

Analyzing Machine Data with Datadog

Rajesh Kumar

www.DevOpsSchool.com



www.DevOpsSchool.com



Basic Windows Administration

Basic Linux Administration

Windows Environment

Hadoop Sandbox

www.DevOpsSchool.com



Introducing Datadog

www.DevOpsSchool.com



www.DevOpsSchool.com

Common Mistakes



“My web host already offer online statistics. This is more than enough information.”

Big mistake. Huge mistake!!!

Comparable to “well there’s usually enough money in the bank, so who needs to plan and budget?”

“ I DON'T HAVE TIME ,”

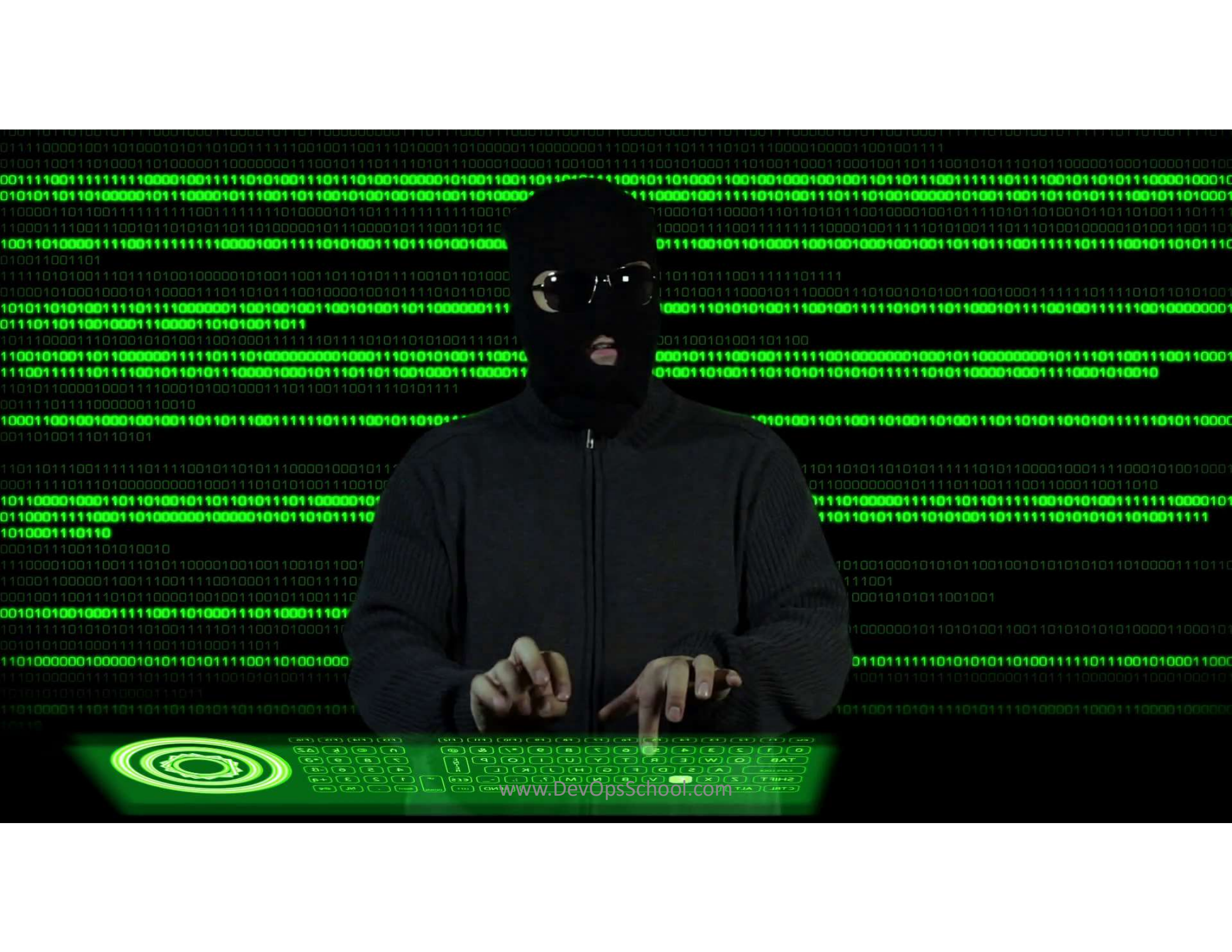
**EVEN
BIGGER
MISTAKE!!!**



www.DevOpsSchool.com

85675867 0023555460 12545022321 24685675867 0023555460 12545022321 24685675867 0023555460 12545022
52768597 02605554864 22301123254 56452768597 02605554864 22301123254 56452768597 02605554864 2230112
97546567 52107905648 89780158595 45197546567 52107905648 89780158595 45197546567 52107905648 8978015
66666666 9201.265340 46243801255 67666666666 9201.265340 46243801255 67666666666 9201.265340 46243801
65468597 5326498235. 56897845022 66665468597 5326498235. 56897845022 66665468597 5326498235. 56897845
21342430 03125643754 24584686530 52421342430 03125643754 24584686530 52421342430 03125643754 24584686
29752834 34201326497 44565752389 43529752834 34201326497 44565752389 43529752834 34201326497 44565752
56749758 88260214687 70122648654 01356749758 88260214687 70122648654 01356749758 88260214687 70122648
01326798 95462032156 89901245984 53701326798 95462032156 89901245984 53701326798 95462032156 89901245
60546412 87546200012 56578021657 78760546412 87546200012 56578021657 78760546412 87546200012 56578021
01352679 56489854222 89535670000 56701352679 56489854222 89535670000 56701352679 56489854222 89535670
524.2134 30215021569 01444587901 886524.2134 30215021569 01444587901 886524.2134 30215021569 01444587
54240404 87459823654 89564875564 54654240404 87459823654 89564875564 54654240404 87459823654 89564875
21404359 85123030213 02654895465 23421404359 85123030213 02654895465 23421404359 85123030213 02654895
53402213 13311123150 13025165465 78553402213 13311000011 13025165465 78553402213 13311125644 13025165
58672464 25468952654 76540215497 49758672464 25468952654 76540215497 49758672464 25468952654 76540215
68652031 78021328503 87654860216 97968652031 78021328503 87654860216 97968652031 78021328503 87654860
79561203 57920045685 54897564202 25679561203 57920045685 54897564202 25679561203 57920045685 54897564
56530979 48314904153 15465465460 26456530979 48314904153 15465465460 26456530979 48314904153 15465465
32031246 18946516746 21654621124 8003493164 18946516746 21654621124 8003493164 18946516746 21654621
56452123 51561687515 40216548 561687515 51561687515 40216548 561687515 51561687515 40216548
45754545 23162685421 56102165 162685421 23162685421 56102165 162685421 23162685421 56102165
91675425 62964975421 62165504 62964975421 62165504 62964975421 62165504 62964975421 62165504
59782135 35656497652 13245450154 34659782135 35656497652 13245450154 34659782135 35656497652 13245450
23100002 31200124556 84987984301 64023100002 31200124556 84987984301 64023100002 31200124556 84987984
56462857 87976423120 24568765435 13656462857 87976423120 24568765435 13656462857 87976423120 24568765
45622256 31655976421 01235435435 55645622256 31655976421 01235435435 55645622256 31655976421 01235435
66566433 05234605242 43021648576 79866566433 05234605242 43021648576 79866566433 05234605242 43021648
23101346 59257561221 53441100000 59823101346 59257561221 53441100000 59823101346 59257561221 53441100
57242104 56024565237 00000001243 56457242104 56024565237 00000001243 56457242104 56024565237 00000001
68976543 85421245454 53727672034 23168976543 85421245454 53727672034 23168976543 85421245454 53727672
12124567 45456402124 25375763520 24212124567 45456402124 25375763520 24212124567 45456402124 25375763
12054976 24575454012 43597572672 54212054976 24575454012 43597572672 54212054976 24575454012 43597572
23051564 42245454440 40133727967 85323051564 42245454440 40133727967 85323051564 42245454440 40133727
46791630 55546520303 97801322479 65246791630 55546520303 97801322479 65246791630 55546520303 97801322
52675642 40555120245 69675014372 21352675642 40555120245 69675014372 21352675642 40555120245 69675014
21000231 21205512563 97846520434 13421000231 21205512563 97846520434 13421000231 21205512563 97846520
00000005 23564012452 52768975403 24000000005 23564012452 52768975403 24000000005 23564012452 52768975
24242412 54545450215 24214672732 42424242412 54545450215 24214672732 42424242412 54545450215 24214672
52424524 88879564501 03427679854 75452424524 88879564501 03427679854 75452424524 88879564501 03427679
01243424 55556523154 64031254596 97501243424 55556523154 64031254596 97501243424 55556523154 64031254

SYSTEM FAILURE



www.DevOpsSchool.com



www.DevOpsSchool.com

I'VE MADE A



HUGE MISTAKE

WHAT HAVE YOU GOTTEN US INTO?



Log

Log = record related to whatever activities occurring on an information system

Also: alert, "event", alarm, message, record, etc

Log Data Sources

- IDS
- Firewalls/IPS
- Anti-malware
- Proxies
- Network Infrastructure
- Servers
- Databases
- Application

Machine Data

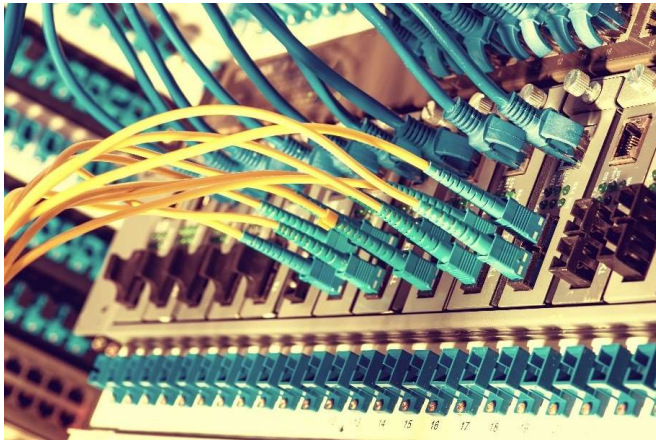
Data generated by machines, computer processing, applications and sensor data.

Machine data is everywhere.
In fact you are generating it
right now!



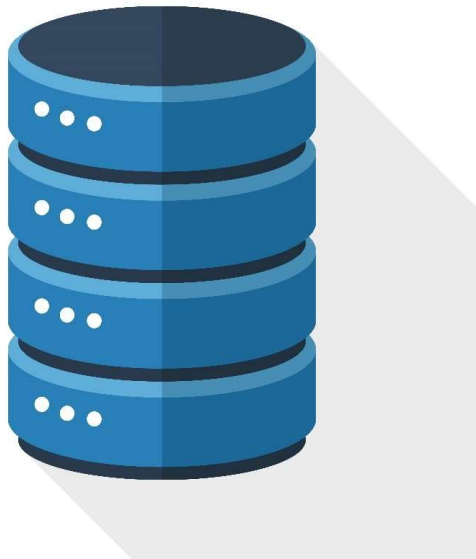
Server & Workstation Logs

- Linux/Windows
- Log files
- Access
- File system



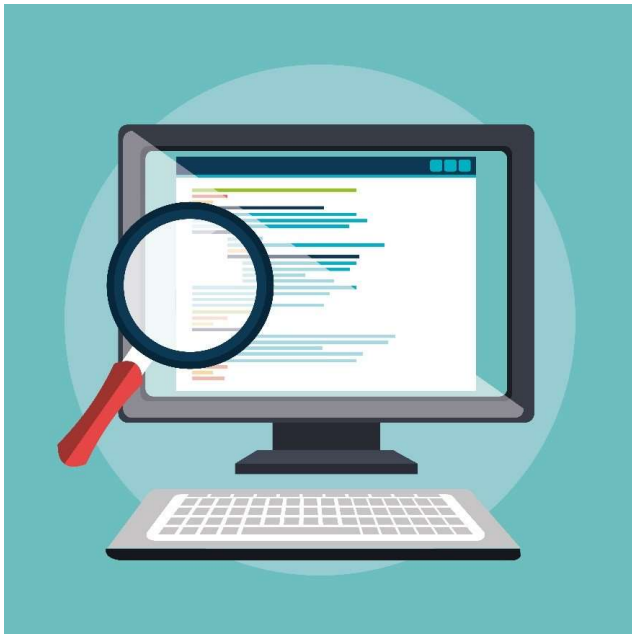
Networks

- Firewall
- Warnings
- Alerts
- IP addresses



Database

- Audit logs
- Configurations
- Schemas
- Tables
- Queries



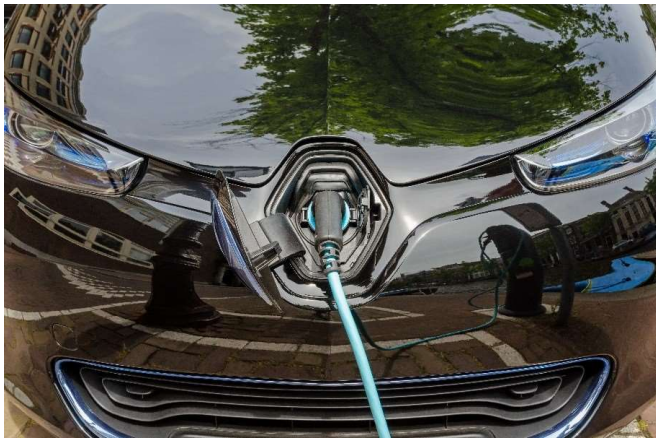
Web

- Transactions
- Click-stream
- Location
- Browser
- Time



DevOps

- Test logs
- log4j alerts
- Event logs
- Code check-in



IOT

- GPS
- RFID
- Biometric
- Temperature
- Limitless

Analyzing Log Data: Why It's Important

- Production Monitoring and Debugging
- Resource Usage
- HTTP Errors
- Slow Queries
- Rogue Automated Robots
- Security

Analyzing Log Data: Why It's Important

- Tracking Your Site's/Platform's Visitors
- Situational awareness and new threat discovery
- Getting more value out of network and security infrastructures
- Extracting what is really actionable automatically
- Measuring security (metrics, trends, etc)
- Compliance and regulations
- Incident response (last, but not least)

Best Practices For Log Analysis

Pattern detection and recognition: to filter messages based on a pattern book.

Normalization: to convert different log elements such as dates to the same format.

Tagging and classification: to tag log elements with keywords and categorize them into a number of classes so you can filter and adjust the way you display your data.

Correlation analysis: to collate logs from different sources and systems and sort meaningful messages that pertain to a particular event.

Artificial ignorance: a machine learning process to identify and “ignore” log entries that are not useful and detect anomalies.

What to look for in Logs?

Password changes

Unauthorized logins

Login failures

New login events

Malware detection

Malware attacks seen by IDS or other evidence

Scans on your firewalls open and closed ports

Denial of service attacks

Errors on network devices

File name changes

File integrity changes

Data exported

New processes started or running processes stopped

Shared access events

Disconnected events

New service installation

File auditing

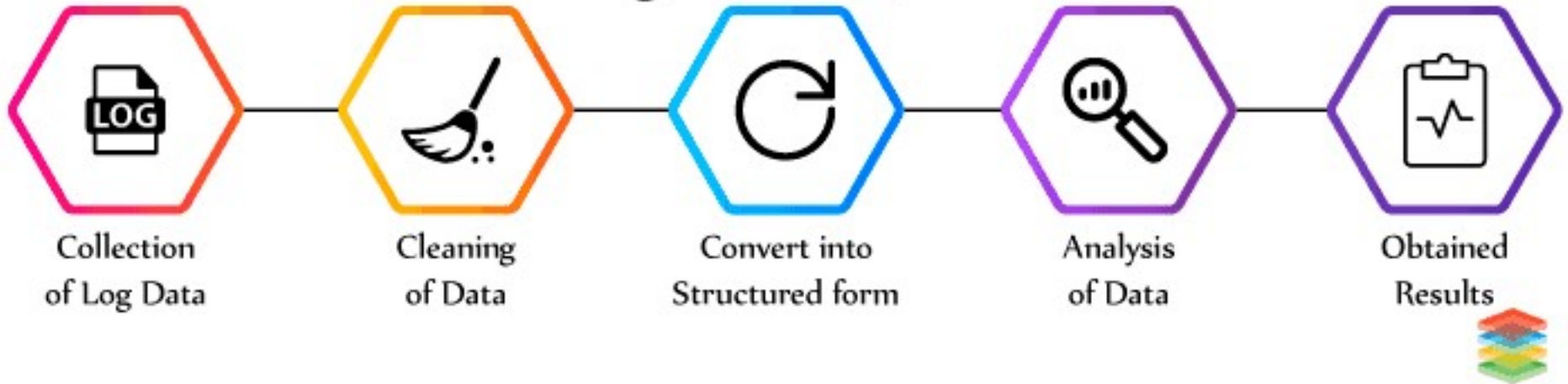
New user accounts

Modified registry values

Common Fields in Log

- ✓ Time
- ✓ Source
- ✓ Destination
- ✓ Protocol
- ✓ Port(s)
- ✓ User name
- ✓ Event/Attach type
- ✓ Bytes exchanged

Log Analysis



Log Analysis Process

- Generate
- Collect
- Aggregate
- Normalize
- Alert
- Store
- Summarize, Baseline
- Make conclusions
- Act on them



www.DevOpsSchool.com





www.DevOpsSchool.com

Analyzing Log Files



Ingest



Store



Visualize

Analyzing Log Files



Ingest

Store

Visualize

Who Is Datadog For?



DevOps



Data Analyst



Anyone

Security is one of the
fastest growing sectors in IT

www.DevOpsSchool.com

A futuristic, highly reflective silver car is shown from a low angle, focusing on its charging port. A blue charging cable is plugged into the port. The car's surface is highly polished, reflecting the surrounding environment, including trees and buildings. The text 'IOT' is overlaid in large, white, sans-serif font in the upper center of the image.

IOT

www.DevOpsSchool.com

What Data?

Index **ANY** data from **ANY** source



- Computers
- Network devices
- Virtual machines
- Internet devices
- Communication devices
- Sensors
- Databases



- Logs
- Configurations
- Messages
- Call detail records
- Clickstream
- Alerts
- Metrics
- Scripts
- Changes
- Tickets



Get Started!

www.DevOpsSchool.com

Where are your logs coming from ?

1 Select a log source

Select one of your existing integrations or a new one. Refer to the full documentation for additional configuration and frameworks. The list of supported OSes for those integrations can be found [here](#).

 **Server**
With the Datadog Agent

 **Container**
Docker, Kubernetes...

 **Cloud**
AWS, GCP, Azure...

 **Client**
JavaScript, Mobile...

 **Other**
Rsyslog, FluentD...



[Full documentation](#) | [Logs FAQ](#) | [Contact Datadog Support](#)

Where are your logs coming from ?



Server

With the Datadog Agent



Container

Docker, Kubernetes...



Cloud

AWS, GCP, Azure...



Client

JavaScript, Mobile...



Other

Rsyslog, FluentD...

1 Select a log source

Select one of your existing integrations, or a new one. Refer to the full [Documentation](#) for additional configuration and frameworks.



Datadog Log Management doesn't yet support the following integrations. Register below for updates and we'll let you know when something is ready.



Request



Request

Other integrations:

Submit

[Full documentation](#) | [Logs FAQ](#) | [Contact Datadog Support](#)

Where are your logs coming from ?



Server

With the Datadog Agent



Container

Docker, Kubernetes...



Cloud

AWS, GCP, Azure...



Client

JavaScript, Mobile...



Other

Rsyslog, FluentD...

1 Select a log source




Datadog Log Management doesn't yet support your log source? Register below for updates and we'll let you know when something is ready.

Other integrations:

Submit

[Full documentation](#) | [Logs FAQ](#) | [Contact Datadog Support](#)

Where are your logs coming from ?

 **Server**
With the Datadog Agent

 **Container**
Docker, Kubernetes...

 **Cloud**
AWS, GCP, Azure...

 **Client**
JavaScript, Mobile...


 **Other**
Rsyslog, FluentD...

1 Select a log source

Select one of your existing integrations or a new one. Refer to the full documentation for additional configuration and frameworks.

Datadog Log Management doesn't yet support the following integrations. Register below for updates and we'll let you know when something is ready.


 Request

Other integrations:

[Full documentation](#) | [Logs FAQ](#) | [Contact Datadog Support](#)

Where are your logs coming from ?



Server

With the Datadog Agent



Container

Docker, Kubernetes...



Cloud

AWS, GCP, Azure...



Client

JavaScript, Mobile...



Other

Rsyslog, FluentD...

1 Select a log source



Datadog Log Management doesn't yet support your log source? Register below for updates and we'll let you know when something is ready.

Other integrations:

Submit

[Full documentation](#) | [Logs FAQ](#) | [Contact Datadog Support](#)

Datadog Log Workflow

Log Collection & Integrations: Ingest all your logs from your hosts, containers, and cloud providers.

Processing: Process and enrich all of your logs with pipelines and processors.

Live Tail: See your ingested logs in real time across all your environments.

Generate Metrics: Generate Metrics from Ingested Logs.

Archives: Archive all enriched logs into S3 buckets.

Index: Dynamically decide what to include or exclude from your indexes to control your costs.

After indexing your logs, explore them in the Log Explorer:

Log Explorer: Discover the Log Explorer view, how to add Facets and Measures.

Search: Search through all of your indexed logs.

Analytics: Perform Log Analytics over your indexed logs.

Patterns: Spot Log Patterns by clustering your indexed logs together.

Saved Views: Use Saved Views to automatically configure your Log Explorer.

Welcome, **Rajesh!**

Get started ▾

You are **83%** done setting up.

You have **12** days left in your trial. [Upgrade](#)



Log Explorer

Save As


15min The Past 15 Minutes ▾



07:39 07:40 07:41 07:42 07:43 07:44 07:45 07:46 07:47 07:48 07:49 07:50 07:51 07:52 07:53

- Facets Saved Views
- Search facets
- Showing 8 of 8 [Add +](#)
- ▼ CORE
 - > Source
 - > Host
 - ▼ Service
No matching values found
 - ▼ Status

[Hide Controls](#) | **0 results found** [Share](#) [Options](#) ⚙️



No entries found

[Try Rehydrating From Archives](#) ↗️

Log Explorer

Save As [15min] The Past 15 Minutes [Play] [Pause] [Next] [Search] [Refresh]

[List] [Table] [Line] [Search]

07:39 07:40 07:41 07:42 07:43 07:44 07:45 07:46 07:47 07:48 07:49 07:50 07:51 07:52 07:53

Facets Saved Views [Hide Controls] **0 results found** [Share] Options [Settings]

Search facets

Showing 8 of 8 [Add +](#)

- ▼ CORE
 - > Source
 - > Host
 - ▼ Service
 - No matching values found
 - ▼ Status
 - ■ ■

No entries found

[Try Rehydrating From Archives](#)

www.DevOpsSchool.com