411: A Framework for Managing Security Alerts

Kai Zhong @sixhundredns
Ken Lee @kennysan
411: A Framework for Managing Security Alerts

Kai Zhong @sixhundredns
Ken Lee @kennysan

OPEN SOURCE!
Who Are We?
Kai Zhong

Product Security Engineer @ Etsy

I wear many hats

Twitter: @sixhundredns
Ken Lee
Senior Product Security Engineer @ Etsy
Spoke at Defcon 21 about Content Security Policy
Loves funny cat gifs
Twitter: @Kennysan
What is Etsy?
What Are We Covering?
History
The Problem(s)
Our Solution
Alert Management @ Etsy
More Examples
But First, Some Terminology
The ELK Stack

elastic + logstash + kibana
Logstash

Data processor and log shipper
Logstash

Data processor and log shipper

Allows you to break out your log data into separate fields
Logstash

Data processor and log shipper

Allows you to break out your log data into separate fields

We use it to ship logs into Elasticsearch!
Elasticsearch

Distributed, real-time search engine
Elasticsearch

Distributed, real-time search engine

Allows storing complex, nested documents
Elasticsearch

Distributed, real-time search engine

Allows storing complex, nested documents

Allows generating statistics over your data
Elasticsearch

Distributed, real-time search engine

Allows storing complex, nested documents

Allows generating statistics over your data

We use it for analyzing logs!
Kibana

Data visualization frontend for Elasticsearch
Kibana

Data visualization frontend for Elasticsearch

Log discovery
Kibana

Data visualization frontend for Elasticsearch

Log discovery

Visualizations!
Switching to ELK

Work started in mid 2014
Switching to ELK

Work started in mid 2014

Finished in mid 2015
Switching to ELK

Work started in mid 2014

Finished in mid 2015

We learned a lot from the migration
Switching to ELK

Work started in mid 2014

Finished in mid 2015

We learned a lot from the migration

And got a bunch of great tools out of it
It Was A Bumpy Road

Hiccups are expected when moving to a new technology
It Was A Bumpy Road

Hiccups are expected when moving to a new technology

Had to deal with annoying, performance-impacting bugs
It Was A Bumpy Road

Hiccups are expected when moving to a new technology

Had to deal with annoying, performance-impacting bugs

Security was concerned about the usability of ELK
It Was A Bumpy Road

Hiccups are expected when moving to a new technology

Had to deal with annoying, performance-impacting bugs

Security was concerned about the usability of ELK

ELK didn’t have functionality to help us monitor attacks in real time
Samsung Acknowledges the SSD 840 EVO Read Performance Bug - Fix Is on the Way

by Kristian Vatto on September 18, 2014 3:23 PM EST

New Samsung SSD 840 EVO Read Performance Fix Coming Later This Month

by Kristian Vatto on April 14, 2015 7:40 PM EST
We have some emergency ELK downtime coming in a few minutes.
It seems we've run into a new kernel bug with NFS mounts, which is causing backups to fail, and causing elasticsearch to behave badly :-(

We're going to try and keep this as fast as possible and hopefully we'll be back up and also caught up on replication in a few hours.
Struggle Bus Coffee Mug | Funny Mug Gift
shopHelloGinger
$16.00
The Problem(s)
Search scheduling?

Reactive Security Mechanisms

Reactive security mechanisms usually consist of real-time event monitoring and alerting. These security mechanisms focus on events that trigger immediate responses based on regular information querying: they query the same data and they query it often.

Some examples of reactive security mechanisms at Etsy are automated Splunk searches and anomaly detection based on StatsD/Graphite logs.
No Search Scheduling

Security heavily relied on Splunk scheduled searches for alerting
No Search Scheduling

Security heavily relied on Splunk scheduled searches for alerting

No equivalent for ES at the time
No Search Scheduling

Security heavily relied on Splunk scheduled searches for alerting

No equivalent for ES at the time

No web UI for managing searches
An Unfamiliar Query Language

Our alerts were complex SPL (Splunk Processing Language) queries
An Unfamiliar Query Language

Our alerts were complex SPL (Splunk Processing Language) queries.

ES’s query language is less robust.
An Unfamiliar Query Language

Our alerts were complex SPL (Splunk Processing Language) queries

ES’s query language is less robust

Some things were non-obvious coming from SPL
The Road to ELK Integration
The Road to ELK Integration

We needed a query language for building complex queries without code
The Road to ELK Integration

We needed a query language for building complex queries without code

We needed a mechanism to run and manage these queries
The Road to ELK Integration

We needed a query language for building complex queries without code.

We needed a mechanism to run and manage these queries.

Preferably before we turned off Splunk ; )
ESQuery
Features

Superset of the standard Lucene syntax
Features

Superset of the standard Lucene syntax

Syntactically similar to SPL!
Features

Superset of the standard Lucene syntax

Syntactically similar to SPL!

Supports all the functionality we need!!!
<table>
<thead>
<tr>
<th>Command</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inline params</td>
<td>$size:20 $sort:user_id $fields:[a,b,c]</td>
</tr>
<tr>
<td>Joins</td>
<td>*</td>
</tr>
<tr>
<td>Aggregations</td>
<td>*</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Variable substitution</td>
<td>src_ip:@internal_ips</td>
</tr>
</tbody>
</table>
source="/data/syslog/current/web/info.log" log_namespace="login"
reason="wrong password" response=403 | top 10 remote_host
type:web_info_log log_namespace:login

logdata.reason:"wrong password" -response:403 |

agg/terms field:logdata.remote_host size:10
splogTASH  SPL to lucene translator

source="/data/syslog/current/web/info.log" "Response to reCAPTCHA" status="incorrect" | transaction ip | where eventcount > 250

Go

type:web_info_log AND "Response to reCAPTCHA" status:"incorrect" | agg:terms field:ip min_doc_count: 250

ENTER SPLUNK QUERY. CLICK GO. TEST QUERY ON KIBANA.
Alert Management

Write queries to be automatically executed
Alert Management

Write queries to be automatically executed

Receive email alerts whenever there are results
Alert Management

Write queries to be automatically executed

Receive email alerts whenever there are results

Manage alerts through the web interface
Scheduling
Under the Hood

Search Job

Search
Alerts

Filters

Targets
Under the Hood

Scheduler

Search Jobs

Workers
Stats

242 Alerts are active (242 New, 0 In Progress)

242 of them are high priority
0 of them are medium priority
0 of them are low priority
0 of them are stale

Alerts in the last 20 days
Stats

242 Alerts are active (242 New, 0 In Progress)

- 242 of them are high priority
- 0 of them are medium priority
- 0 of them are low priority
- 0 of them are stale

Alerts in the last 20 days
242 Alerts are active (242 New, 0 In Progress)

- 242 of them are high priority
- 0 of them are medium priority
- 0 of them are low priority
- 0 of them are stale

Alerts in the last 20 days
Managing queries
<table>
<thead>
<tr>
<th>Name</th>
<th>Category</th>
<th>Tags</th>
<th>Type</th>
<th>Priority</th>
<th>Health</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appsec</td>
<td></td>
<td></td>
<td>Logstash</td>
<td>Medium</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Appsec</td>
<td></td>
<td></td>
<td>Logstash</td>
<td>High</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Appsec</td>
<td></td>
<td>api, hardc1ty</td>
<td>Logstash</td>
<td>High</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Risk</td>
<td></td>
<td>recaptcha signature</td>
<td>Logstash</td>
<td>Low</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Appsec</td>
<td></td>
<td>signature</td>
<td>Logstash</td>
<td>Low</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Appsec</td>
<td></td>
<td>login</td>
<td>Graphite</td>
<td>Low</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Risk</td>
<td></td>
<td>API Follow</td>
<td>Logstash</td>
<td>High</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Appsec</td>
<td></td>
<td>APIv3</td>
<td>Logstash</td>
<td>High</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Appsec</td>
<td></td>
<td>authservice</td>
<td>Logstash</td>
<td>High</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Netsec</td>
<td></td>
<td>authservice</td>
<td>Logstash</td>
<td>High</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Netsec</td>
<td></td>
<td>authservice</td>
<td>Logstash</td>
<td>High</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Appsec</td>
<td></td>
<td>authservice</td>
<td>Logstash</td>
<td>High</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Appsec</td>
<td></td>
<td>authservice</td>
<td>Logstash</td>
<td>High</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Appsec</td>
<td></td>
<td>authservice</td>
<td>Logstash</td>
<td>High</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Appsec</td>
<td></td>
<td>bugbounty 806</td>
<td>Logstash</td>
<td>High</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Category</td>
<td>Tags</td>
<td>Type</td>
<td>Priority</td>
<td>Health</td>
<td>Enabled</td>
</tr>
<tr>
<td>---------------</td>
<td>----------------</td>
<td>--------------</td>
<td>--------------</td>
<td>----------</td>
<td>--------</td>
<td>---------</td>
</tr>
<tr>
<td>Appsec</td>
<td></td>
<td></td>
<td>Logstash</td>
<td>Medium</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Appsec</td>
<td></td>
<td></td>
<td>Logstash</td>
<td>High</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Appsec</td>
<td>api</td>
<td>hardship</td>
<td>Logstash</td>
<td>High</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Appsec</td>
<td></td>
<td></td>
<td>Logstash</td>
<td>High</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Risk</td>
<td>Reception</td>
<td>signature</td>
<td>Logstash</td>
<td>Low</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Risk</td>
<td></td>
<td>signature</td>
<td>Logstash</td>
<td>Low</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Appsec</td>
<td></td>
<td>login</td>
<td>Graphite</td>
<td>Low</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Appsec</td>
<td>API</td>
<td>Follow</td>
<td>Logstash</td>
<td>High</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Appsec</td>
<td>APIv3</td>
<td></td>
<td>Logstash</td>
<td>High</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Netsec</td>
<td>authservice</td>
<td></td>
<td>Logstash</td>
<td>High</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Netsec</td>
<td>authservice</td>
<td></td>
<td>Logstash</td>
<td>High</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Appsec</td>
<td>authservice</td>
<td></td>
<td>Logstash</td>
<td>High</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Appsec</td>
<td>authservice</td>
<td></td>
<td>Logstash</td>
<td>High</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Appsec</td>
<td>authservice</td>
<td></td>
<td>Logstash</td>
<td>High</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Appsec</td>
<td>authservice</td>
<td></td>
<td>Logstash</td>
<td>High</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Appsec</td>
<td>authservice</td>
<td></td>
<td>Logstash</td>
<td>High</td>
<td>OK</td>
<td></td>
</tr>
</tbody>
</table>
Configuring a query
[Daily] CSRF errors from /wp-login.php

Last Status
1 Alerts generated

Type
Logstash

Basic
Notifications
Advanced

Query

type:web_info_log log_namespace:SECURITY logdata_sec_namespace:CSRF logdata_request_uri:/wp-login.php

The search query to execute against the Search type.

Result Type
- Fields
- Count
- No results

Result Filter
At least inf
At most inf

Description
Generate a summary of people trying to brute force creds on /wp-login (which doesn't even exist).

A description of what this Search does.
[Daily] CSRF errors from /wp-login.php

Last Status

1 Alerts generated

Type
Logstash

Basic
Notifications
Advanced

Query

```
type:web_info_log log_namespace:SECURITY logdata.sec_namespace:CSRF logdata.request_uri:('/wp-login.php')
```

The search query to execute against the Search type.

Result Type

Fields
Count
No results

Result Filter

At least
At most

Description

Generate a summary of people trying to brute force creds on /wp-login (which doesn't even exist).

A description of what this Search does.
[Daily] CSRF errors from /wp-login.php

1 Alerts generated

The search query to execute against the Search type.

Query

type:web_info_log log_namespace:SECURITY logdata.sec_namespace:CSRF logdata.request_uri:('/wp-login.php')

Result Type
- Fields
- Count
- No results

Result Filter
- At least: -inf
- At most: inf

Description
Generate a summary of people trying to brute force creds on /wp-login (which doesn't even exist).

A description of what this Search does.
Query:
```
type:web_info_log log_namespace:SECURITY logdata.sec_namespace:CSRF logdata.request_url:('/wp-login.php')
```

The search query to execute against the Search type.

Result Type
- Fields
- Count
- No results

Result Filter
- At least: -inf
- At most: inf

Description
Generate a summary of people trying to brute force login on `/wp-login` (which doesn't even exist).

A description of what this Search does.

Category: Appsec
Tags: 
Priority: Low
Frequency: 1 day
Status: Enable
The search query to execute against the Search type.

```
type:web_info_log log_namespace:SECURITY logdata.sec_namespace:CSRF logdata.request_uri:\"/wp-login.php\"
```

The search query is:

- Type: `web_info_log`
- Log namespace: `SECURITY`
- Logdata security namespace: `CSRF`
- Logdata request URI: `"/wp-login.php"`

Description:

Generate a summary of people trying to brute force login on `/wp-login` (which doesn’t even exist).

A description of what this Search does:

- Category: `Appsec`
- Priority: `Low`
- Time Range: `1 day`
- Status: `Enable`
Query:

type:web_info_log log_namespace:SECURITY logdata.sec_namespace:CSRF logdata.request_uri:('/wp-login.php')

Description:

Generate a summary of people trying to brute force logins on /wp-login (which doesn’t even exist).

Category:

Appsec

Tags:

Priority:

Low

Time Range:

1 day

Status:

Enable
<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Range</td>
<td>1 day</td>
</tr>
<tr>
<td>Frequency</td>
<td>Cron? 1 day</td>
</tr>
<tr>
<td>Status</td>
<td>Enable</td>
</tr>
</tbody>
</table>
Query:
```
type:web_info_log log_namespace:SECURITY logdata.sec_namespace:CSRF logdata.request_uri:/{\"wp-login.php\"}
```

The search query to execute against the Search type.

**Result Type**
- Fields
- Count
- No results

**Result Filter**
- At least: -inf
- At most: inf

**Description**
Generate a summary of people trying to brute force logins on /wp-login (which doesn't even exist).

**Category**
- Appsec

**Tags**

**Priority**
- Low

**Frequency**
- 1 day

**Status**
- Enable
1 Alerts generated

Type: Logstash

Basic

Notification Type: Enable
Notification Format: On demand
Source Link: 

Notifications

Assignee: Group: AppSec
Owner: Destiny Montague

Advanced

Description of changes:

Test Execute Update Delete
Group

AppSec

Type

All

Targets

User: Kai Zhong
User: Omar Ahmed
User: Ken Lee
User: Will Rogers
User: Rich Smith
User: Joseph Pistone
User: Jerry Soung
User: Chuck Clark
User: Destiny Montague

New

Select a user from the list or type in an email to add an entry to the Group.
<table>
<thead>
<tr>
<th>User</th>
<th>User</th>
<th>User</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kai Zhong</td>
<td>Omar Ahmed</td>
<td>Ken Lee</td>
<td>Will Rogers</td>
</tr>
<tr>
<td>Rich Smith</td>
<td>Joseph Pistone</td>
<td>Jerry Soung</td>
<td>Chuck Clark</td>
</tr>
<tr>
<td>Destiny Montague</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Last Status
1 Alerts generated

Type
Logstash

Basic Notifications Advanced

Autoclose
Enable Unspecified

Filters
New
Select a filter type to add it to the list and configure it.

Targets
New
Select a target type to add it to the list and configure it.

Save Filters and Targets
Select a target type to add it to the list and configure it.
Managing alerts
### Group: AppSec

#### API AuthZ Hits

<table>
<thead>
<tr>
<th>Time</th>
<th>logdata.endpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wed, 03 Aug 2016 19:57:11 GMT</td>
<td>Api_Shop_Settings</td>
</tr>
<tr>
<td>Wed, 03 Aug 2016 16:07:35 GMT</td>
<td>Api_Shop_Orders_GetAll</td>
</tr>
</tbody>
</table>

#### [Daily] CSRF errors from /wp-login.php

<table>
<thead>
<tr>
<th>Time</th>
<th>count</th>
<th>logdata.ip_addr</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wed, 03 Aug 2016 16:05:51 GMT</td>
<td>59</td>
<td>91.200.12.25</td>
</tr>
<tr>
<td>Wed, 03 Aug 2016 16:06:51 GMT</td>
<td>221</td>
<td>199.15.233.171</td>
</tr>
</tbody>
</table>
Reviewing an alert
[Daily] CSRF errors from /wp-login.php

- Time: Wed, 03 Aug 2016 16:00:51 GMT
- Assignee: AppSec
- Status: New
- count: 221
- logdata.ip_addr: 199.15.233.171

Changelog

- Wed, 03 Aug 2016 16:32:11 GMT: Alert created
### Alert

**[Daily] CSRF errors from /wp-login.php**

- **Time**: Wed, 03 Aug 2016 16:00:51 GMT
- **Assignee**: AppSec
- **Status**: New
- **count**: 221
- **logdata.ip_addr**: 199.15.233.171

### Changelog

- **Wed, 03 Aug 2016 16:02:11 GMT**: Alert created
[Daily] CSRF errors from /wp-login.php

Time: Wed, 03 Aug 2016 16:00
Assignee: AppSec
Status: New
count: 221
logdata.ip_addr: 199.15.233.171

Changelog

Wed, 03 Aug 2016 16:02:11 GMT | Alert created

Resolve

Resolution:
- Not an issue

Note:
Scammer.
[Daily] CSRF errors from /wp-login.php

Time: Wed, 03 Aug 2016 16:00:51 GMT
Assignee: AppSec
Status: Resolved
Resolution: Not an issue
count: 221
logdata.ip_addr: 199.15.233.171

Changelog

Wed, 03 Aug 2016 16:02:11 GMT | Alert created

Wed, 03 Aug 2016 21:16:54 GMT | Kai Zhong marked Resolved

Scanner.
<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Alert Description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mon, 11 Jul 2016 16:01:12 GMT</td>
<td>[Daily] Captcha - high number errors from blacklisted</td>
<td>Alert created</td>
<td></td>
</tr>
<tr>
<td>Mon, 11 Jul 2016 15:44:11 GMT</td>
<td>Captcha - high number errors</td>
<td>Alert created</td>
<td></td>
</tr>
<tr>
<td>Mon, 11 Jul 2016 14:26:12 GMT</td>
<td>Destinato</td>
<td>Alert created</td>
<td></td>
</tr>
<tr>
<td>Mon, 11 Jul 2016 14:26:12 GMT</td>
<td>Destinato</td>
<td>Alert created</td>
<td></td>
</tr>
<tr>
<td>Mon, 11 Jul 2016 14:26:12 GMT</td>
<td>Destinato</td>
<td>Alert created</td>
<td></td>
</tr>
<tr>
<td>Mon, 11 Jul 2016 14:26:12 GMT</td>
<td>Destinato</td>
<td>Alert created</td>
<td></td>
</tr>
<tr>
<td>Mon, 11 Jul 2016 14:26:12 GMT</td>
<td>Destinato</td>
<td>Alert created</td>
<td></td>
</tr>
<tr>
<td>Mon, 11 Jul 2016 14:26:12 GMT</td>
<td>Destinato</td>
<td>Alert created</td>
<td></td>
</tr>
<tr>
<td>Mon, 11 Jul 2016 14:26:12 GMT</td>
<td>Destinato</td>
<td>Alert created</td>
<td></td>
</tr>
<tr>
<td>Time</td>
<td>Description</td>
<td>Alert Type</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------------------------------------</td>
<td>------------------</td>
<td></td>
</tr>
<tr>
<td>Mon, 11 Jul 2016</td>
<td>[Daily] Captcha - high number errors from blacklisted</td>
<td>Alert created</td>
<td></td>
</tr>
<tr>
<td>16:01:12 GMT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mon, 11 Jul 2016</td>
<td>Captcha - high number errors</td>
<td>Alert created</td>
<td></td>
</tr>
<tr>
<td>15:44:11 GMT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mon, 11 Jul 2016</td>
<td>Destinato</td>
<td>Alert created</td>
<td></td>
</tr>
<tr>
<td>14:26:12 GMT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mon, 11 Jul 2016</td>
<td>Destinato</td>
<td>Alert created</td>
<td></td>
</tr>
<tr>
<td>14:26:12 GMT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mon, 11 Jul 2016</td>
<td>Destinato</td>
<td>Alert created</td>
<td></td>
</tr>
<tr>
<td>14:26:12 GMT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mon, 11 Jul 2016</td>
<td>Destinato</td>
<td>Alert created</td>
<td></td>
</tr>
<tr>
<td>14:26:12 GMT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mon, 11 Jul 2016</td>
<td>Destinato</td>
<td>Alert created</td>
<td></td>
</tr>
<tr>
<td>14:26:12 GMT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mon, 11 Jul 2016</td>
<td>Destinato</td>
<td>Alert created</td>
<td></td>
</tr>
<tr>
<td>14:26:12 GMT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mon, 11 Jul 2016</td>
<td>Destinato</td>
<td>Alert created</td>
<td></td>
</tr>
<tr>
<td>14:26:12 GMT</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Alert Management @ Etsy
Login 500s

Login 500s investigate!

Time range: 5 minute(s)

Date  message

[Thu Jul 07 16:47:02 2016] [:error] [client [REDACTED]] PHP Parse error: syntax error, unexpected end of file, expecting variable ($ VARIABLE) or $( $DOLLAR_OPEN_OURLY_BRACES) or $( $URLY_OPEN) in connections.php on line 2346 [host [REDACTED]] [request_log_id Co5ub44w8o]

Omar Ahmed to [REDACTED]  Jul 7

Ebbo ebbo wauo wauo

Can someone take a look at this file?

...

Kai Zhong to [REDACTED]  Jul 7

Asking in #mysql.
i'm sensitive - pinback button badge
beanforest $1.50
Incident Response

High sensitivity alerts
Incident Response

High sensitivity alerts

Low alerts don’t generate notification e-mails
Incident Response

High sensitivity alerts

Low alerts don’t generate notification e-mails

Medium/High alerts generate alerts
Incident Response

High sensitivity alerts

Low alerts don’t generate notification e-mails

Medium/High alerts generate alerts

Attackers often generate a lot of noise -- can result in numerous alerts firing!
Responding to an Alert

Is this an alert that can wait till morning?
Responding to an Alert

Is this an alert that can wait till morning?

How many other related alerts went off during this time period?
Alert Maintenance

Sometimes certain queries are no longer useful
Alert Maintenance

Sometimes certain queries are no longer useful

Review noisy alerts
Alert Maintenance

Sometimes certain queries are no longer useful

Review noisy alerts

Add in other useful fields
What Deserves an Alert?

Potential error conditions
What Deserves an Alert?

Potential error conditions

Volume of traffic/Thresholds being hit
What Deserves an Alert?

Potential error conditions

Volume of traffic/Thresholds being hit

Deprecating old code
Instances

Sec411
Instances

Sec411

Netsec411
Instances

Sec411

Netsec411

Sox411
More Examples
Better Queries with Lists

Duo: Activity from TOR exit notes

**Last Status**

**Type**
- TMS
- Basic
- Notifications
- Advanced

**Query**

```
type:duo_login duo.ip_address:@torexits
```

The search query to execute against the Search type.

**Result Type**
- Fields
- Count
- No results

**Result Filter**
- At least
- `-inf`

**Fields**
- `duo`
- `geoip`
- `torexits`
- `badips`
Better Queries with Lists
Graphite

A way to store and graph time series data
Graphite

A way to store and graph time series data

Best for simple threshold alerting
Graphite

A way to store and graph time series data

Best for simple threshold alerting

All of Graphite’s data transforms are available
HTTP

Detect when a HTTP endpoint returns an unexpected response
HTTP

Detect when a HTTP endpoint returns an unexpected response

Useful for web services
Detect when a HTTP endpoint returns an unexpected response

Useful for web services

Similar in functionality to Nagios
Demo
Questions?

Check out 411 here:

https://fouroneone.io

Kai
@sixhundredns
kai@etsy.com

Ken Lee
@kennysan
ken@etsy.com