
# Machine data

Machines are talking.
Are you listening?

Francesco Fresta
Associate Consultant @ TIBCO

# Obiettivi

Cosa si intende per “machine data”

Caratteristiche e proprietà

Software & Tools

**$ 1,500**

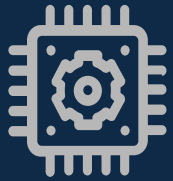
Costo di 1 ora di inattività di una macchina da stampa industriale di medie dimensioni

**11M $**

Costo medio di un attacco informatico

# Machine data

Insieme di dati generati da una macchina (server, OS, controller) ogni volta che compie una operazione, senza intervento manuale da parte dell’utente.



# Machine data - Perché?

In contesti enterprise si producono quantità **impressionanti** di dati provenienti da sistemi, network, traffico web, database…
Scovare errori e definire trend è complesso.

```
  .   ____          _            __ _ _
 /\\ / ___'_ __ _ _(_)_ __  __ _ \ \ \ \
( ( )\___ | '_ | '_| | '_ \/ _` | \ \ \ \
 \\/  ___)| |_)| | | | | || (_| |  ) ) ) )
  '  |____| .__|_| |_|_| |_\__, | / / / /
 =========|_|==============|___/=/_/_/_/
 :: Spring Boot ::        (v2.0.3.RELEASE)

2018-06-17 16:55:55.601  INFO 6082 --- [           main] c.b.s.SpringBootLoggingApplication       : Starting SpringBootLoggingApplication v0.0.1-SNAPSHOT on Phoenix2 with PID 6082 (/home/andrea/git/tutorials/spring-boot-logging/target/spring-boot-logging-0.0.1-SNAPSHOT.jar started by andrea in /home/andrea/git/tutorials/spring-boot-logging)
2018-06-17 16:55:55.609  INFO 6082 --- [           main] c.b.s.SpringBootLoggingApplication       : No active profile set, falling back to default profiles: default
2018-06-17 16:55:55.749  INFO 6082 --- [           main] ConfigServletWebServerApplicationContext : Refreshing org.springframework.boot.web.servlet.context.AnnotationConfigServletWebServerApplicationContext@1d9b7cce: startup date [Sun Jun 17 16:55:55 CEST 2018]; root of context hierarchy
WARNING: An illegal reflective access operation has occurred
WARNING: Illegal reflective access by org.springframework.cglib.core.ReflectUtils$1 (jar:file:/home/andrea/git/tutorials/spring-boot-logging/target/spring-boot-logging-0.0.1-SNAPSHOT.jar!/BOOT-INF/lib/spring-core-5.0.7.RELEASE.jar!/) to method java.lang.ClassLoader.defineClass(java.lang.String,byte[],int,int,java.security.ProtectionDomain)
WARNING: Please consider reporting this to the maintainers of org.springframework.cglib.core.ReflectUtils$1
WARNING: Use --illegal-access=warn to enable warnings of further illegal reflective access operations
WARNING: All illegal access operations will be denied in a future release
2018-06-17 16:55:59.231  INFO 6082 --- [           main] o.s.b.w.embedded.tomcat.TomcatWebServer  : Tomcat initialized with port(s): 8080 (http)
2018-06-17 16:55:59.312  INFO 6082 --- [           main] o.apache.catalina.core.StandardService   : Starting service [Tomcat]
2018-06-17 16:55:59.313  INFO 6082 --- [           main] org.apache.catalina.core.StandardEngine  : Starting Servlet Engine: Apache Tomcat/8.5.31
2018-06-17 16:55:59.331  INFO 6082 --- [ost-startStop-1] o.a.catalina.core.AprLifecycleListener   : The APR based Apache Tomcat Native library which allows optimal performance in production environments was not found on the java.library.path: [/usr/java/packages/lib:/usr/lib/x86_64-linux-gnu/jni:/lib/x86_64-linux-gnu:/usr/lib/x86_64-linux-gnu:/usr/lib/jni:/lib:/usr/lib]
2018-06-17 16:55:59.471  INFO 6082 --- [ost-startStop-1] o.a.c.c.C.[Tomcat].[localhost].[/]       : Initializing Spring embedded WebApplicationContext
2018-06-17 16:55:59.472  INFO 6082 --- [ost-startStop-1] o.s.web.context.ContextLoader            : Root WebApplicationContext: initialization completed in 3737 ms
2018-06-17 16:55:59.926  INFO 6082 --- [ost-startStop-1] o.s.b.w.servlet.ServletRegistrationBean  : Servlet dispatcherServlet mapped to [/]
2018-06-17 16:55:59.933  INFO 6082 --- [ost-startStop-1] o.s.b.w.servlet.FilterRegistrationBean   : Mapping filter: 'characterEncodingFilter' to: [/*]
2018-06-17 16:55:59.933  INFO 6082 --- [ost-startStop-1] o.s.b.w.servlet.FilterRegistrationBean   : Mapping filter: 'hiddenHttpMethodFilter' to: [/*]
2018-06-17 16:55:59.933  INFO 6082 --- [ost-startStop-1] o.s.b.w.servlet.FilterRegistrationBean   : Mapping filter: 'httpPutFormContentFilter' to: [/*]
2018-06-17 16:55:59.934  INFO 6082 --- [ost-startStop-1] o.s.b.w.servlet.FilterRegistrationBean   : Mapping filter: 'requestContextFilter' to: [/*]
2018-06-17 16:56:00.228  INFO 6082 --- [           main] o.s.w.s.handler.SimpleUrlHandlerMapping  : Mapped URL path [/**/favicon.ico] onto handler of type [class org.springframework.web.servlet.resource.ResourceHttpRequestHandler]
2018-06-17 16:56:00.810  INFO 6082 --- [           main] s.w.s.m.m.a.RequestMappingHandlerAdapter : Looking for @ControllerAdvice: org.springframework.boot.web.servlet.context.AnnotationConfigServletWebServerApplicationContext@1d9b7cce: startup date [Sun Jun 17 16:55:55 CEST 2018]; root of context hierarchy
2018-06-17 16:56:01.023  INFO 6082 --- [           main] s.w.s.m.m.a.RequestMappingHandlerMapping : Mapped "{[/]}" onto public java.lang.String com.baeldung.springbootlogging.LoggingController.index()
2018-06-17 16:56:01.044  INFO 6082 --- [           main] s.w.s.m.m.a.RequestMappingHandlerMapping : Mapped "{[/error],produces=[text/html]}" onto public org.springframework.web.servlet.ModelAndView org.springframework.boot.autoconfigure.web.servlet.error.BasicErrorController.errorHtml(javax.servlet.http.HttpServletRequest,javax.servlet.http.HttpServletResponse)
2018-06-17 16:56:01.047  INFO 6082 --- [           main] s.w.s.m.m.a.RequestMappingHandlerMapping : Mapped "{[/error]}" onto public org.springframework.http.ResponseEntity<java.util.Map<java.lang.String, java.lang.Object>> org.springframework.boot.autoconfigure.web.servlet.error.BasicErrorController.error(javax.servlet.http.HttpServletRequest)
2018-06-17 16:56:01.119  INFO 6082 --- [           main] o.s.w.s.handler.SimpleUrlHandlerMapping  : Mapped URL path [/webjars/**] onto handler of type [class org.springframework.web.servlet.resource.ResourceHttpRequestHandler]
2018-06-17 16:56:01.120  INFO 6082 --- [           main] o.s.w.s.handler.SimpleUrlHandlerMapping  : Mapped URL path [/**] onto handler of type [class org.springframework.web.servlet.resource.ResourceHttpRequestHandler]
2018-06-17 16:56:01.398  INFO 6082 --- [           main] o.s.j.e.a.AnnotationMBeanExporter        : Registering beans for JMX exposure on startup
2018-06-17 16:56:01.528  INFO 6082 --- [           main] o.s.b.w.embedded.tomcat.TomcatWebServer  : Tomcat started on port(s): 8080 (http) with context path ''
2018-06-17 16:56:01.538  INFO 6082 --- [           main] c.b.s.SpringBootLoggingApplication       : Started SpringBootLoggingApplication in 7.455 seconds (JVM running for 8.627)
2018-06-17 16:56:03.085  INFO 6082 --- [nio-8080-exec-1] o.a.c.c.C.[Tomcat].[localhost].[/]       : Initializing Spring FrameworkServlet 'dispatcherServlet'
2018-06-17 16:56:03.085  INFO 6082 --- [nio-8080-exec-1] o.s.web.servlet.DispatcherServlet        : FrameworkServlet 'dispatcherServlet': initialization started
2018-06-17 16:56:03.103  INFO 6082 --- [nio-8080-exec-1] o.s.web.servlet.DispatcherServlet        : FrameworkServlet 'dispatcherServlet': initialization completed in 18 ms
2018-06-17 16:56:03.141  INFO 6082 --- [nio-8080-exec-1] c.b.springbootlogging.LoggingController  : An INFO Message
2018-06-17 16:56:03.142  WARN 6082 --- [nio-8080-exec-1] c.b.springbootlogging.LoggingController  : A WARN Message
2018-06-17 16:56:03.142 ERROR 6082 --- [nio-8080-exec-1] c.b.springbootlogging.LoggingController  : An ERROR Message
```

# Machine data - Perché?

Collezionare, analizzare e interpretare i dati consente di semplificare attività di routine quotidiane (BAU), controllo e monitoraggio.

# Machine data - Vantaggi

Generare conoscenza a partire dai machine data porta benefici in termini economici, di sicurezza, di performance e business.

# Caratteristiche

Multiforma

Tipologia e frequenza non-standard

Alta affidabilità

# Machine-data Sources

| Data Type | Esempio |
| --- | --- |
| System Logs | Utili per investigare problemi nei sistemi informatici e anche per allertare i gruppi addetti alla sicurezza riguardo attacchi di rete e breach. |
| Web Server | Servono per debuggare le applicazioni Web e per investigare problemi lato server. |
| Authentication | Questi dati permettono di identificare gli utenti che presentano difficoltà nell'autenticazione. |
| Industrial Control Systems (ICS) | I dati ICS forniscono uptime e disponibilità di asset critici e giocano un ruolo primario se il sistema è vittima di attività malevoli. |

# Software & Tools

# ELK

Elasticsearch + Logstash + Kibana formano uno stack Open Source gratuito disponibile come prodotto o servizio (EaaS).

# ELK - Setup

Logstash processa i dati in ingresso. Elasticsearch li memorizza e li usa per effettuare le ricerche. Kibana costruisce delle interfacce sulla base delle ricerche per mostrare i risultati.

Logstash Search

2 days ago to 3 minutes ago

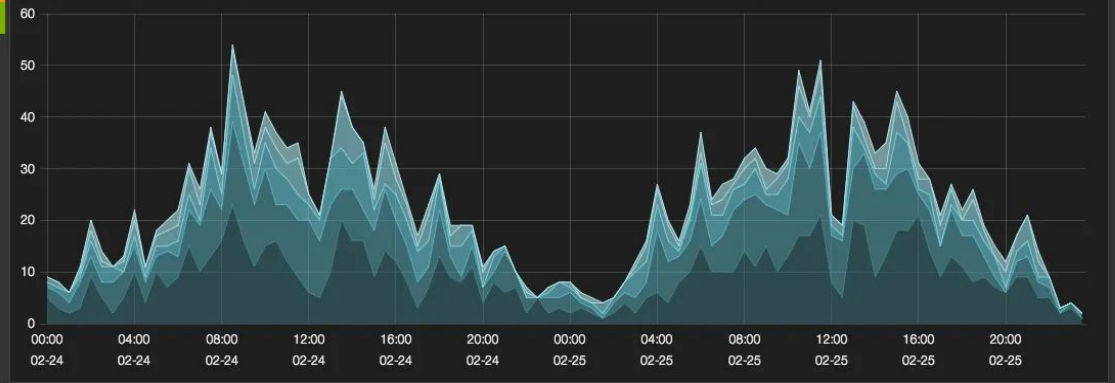
QUERY

bytes:[0 TO 4000000] AND @tags:success

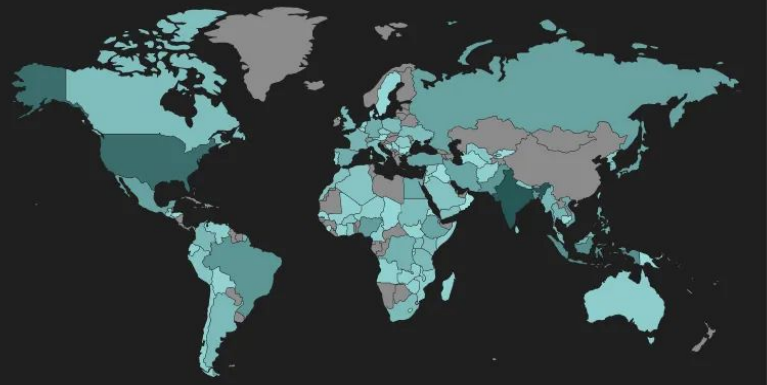
FILTERING

## EVENTS OVER TIME

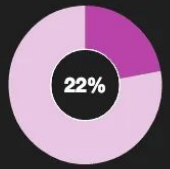
View | Zoom Out | html (ext) (888) php (ext) (659) png (ext) (317) gif (ext) (229) css (ext) (121) count per **30m** | (**2214** hits)



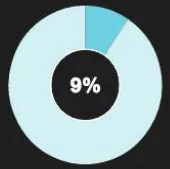

## MAP



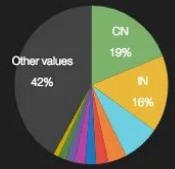
## REVENUE



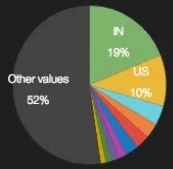

## VOLUME



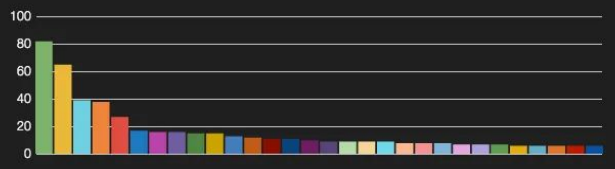

## TOP DESTINATIONS




## TOP SOURCES




## GEO PAIRS




## ALL EVENTS

**0** to **100** of 500 available for paging

Fields

All (31) / Current (28)

Type to filter...

- @message
- @tags

| @tags | geo.srcdst | extension | clientip | bytes | id | phpmemory | response |
|---|---|---|---|---|---|---|---|
| success,security | MY:VN | html | 167.12.22.189 | 8540 | 1066 | | 200 |
| success,info | IT:MM | png | 164.87.170.73 | 2045 | 1903 | | 200 |
| success,info | AR:ES | html | 222.23.102.238 | 1801 | 1133 | | 200 |
| success,info | IN:DZ | html | 138.226.66.81 | 7029 | 1801 | | 200 |

# Splunk

Software per esplorare e visualizzare dati di tutti i tipi. Consente di effettuare ricerche, costruire report e produrre grafici. Si possono creare regole di alert in base all’andamento dei dati.

# Splunk

È un software commerciale ma esiste anche una versione gratuita. È lo standard de-facto in aziende di dimensioni medio-grandi e in settori come quello bancario.

# Splunk - Funzionalità principali

Searching

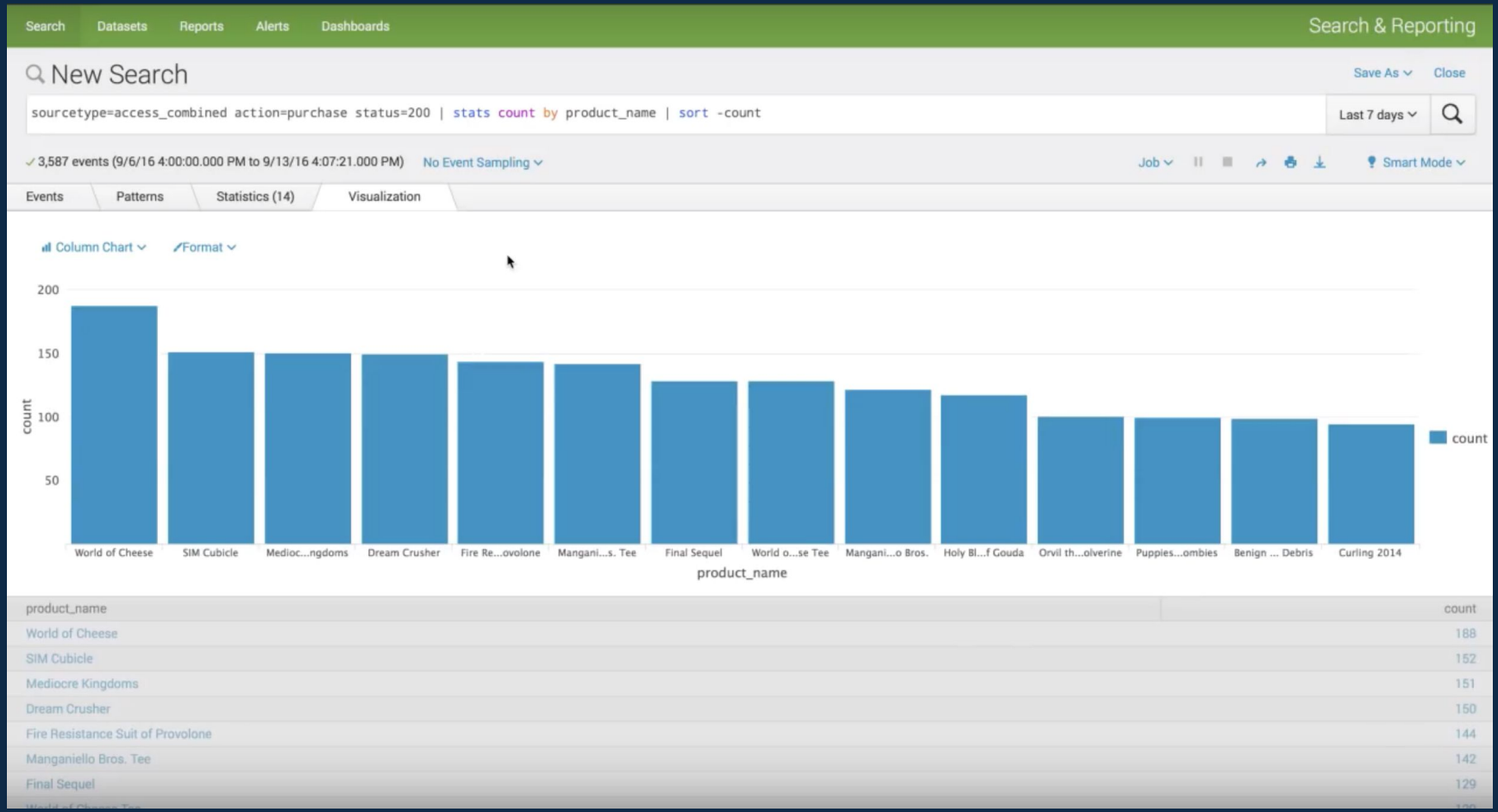
Dashboard & Visualization

Monitoring & Alerting

Reporting

# Splunk - Searching

Con Search Processing Language (SPL) è possibile effettuare le interrogazioni sui dati. Le ricerche sono rapidissime poiché i dati sono già indicizzati.




Ricerca dei prodotti più venduti online negli ultimi 7 giorni raffigurati su un istogramma

# Splunk - Dashboard & Visualization

Dashboard personalizzabili per graficare i dati.
È possibile scegliere diversi tipi di diagrammi e strumenti intuitivi, in modo da identificare problemi e opportunità.

splunk>enterprise App: Speedtest ▾ Administrator ▾ 2 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search Speedtest SPEEDTEST

Edit Dashboard UI Source + Add Panel + Add Input ▾ Cancel Save as... Save

# Performance Check

No description

Autorun dashboard

Select a Time Range: Last 7 days

Select a Time Span: 2 hours

## Fastest Download Speed

No title 42

219 Mbps

## Slowest Download Speed

No title 42

61 Mbps

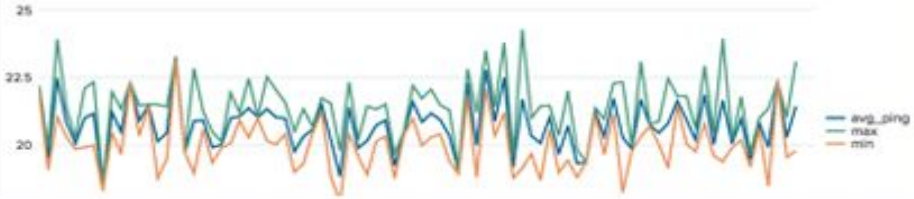
## Latest Download Speed

No title 42

119 Mbps

## Avg Ping/Latency

No title

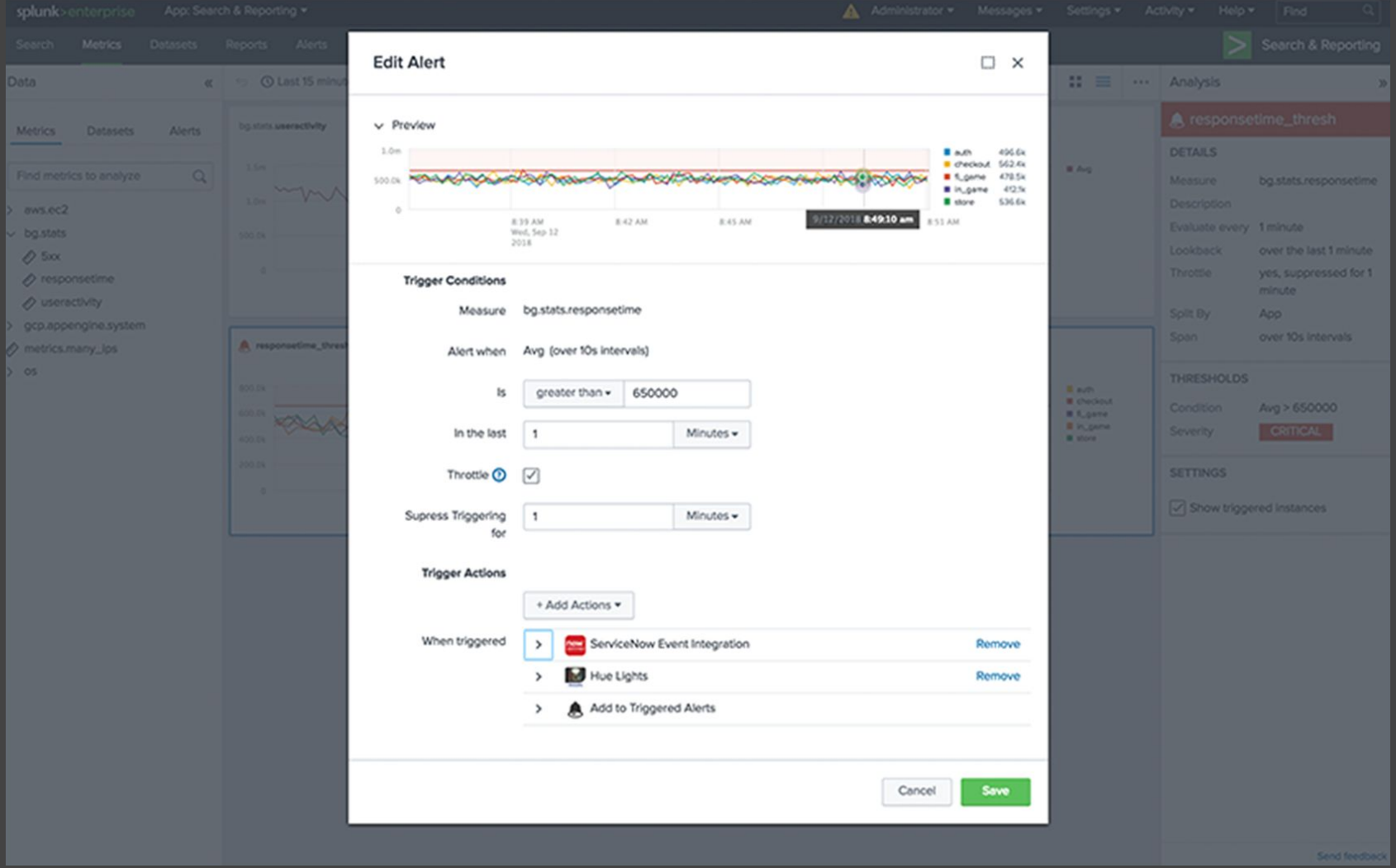



## Avg Download Speed Mbit/s

No title

# Splunk - Monitoring & Alerting

Monitoraggio continuo di eventi, condizioni e KPI critici. Con le ricerche schedulate è possibile realizzare dashboard in real-time per tenere il management e il team sempre informato.


splunk>enterprise
App: Search & Reporting
Administrator
Messages
Settings
Activity
Help
Find
Search
Metrics
Datasets
Reports
Alerts
Search & Reporting
Data
Metrics
Datasets
Alerts
Find metrics to analyze
aws.ec2
bg.stats
5xx
responsetime
useractivity
gcp.appengine.system
metrics.many_ips
os
Analysis
responsetime_thresh
DETAILS
Measure
bg.stats.responsetime
Description
Evaluate every
1 minute
Lookback
over the last 1 minute
Throttle
yes, suppressed for 1 minute
Split By
App
Span
over 10s intervals
THRESHOLDS
Condition
Avg > 650000
Severity
CRITICAL
SETTINGS
Show triggered instances
Send feedback
Edit Alert
Preview
1.0m
500.0k
0
8:39 AM
Wed, Sep 12
2018
8:42 AM
8:45 AM
9/12/2018 8:49:10 am
8:51 AM
auth 496.6k
checkout 562.4k
fl_game 478.5k
in_game 412.1k
store 536.6k
Trigger Conditions
Measure
bg.stats.responsetime
Alert when
Avg (over 10s intervals)
Is
greater than
650000
In the last
1
Minutes
Throttle
Supress Triggering for
1
Minutes
Trigger Actions
+ Add Actions
When triggered
ServiceNow Event Integration
Remove
Hue Lights
Remove
Add to Triggered Alerts
Cancel
Save

# Domande?

# Per saperne di più...

1) https://bit.ly/2P0euRH
2) https://www.elastic.co/what-is/elk-stack
3) “Splunk 7 Essentials - Third Edition: Demystify machine data by leveraging datasets, building reports, and sharing powerful insights”


# Machine data

Machines are talking.
Are you listening?

Francesco Fresta
Associate Consultant @ TIBCO