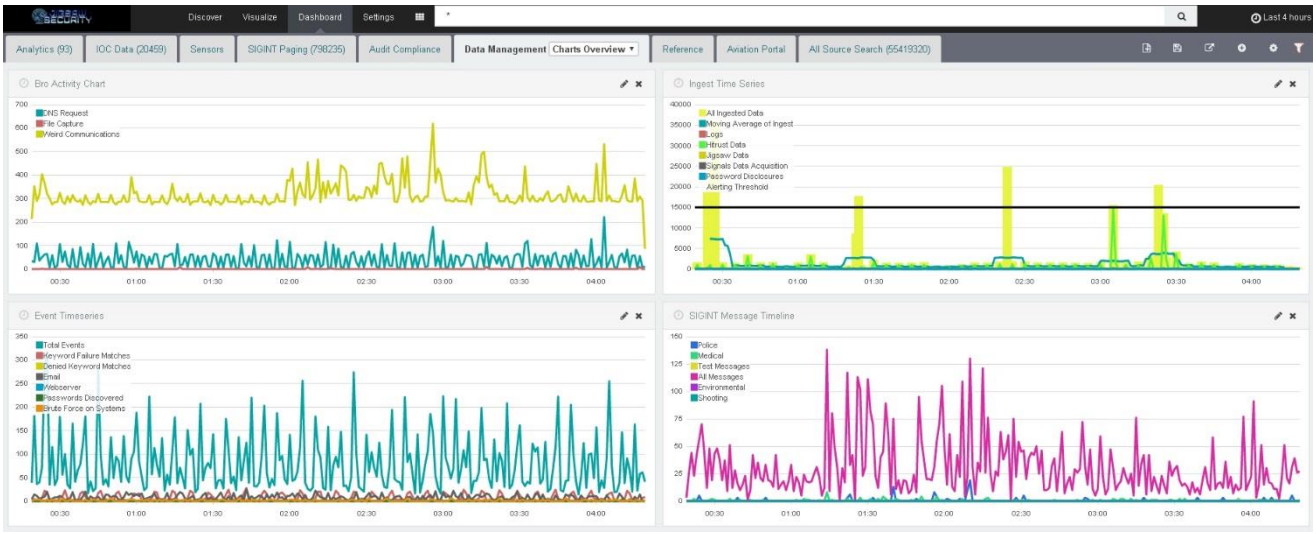


Apache Nifi Integration

Easily add new ingest pipelines using Apache Nifi. The utility allows you to virtually ingest any format of data and write the data to Elasticsearch right in a web based interface.

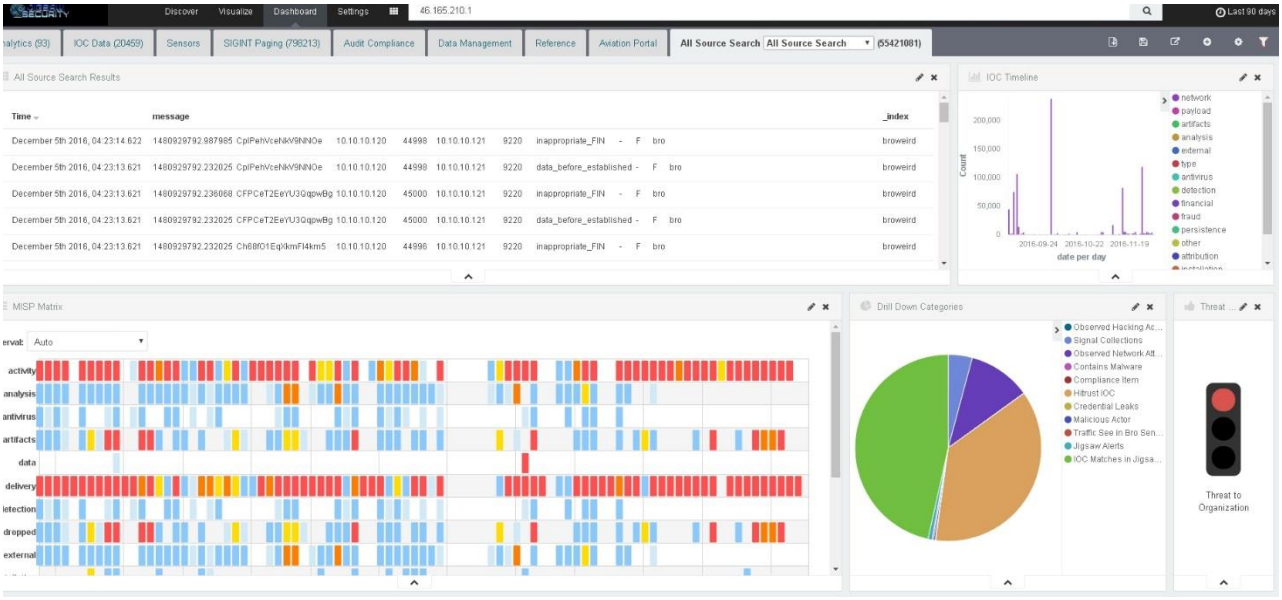
Time Series Applications

You can utilize the Jigsaw Platform to create time series of data. You can also alert on keyword and time series with the Watcher utility.



Searching for IOC data and reference information

The platform provides a master search feature that will look in all indexes and data sets and report back exactly where data is being seen in indexes. This will tell you if the IOC is present in logs, packet captures, IDS systems, etc. and how often the IOC is being seen. See the screenshot below as an example.



About Visualizations and Platform Training

Customers can create whatever visualizations they wish as well as reporting and similar output in the platform. Not all customers have the same use cases or data sets, products or information stored in their systems. For this reason we provide a serious of examples and then we provide 40 hours of

consultation to get everything setup and usually provide training so that customers can use and support the platform.

Each system is different from a visualization stance but the underlying technologies we use are the same throughout our customer based allowing use to provide tiered support under support contracts if needed. The customer can purchase a block of support hours or we can provide on site resource consulting if needed for complex integrations.

About the Jigsaw Honeypot Network

As of September 2016 Jigsaw Security has deployed over 280 honeypots in Government, Telecom, Retail, Healthcare and other verticals. This network provides threat intelligence that we can correlate and then ship to customer IOC repositories to help protect them from attackers. We have sensors in over 40 countries and in many top tier networks. Our threat feed quality is greater than our competition with less false positives because we harvest this data and then compare to what other customers are reporting. In many cases we have IOC's days or weeks before our competition due to our large deployment of detection technologies. We utilize over 20 Honeypot products to gather indicators, binaries and activity reports and protect you based on what we are seeing in other parts of the world and through pattern recognition.

By subscribing to the Jigsaw Threat Intelligence product you gain the benefit of receiving our high quality observations generated from our honeypot networks.