elastic

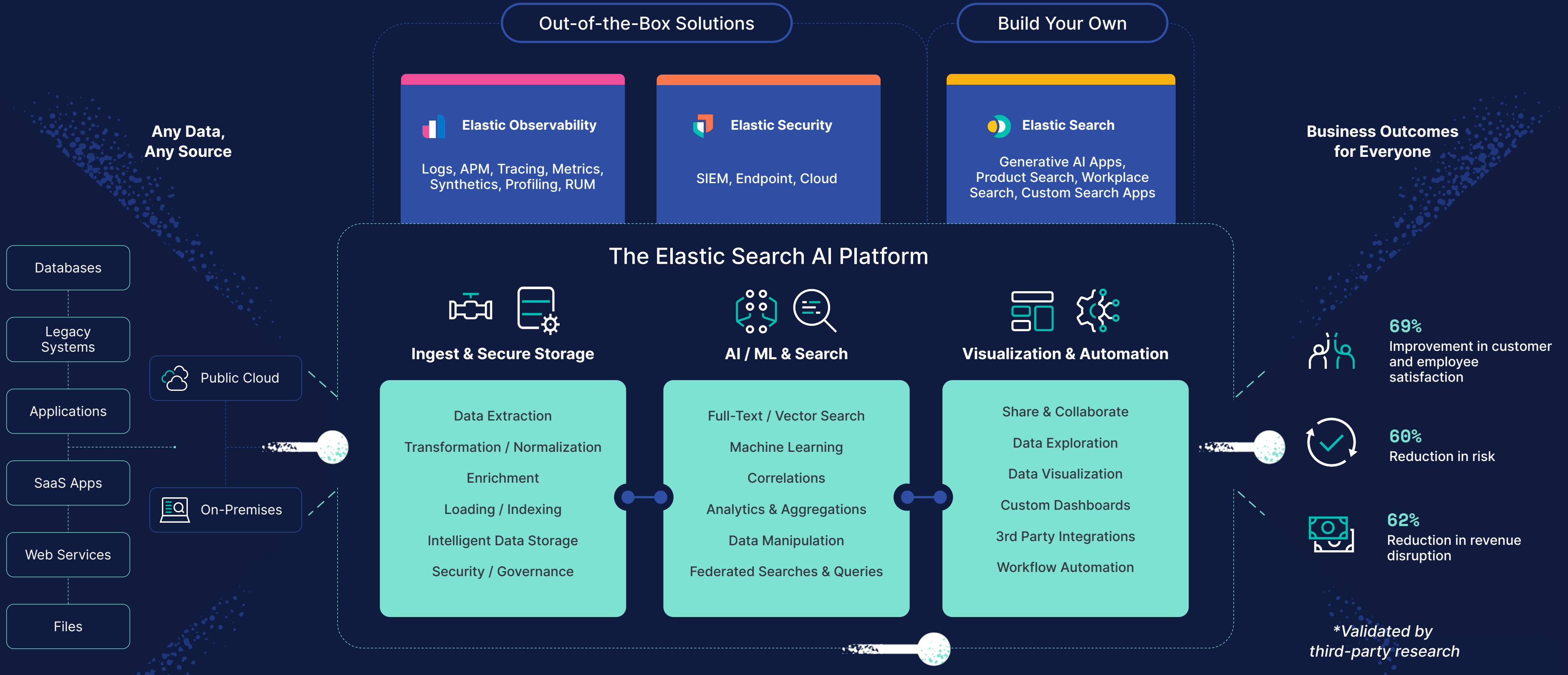
The Search Analytics Company

BBL at

Talan

```
$ curl http://localhost:9200/speaker/_doc/dpilato
{
  "name" : "David Pilato",
  "jobs" : [
    { "name" : "SRA Europe (SSII)", "date" : "1995" },
    { "name" : "SFR", "date" : "1997"  },
    { "name" : "e-Brands / Vivendi", "date": "2000" },
    { "name" : "DGDDI (douane)", "date" : "2005" },
    { "name" : "elastic", "date" : "2013" }
  ],
  "motivations" : [ "family", "job", "deejay" ],
  "blog" : "https://david.pilato.fr/",
  "twitter" : [ "@dadoonet", "@elasticfr" ],
  "email" : "david@pilato.fr"
}
```

Performance that Delivers Relevant Results in Real-time



Any Data, Any Source

- Databases
- Legacy Systems
- Applications
- SaaS Apps
- Web Services
- Files

- Public Cloud
- On-Premises

Out-of-the-Box Solutions

Elastic Observability

Logs, APM, Tracing, Metrics, Synthetics, Profiling, RUM

Elastic Security

SIEM, Endpoint, Cloud

Build Your Own

Elastic Search

Generative AI Apps, Product Search, Workplace Search, Custom Search Apps

The Elastic Search AI Platform

Ingest & Secure Storage

- Data Extraction
- Transformation / Normalization
- Enrichment
- Loading / Indexing
- Intelligent Data Storage
- Security / Governance

AI / ML & Search

- Full-Text / Vector Search
- Machine Learning
- Correlations
- Analytics & Aggregations
- Data Manipulation
- Federated Searches & Queries

Visualization & Automation

- Share & Collaborate
- Data Exploration
- Data Visualization
- Custom Dashboards
- 3rd Party Integrations
- Workflow Automation

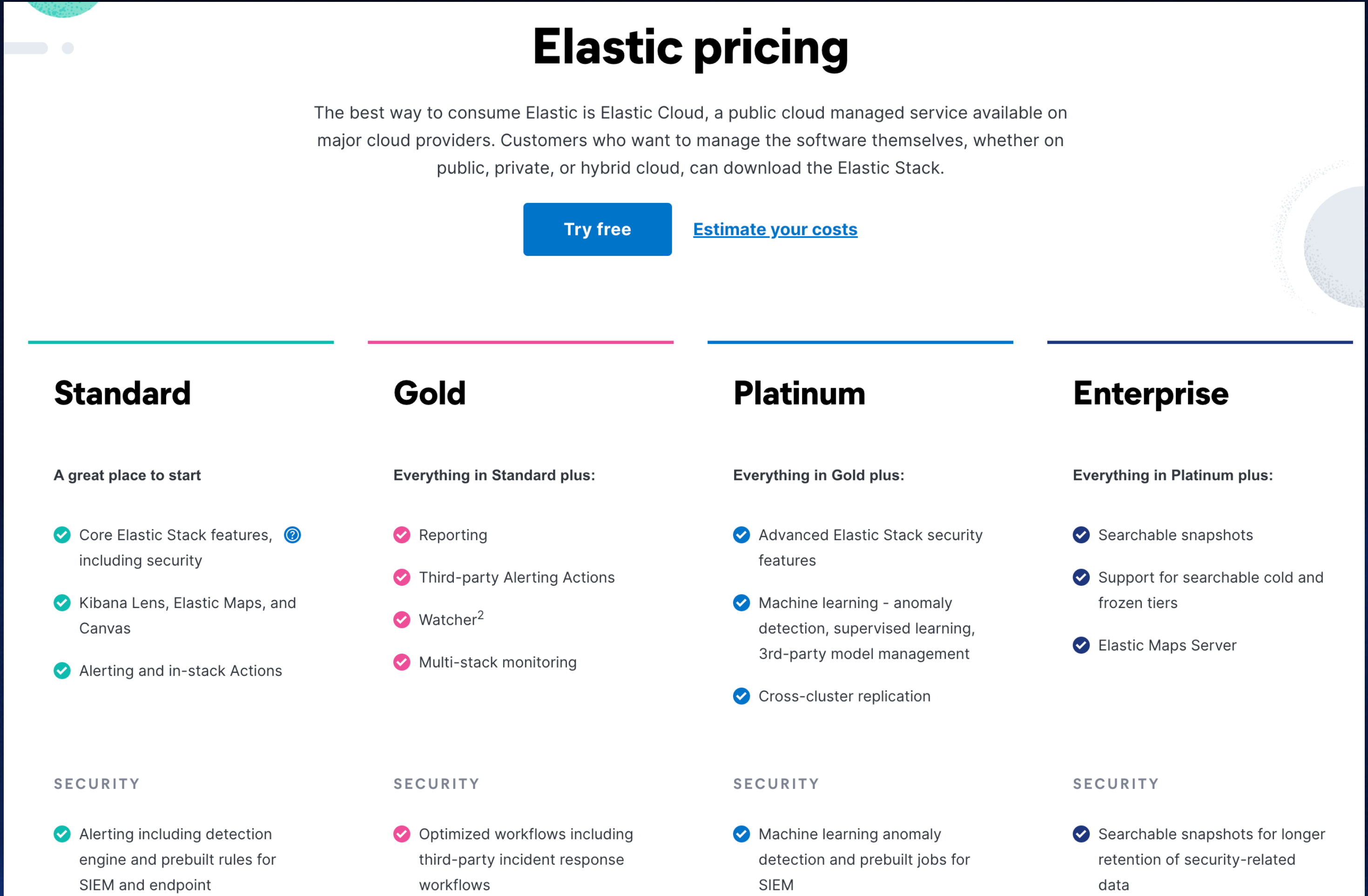
Business Outcomes for Everyone

69% Improvement in customer and employee satisfaction

60% Reduction in risk

62% Reduction in revenue disruption

**Validated by third-party research*



Elastic pricing

The best way to consume Elastic is Elastic Cloud, a public cloud managed service available on major cloud providers. Customers who want to manage the software themselves, whether on public, private, or hybrid cloud, can download the Elastic Stack.

Standard

A great place to start

- ✓ Core Elastic Stack features, including security ?
- ✓ Kibana Lens, Elastic Maps, and Canvas
- ✓ Alerting and in-stack Actions

SECURITY

- ✓ Alerting including detection engine and prebuilt rules for SIEM and endpoint

Gold

Everything in Standard plus:

- ✓ Reporting
- ✓ Third-party Alerting Actions
- ✓ Watcher[2]
- ✓ Multi-stack monitoring

SECURITY

- ✓ Optimized workflows including third-party incident response workflows

Platinum

Everything in Gold plus:

- ✓ Advanced Elastic Stack security features
- ✓ Machine learning - anomaly detection, supervised learning, 3rd-party model management
- ✓ Cross-cluster replication

SECURITY

- ✓ Machine learning anomaly detection and prebuilt jobs for SIEM

Enterprise

Everything in Platinum plus:

- ✓ Searchable snapshots
- ✓ Support for searchable cold and frozen tiers
- ✓ Elastic Maps Server

SECURITY

- ✓ Searchable snapshots for longer retention of security-related data

A typical search implementation…

```
CREATE TABLE user
(
   name VARCHAR(100),
   comments VARCHAR(1000)
);
INSERT INTO user VALUES ('David Pilato', 'Developer at elastic');
INSERT INTO user VALUES ('Malloum Laya', 'Worked with David at french
customs service');
INSERT INTO user VALUES ('David Gageot', 'Engineer at Doctolib');
INSERT INTO user VALUES ('David David', 'Who is that guy?');
```

David

Search on term

```
INSERT INTO user VALUES ('David Pilato', 'Developer at elastic');
INSERT INTO user VALUES ('Malloum Laya', 'Worked with David at french
customs service');
INSERT INTO user VALUES ('David Gageot', 'Engineer at Doctolib');
INSERT INTO user VALUES ('David David', 'Who is that guy?');
```

```
SELECT * FROM user WHERE name="David";
Empty set (0,00 sec)
```

Search like

```
INSERT INTO user VALUES ('David Pilato', 'Developer at elastic');
INSERT INTO user VALUES ('Malloum Laya', 'Worked with David at french
customs service');
INSERT INTO user VALUES ('David Gageot', 'Engineer at Doctolib');
INSERT INTO user VALUES ('David David', 'Who is that guy?');
```

```
SELECT * FROM user WHERE name LIKE "%David%";
+--------------+----------------------+
| name         | comments             |
+--------------+----------------------+
| David Pilato | Developer at elastic |
| David Gageot | Engineer at Doctolib |
| David David  | Who is that guy?     |
+--------------+----------------------+
```

elastic

Search for terms

```
INSERT INTO user VALUES ('David Pilato', 'Developer at elastic');
INSERT INTO user VALUES ('Malloum Laya', 'Worked with David at french
customs service');
INSERT INTO user VALUES ('David Gageot', 'Engineer at Doctolib');
INSERT INTO user VALUES ('David David', 'Who is that guy?');
```

```
SELECT * FROM user WHERE name LIKE "%David Pilato%";
+--------------+----------------------+
| name         | comments             |
+--------------+----------------------+
| David Pilato | Developer at elastic |
+--------------+----------------------+
```

David Pilato

Search with inverted terms

```
INSERT INTO user VALUES ('David Pilato', 'Developer at elastic');
INSERT INTO user VALUES ('Malloum Laya', 'Worked with David at french
customs service');
INSERT INTO user VALUES ('David Gageot', 'Engineer at Doctolib');
INSERT INTO user VALUES ('David David', 'Who is that guy?');
```

```
SELECT * FROM user WHERE name LIKE "%Pilato David%";
Empty set (0,00 sec)
SELECT * FROM user WHERE name LIKE "%Pilato%David%";
Empty set (0,00 sec)
```

Pilato David

Search for terms

```
INSERT INTO user VALUES ('David Pilato', 'Developer at elastic');
INSERT INTO user VALUES ('Malloum Laya', 'Worked with David at french
customs service');
INSERT INTO user VALUES ('David Gageot', 'Engineer at Doctolib');
INSERT INTO user VALUES ('David David', 'Who is that guy?');
```

```
SELECT * FROM user WHERE name LIKE "%David%" AND
                         name LIKE "%Pilato%";
+--------------+----------------------+
| name         | comments             |
+--------------+----------------------+
| David Pilato | Developer at elastic |
+--------------+----------------------+
```

Pilato David

Search in two fields

```
INSERT INTO user VALUES ('David Pilato', 'Developer at elastic');
INSERT INTO user VALUES ('Malloum Laya', 'Worked with David at french
customs service');
INSERT INTO user VALUES ('David Gageot', 'Engineer at Doctolib');
INSERT INTO user VALUES ('David David', 'Who is that guy?');
```

```
SELECT * FROM user WHERE name LIKE "%David%" OR
                         comments LIKE "%David%";
+--------------+---------------------------------------------+
| name         | comments                                    |
+--------------+---------------------------------------------+
| David Pilato | Developer at elastic                        |
| Malloum Laya | Worked with David at french customs service |
| David Gageot | Engineer at Doctolib                        |
| David David  | Who is that guy?                            |
+--------------+---------------------------------------------+
```

David

Search with typos

```
INSERT INTO user VALUES ('David Pilato', 'Developer at elastic');
INSERT INTO user VALUES ('Malloum Laya', 'Worked with David at french
customs service');
INSERT INTO user VALUES ('David Gageot', 'Engineer at Doctolib');
INSERT INTO user VALUES ('David David', 'Who is that guy?');
```

```
SELECT * FROM user WHERE name LIKE "%Dadid%";
Empty set (0,00 sec)
```

Dadid

Search with typos

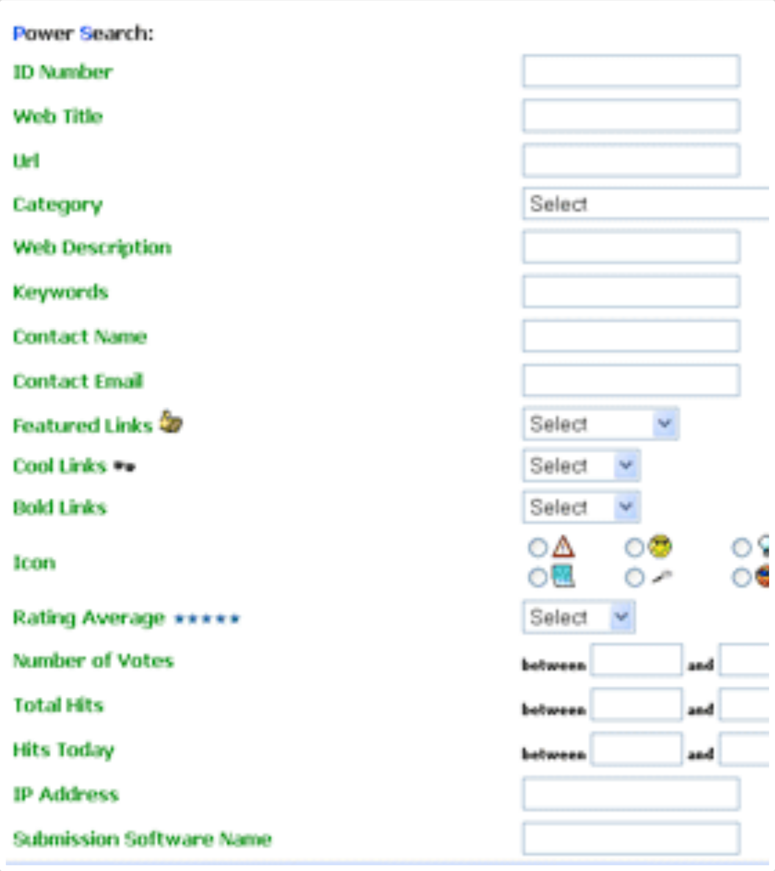
```
INSERT INTO user VALUES ('David Pilato', 'Developer at elastic');
INSERT INTO user VALUES ('Malloum Laya', 'Worked with David at french
customs service');
INSERT INTO user VALUES ('David Gageot', 'Engineer at Doctolib');
INSERT INTO user VALUES ('David David', 'Who is that guy?');
```

```
SELECT * FROM user WHERE name LIKE "%_adid%" OR
                         name LIKE "%D_did%" OR
                         name LIKE "%Da_id%" OR
                         name LIKE "%Dad_d%" OR
                         name LIKE "%Dadi_%";
+--------------+----------------------+
| name         | comments             |
+--------------+----------------------+
| David Pilato | Developer at elastic |
| David Gageot | Engineer at Doctolib |
| David David  | Who is that guy?     |
+--------------+----------------------+
```

Dadid

elastic

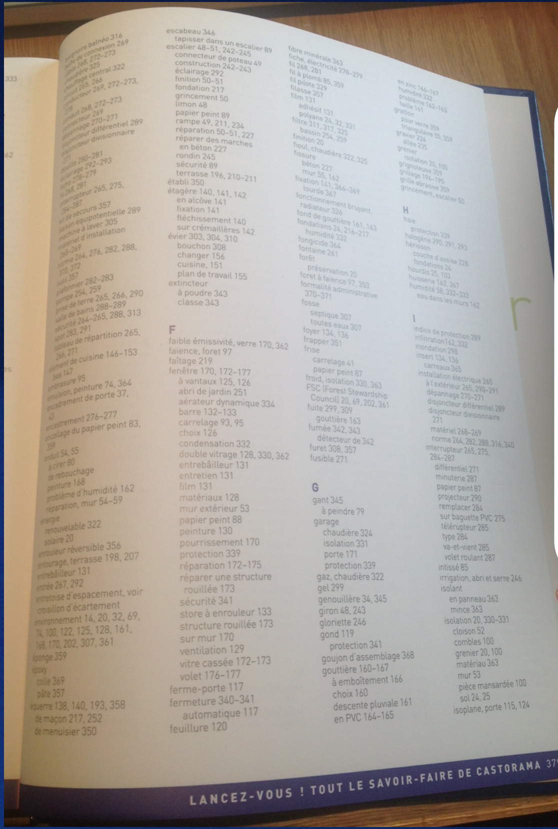
User Interface



Power Search:

ID Number	
Web Title	
Url	
Category	Select
Web Description	
Keywords	
Contact Name	
Contact Email	
Featured Links	Select
Cool Links	Select
Bold Links	Select
Icon	○ ○ ○ ○ ○ ○
Rating Average ★★★★★	Select
Number of Votes	between and
Total Hits	between and
Hits Today	between and
IP Address	
Submission Software Name	

What is a search engine?



baignoire balnéo 316
boîte de connexion 269
câble 268, 272–273
chaudière 325
chauffage central 322
circuit 265, 266
conducteur 269, 272–273, 278
conduit 268, 272–273
connecteur 269
dépannage 270–271
disjoncteur différentiel 289
disjoncteur divisionnaire 271
douille 280–281
éclairage 292–293
fiche 278–279
fil 268, 281
interrupteur 265, 275, 284–287
kit de secours 357
liaison équipotentielle 289
machine à laver 305
matériel d'installation 268–269
norme 264, 276, 282, 288, 370, 372
outil 357
plafonnier 282–283
pompe 254, 259
prise de terre 265, 266, 290
salle de bains 288–289
sécurité 264–265, 288, 313
spot 283, 291
tableau de répartition 265, 266, 271
élément de cuisine 146–153
bas 147
embrasure 95
émulsion, peinture 74, 364
encadrement de porte 37, 43
encastrement 276–277
encollage du papier peint 83, 359
enduit 54, 55
à cirer 80
de rebouchage
peinture 168
problème d'humidité 162
réparation, mur 54–59
énergie
renouvelable 322
solaire 20
enrouleur réversible 356
entourage, terrasse 198, 207
entrebâilleur 131
entrée 267, 292
entretoise d'espacement, voir croisillon d'écartement
environnement 14, 20, 32, 69, 74, 100, 122, 125, 128, 161, 168, 170, 202, 307, 361
éponge 359
époxy
colle 369
pâte 357
équerre 138, 140, 193, 358
de maçon 217, 252
de menuisier 350

escabeau 346
tapisser dans un escalier 89
escalier 48–51, 242–245
connecteur de poteau 49
construction 242–243
éclairage 292
finition 50–51
fondation 217
grincement 50
limon 48
papier peint 89
rampe 49, 211, 234
réparation 50–51, 227
réparer des marches en béton 227
rondin 245
sécurité 89
terrasse 196, 210–211
établi 350
étagère 140, 141, 142
en alcôve 141
fixation 141
fléchissement 140
sur crémaillères 142
évier 303, 304, 310
bouchon 308
changer 156
cuisine, 151
plan de travail 155
extincteur
à poudre 343
classe 343

F

faible émissivité, verre 170, 362
faïence, foret 97
faîtage 219
fenêtre 170, 172–177
à vantaux 125, 126
abri de jardin 251
aérateur dynamique 334
barre 132–133
carrelage 93, 95
choix 126
condensation 332
double vitrage 128, 330, 362
entrebâilleur 131
entretien 131
film 131
matériaux 128
mur extérieur 53
papier peint 88
peinture 130
pourrissement 170
protection 339
réparation 172–175
réparer une structure rouillée 173
sécurité 341
store à enrouleur 133
structure rouillée 173
sur mur 170
ventilation 129
vitre cassée 172–173
volet 176–177
ferme-porte 117
fermeture 340–341
automatique 117
feuillure 120

fibre minérale 363
fiche, électricité 278–279
fil 268, 281
fil à plomb 85, 359
fil pilote 329
filasse 357
film 131
adhésif 131
polyane 24, 32, 331
filtre 311, 317, 325
bassin 254, 259
finition 20
fioul, chaudière 322, 325
fissure
béton 227
mur 55, 162
fixation 141, 366–369
lourde 367
fonctionnement bruyant, radiateur 326
fond de gouttière 161, 163
fondations 24, 216–217
humidité 332
fongicide 364
fontaine 261
forêt
préservation 20
foret à faïence 97, 353
formalité administrative 370–371
fosse
septique 307
toutes eaux 307
foyer 134, 136
frapper 351
frise
carrelage 41
papier peint 87
froid, isolation 330, 363
FSC (Forest Stewardship Council) 20, 69, 202, 361
fuite 299, 309
gouttière 163
fumée 342, 343
détecteur de 342
furet 308, 357
fusible 271

G

gant 345
à peindre 79
garage
chaudière 324
isolation 331
porte 171
protection 339
gaz, chaudière 322
gel 299
genouillère 34, 345
giron 48, 243
gloriette 246
gond 119
protection 341
goujon d'assemblage 368
gouttière 160–167
à emboîtement 166
choix 160
descente pluviale 161
en PVC 164–165

en zinc 166–167
humidité 332
problème 162–163
taille 161
grattoir
pour verre 359
triangulaire 55, 359
gravier 224
allée 235
grenier
isolation 20, 100
grignoteuse 359
grillage 194–195
grille abrasive 359
grincement, escalier 50

H

haie
protection 339
halogène 290, 291, 293
hérisson
couche d'assise 228
fondations 24
hourdis 25, 103
huisserie 162, 367
humidité 58, 332–333
eau dans les murs 162

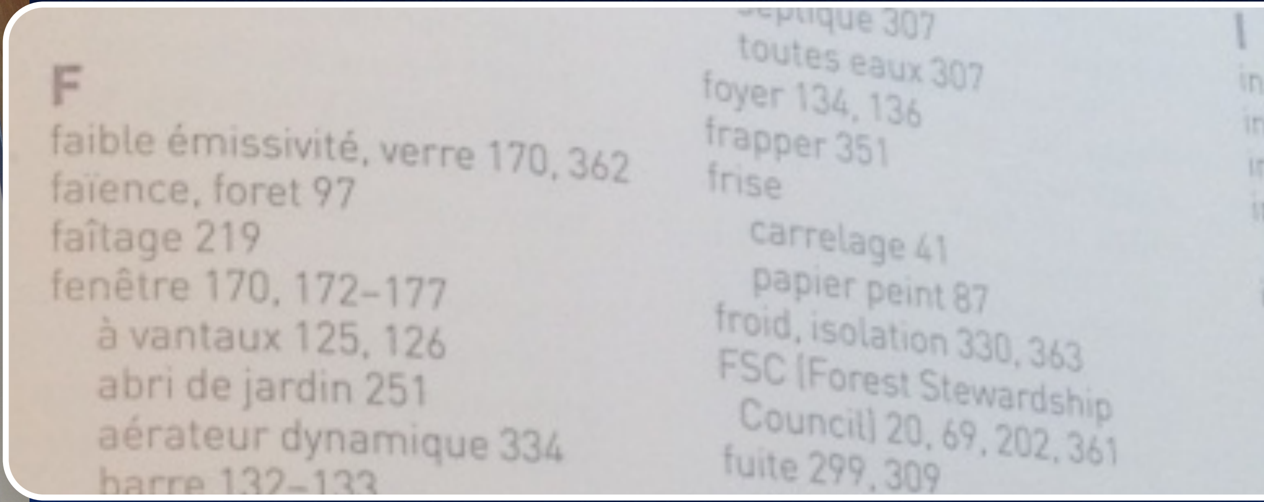
I

indice de protection 289
infiltration162, 332
inondation 298
insert 134, 136
carreaux 365
installation électrique 265
à l'extérieur 265, 290–291
dépannage 270–271
disjoncteur différentiel 289
disjoncteur divisionnaire 271
matériel 268–269
norme 264, 282, 288, 316, 340
interrupteur 265, 275, 284–287
différentiel 271
minuterie 287
papier peint 87
projecteur 290
remplacer 284
sur baguette PVC 275
télérupteur 285
type 284
va-et-vient 285
volet roulant 287
intissé 85
irrigation, abri et serre 246
isolant
en panneau 363
mince 363
isolation 20, 330–331
cloison 52
combles 100
grenier 20, 100
matériau 363
mur 53
pièce mansardée 100
sol 24, 25
isoplane, porte 115, 124

INDEX

LANCEZ-VOUS ! TOUT LE SAVOIR-FAIRE DE CASTORAMA 379

- **Index engine** (indexing documents)



F
faible émissivité, verre 170, 362
faïence, foret 97
faîtage 219
fenêtre 170, 172–177
à vantaux 125, 126
abri de jardin 251
aérateur dynamique 334
barre 132–133

septique 307
toutes eaux 307
foyer 134, 136
frapper 351
frise
carrelage 41
papier peint 87
froid, isolation 330, 363
FSC (Forest Stewardship Council) 20, 69, 202, 361
fuite 299, 309

- **Search engine** (within the created indices)

Demo time!

Elasticsearch

You Know, for Search

elastic

```
GET /_analyze
{
  "char_filter": [ "html_strip" ],
  "tokenizer": "standard",
  "filter": [ "lowercase", "stop", "snowball" ],
  "text": "These are <em>not</em> the droids
           you are looking for."
}
```

```
These are <em>not</em> the droids you are looking for.
```

```
{ "tokens": [{
      "token": "droid",
      "start_offset": 27, "end_offset": 33,
      "type": "<ALPHANUM>", "position": 4
    },{
      "token": "you",
      "start_offset": 34, "end_offset": 37,
      "type": "<ALPHANUM>", "position": 5
    }, {
      "token": "look",
      "start_offset": 42, "end_offset": 49,
      "type": "<ALPHANUM>", "position": 7
    }]}
```

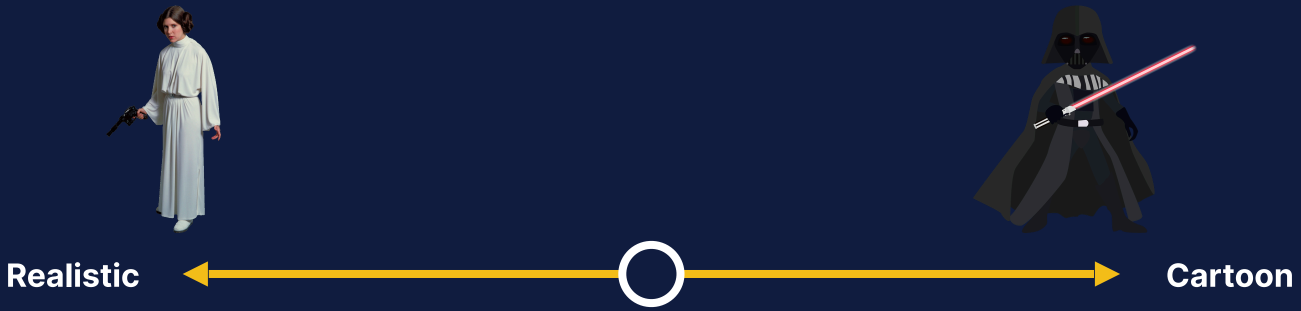
Elasticsearch

You Know, for **Vector** Search

elastic

Embeddings represent your data

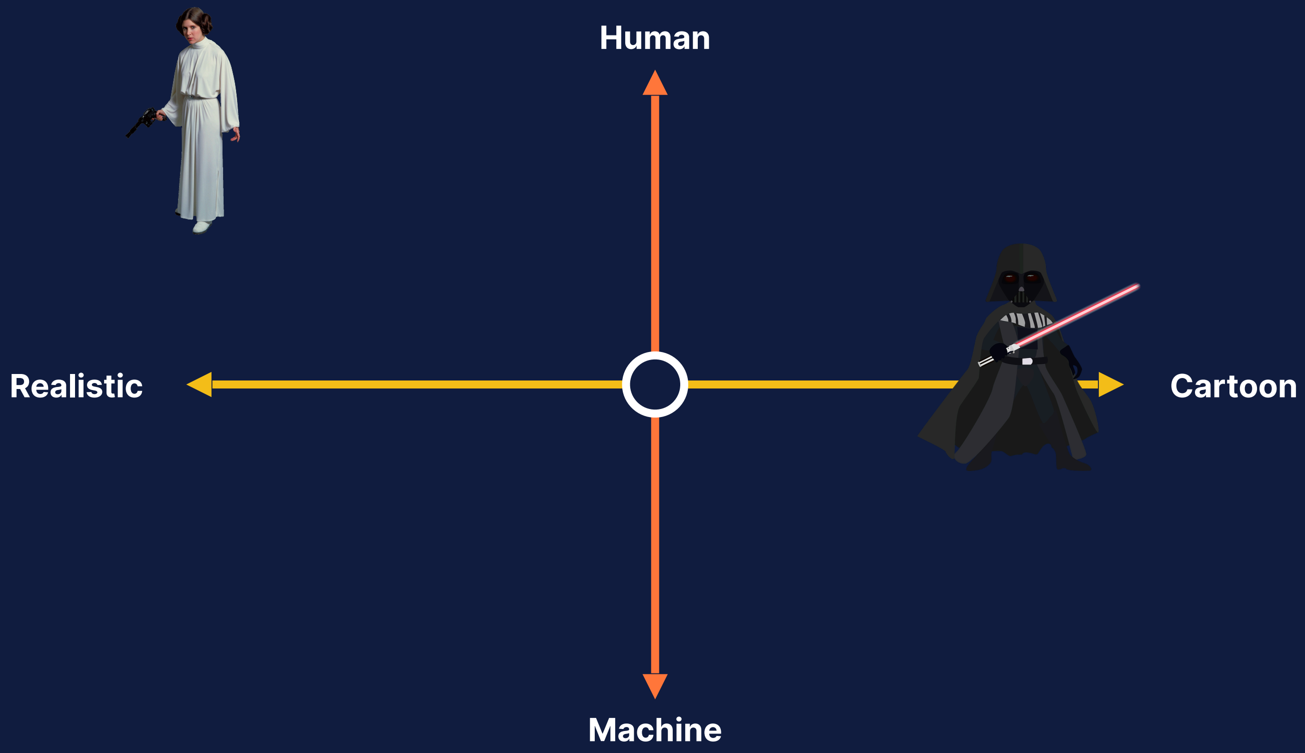
Example: 1-dimensional vector



Character	Vector
	[-1]
	[1]

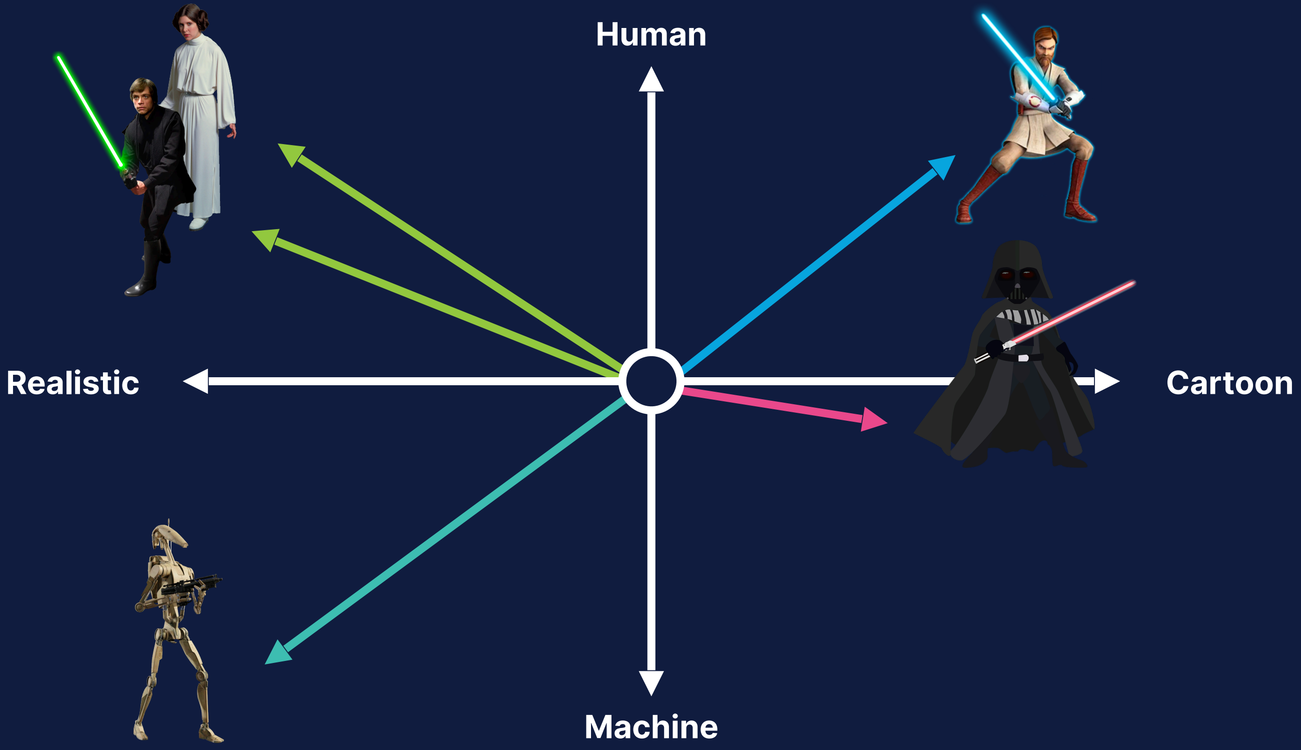
Multiple dimensions

represent different data aspects



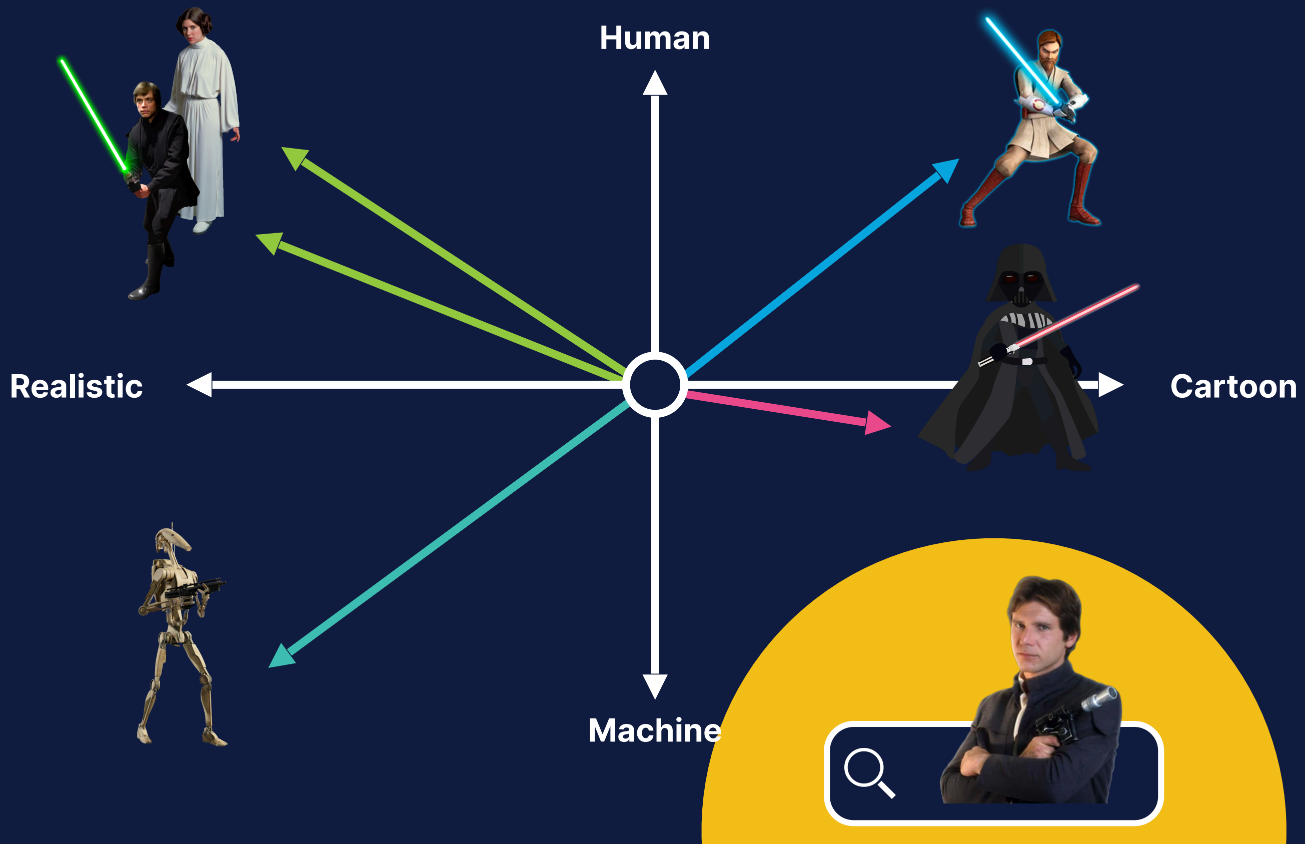
Character	Vector
	[-1, 1]
	[1, 0]

Similar data
is grouped together



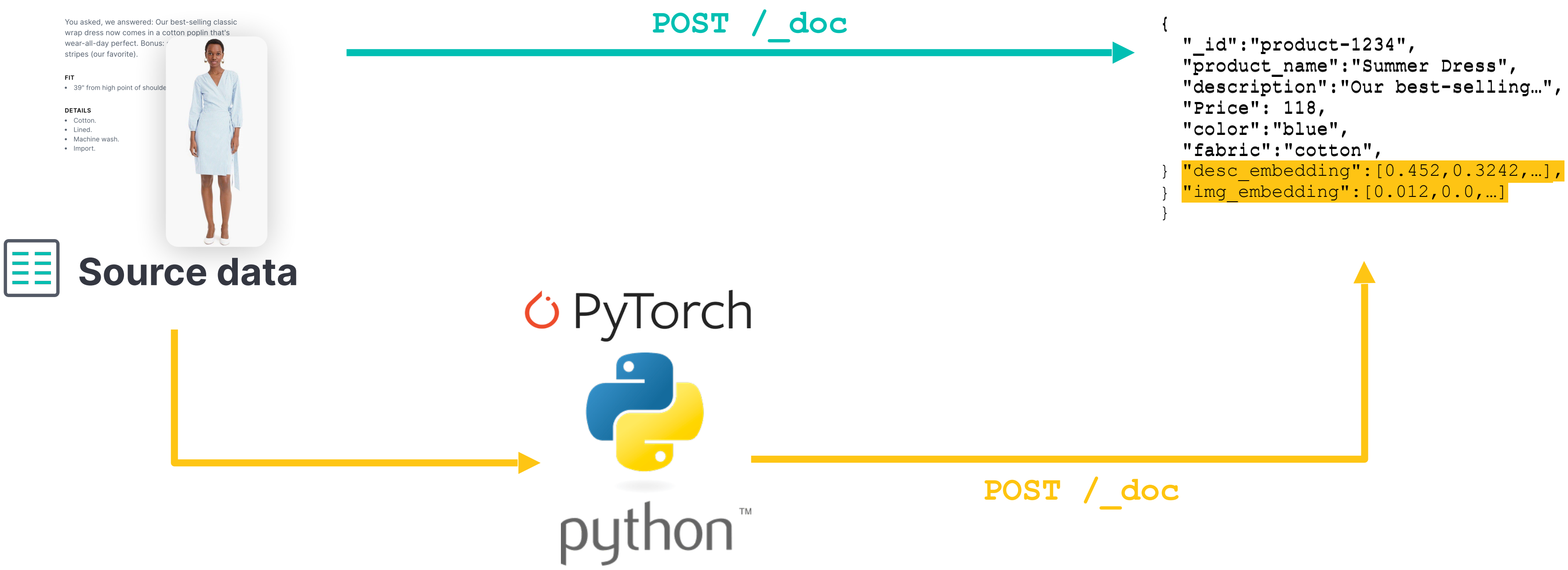
Character	Vector
	[-1.0, 1.0]
	[1.0, 0.0]
	[-1.0, 0.8]

Vector search ranks objects
by similarity (~relevance) to the query



Rank	Result
Query	
1	
2	
3	
4	
5	

Data Ingestion and Embedding Generation



You asked, we answered: Our best-selling classic wrap dress now comes in a cotton poplin that's wear-all-day perfect. Bonus: stripes (our favorite).

FIT

- 39" from high point of shoulde

DETAILS

- Cotton.
- Lined.
- Machine wash.
- Import.

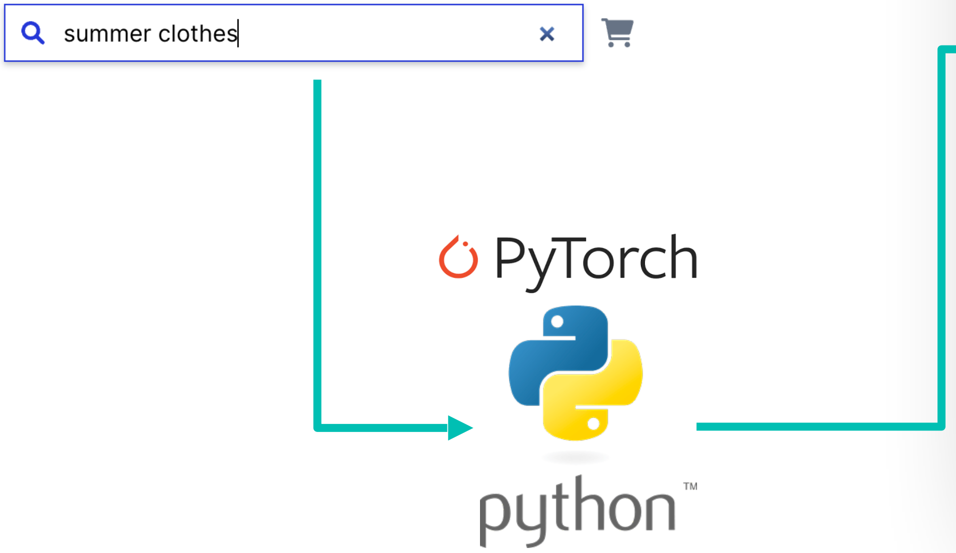
Source data

POST /_doc

```
{
  "_id":"product-1234",
  "product_name":"Summer Dress",
  "description":"Our best-selling…",
  "Price": 118,
  "color":"blue",
  "fabric":"cotton",
} "desc_embedding":[0.452,0.3242,…],
} "img_embedding":[0.012,0.0,…]
}
```

POST /_doc

Vector Query

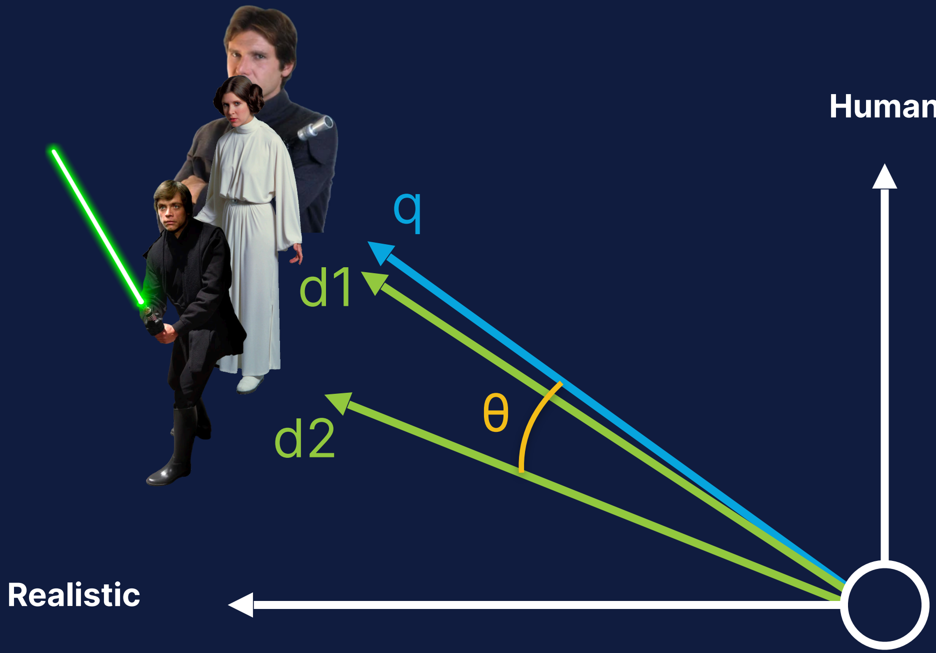


```
GET product-catalog/_search
{
 "query" : {
    "bool": {
      "must": [{
         "knn": {
           "field": "desc_embbeding",
           "num_candidates": 50,
           "query_vector": [0.123, 0.244,...]




         }
      }],
      "filter": {
        "term": {
          "department": "women"
        }
      }
    }
  },
  "size": 10
}
```

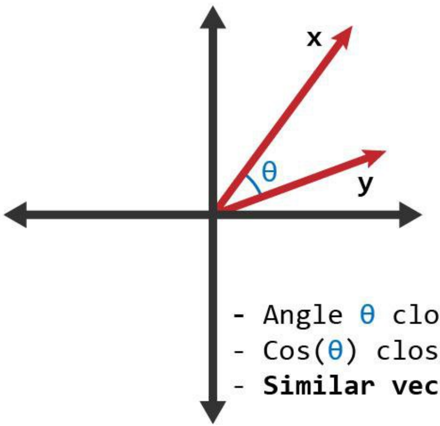
Similarity: cosine (cosine)



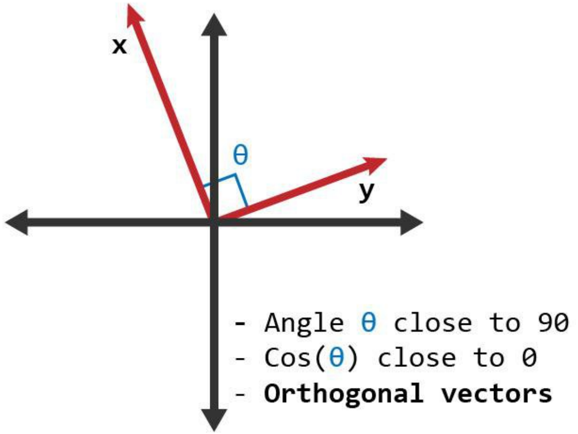
$$cos(\theta) = \frac{\vec{q} \times \vec{d}}{|\vec{q}| \times |\vec{d}|}$$

$$\_score = \frac{1 + cos(\theta)}{2}$$

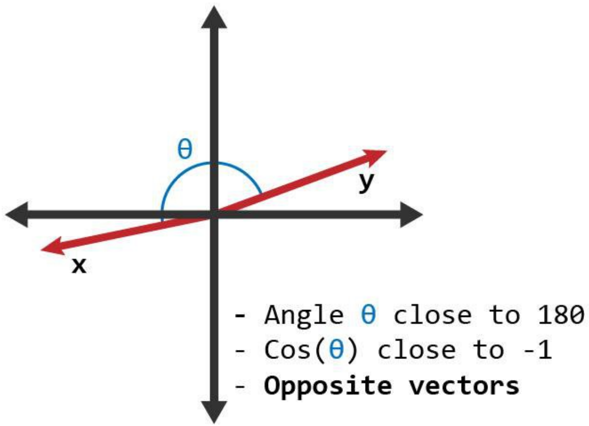
Similarity: cosine (cosine)



- Angle θ close to 0
- Cos(θ) close to 1
- **Similar vectors**



- Angle θ close to 90
- Cos(θ) close to 0
- **Orthogonal vectors**



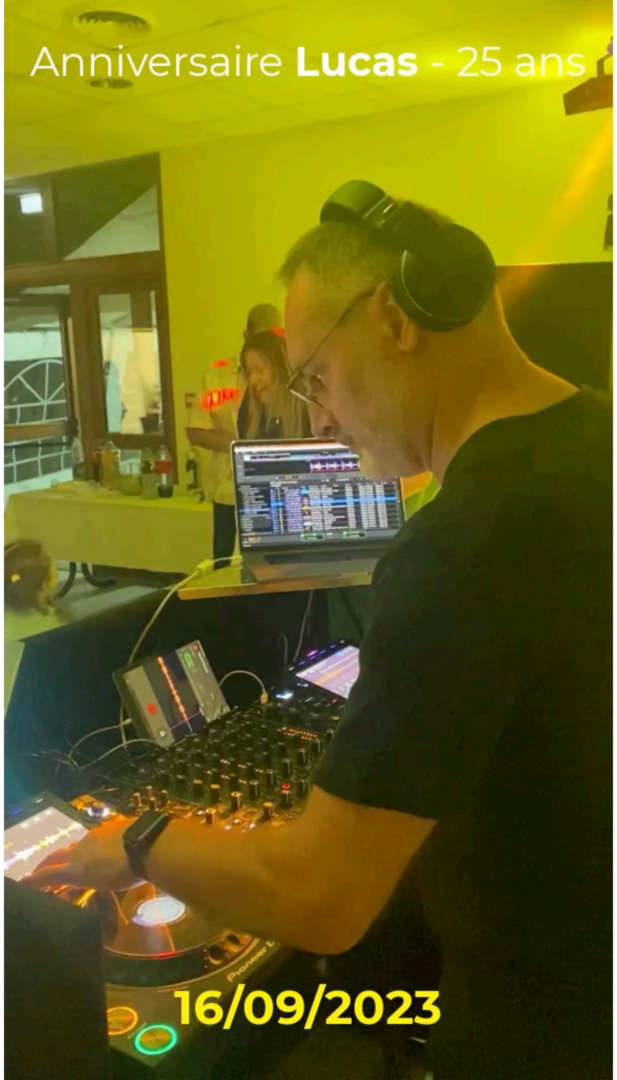
- Angle θ close to 180
- Cos(θ) close to -1
- **Opposite vectors**

$$\_score = \frac{1+1}{2} = 1$$

$$\_score = \frac{1+0}{2} = 0.5$$

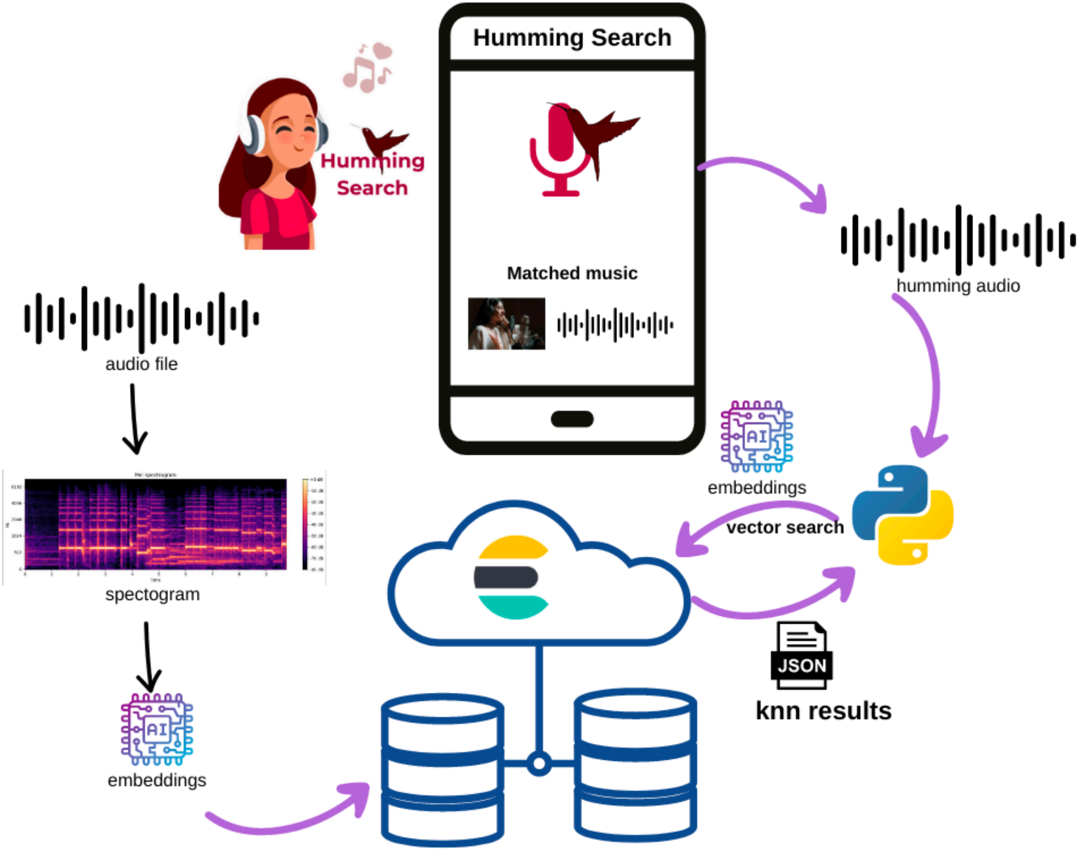
$$\_score = \frac{1-1}{2} = 0$$

https://djdadoo.pilato.fr/



Anniversaire **Lucas** - 25 ans

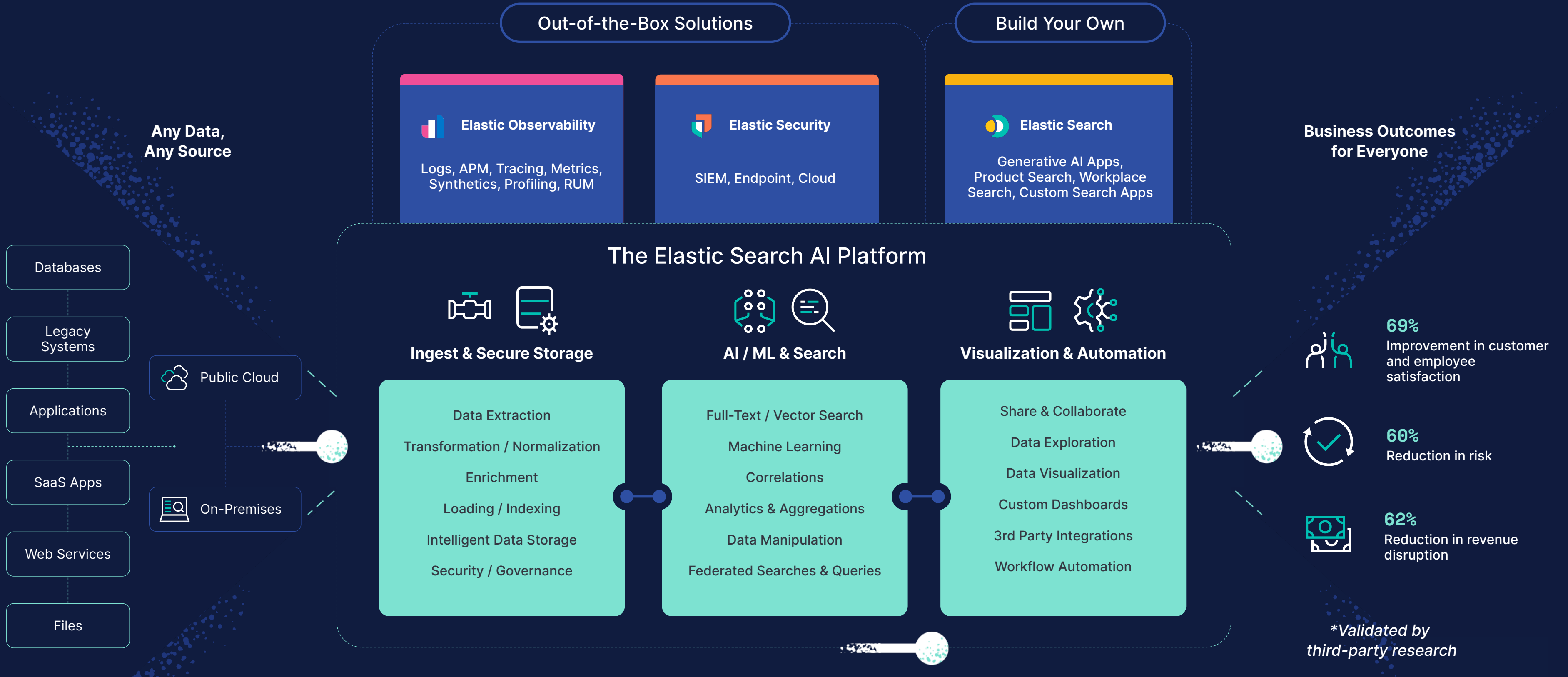
16/09/2023



https://github.com/dadoonet/music-search/

elastic

Performance that Delivers Relevant Results in Real-time



Any Data, Any Source

- Databases
- Legacy Systems
- Applications
- SaaS Apps
- Web Services
- Files

Public Cloud

On-Premises

Out-of-the-Box Solutions

Elastic Observability

Logs, APM, Tracing, Metrics, Synthetics, Profiling, RUM

Elastic Security

SIEM, Endpoint, Cloud

Build Your Own

Elastic Search

Generative AI Apps, Product Search, Workplace Search, Custom Search Apps

The Elastic Search AI Platform

Ingest & Secure Storage

- Data Extraction
- Transformation / Normalization
- Enrichment
- Loading / Indexing
- Intelligent Data Storage
- Security / Governance

AI / ML & Search

- Full-Text / Vector Search
- Machine Learning
- Correlations
- Analytics & Aggregations
- Data Manipulation
- Federated Searches & Queries

Visualization & Automation

- Share & Collaborate
- Data Exploration
- Data Visualization
- Custom Dashboards
- 3rd Party Integrations
- Workflow Automation

Business Outcomes for Everyone

69%
Improvement in customer and employee satisfaction

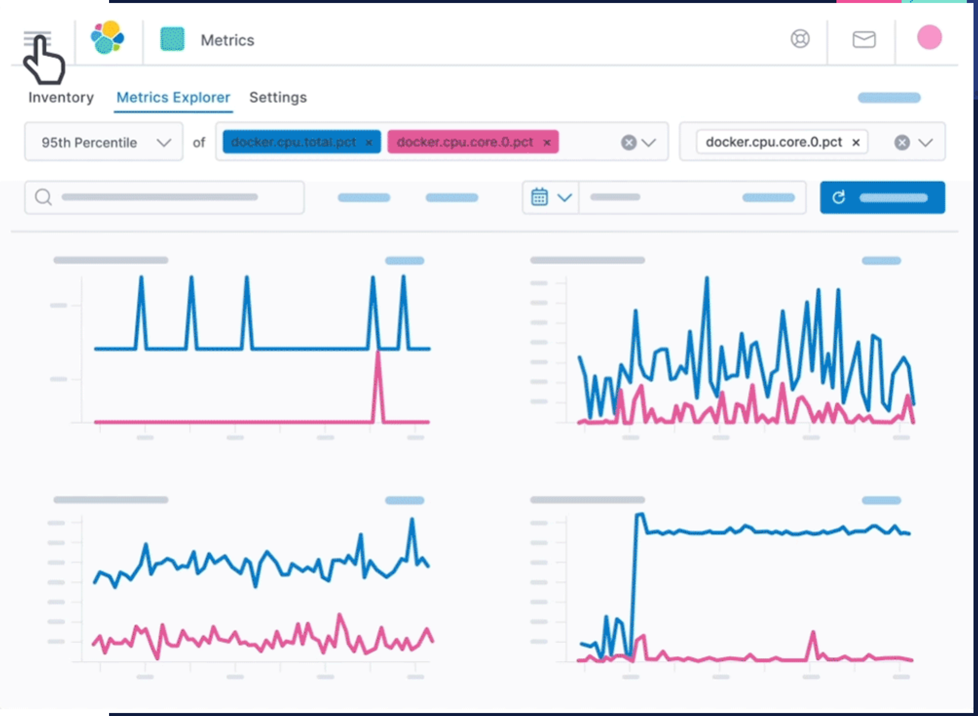
60%
Reduction in risk

62%
Reduction in revenue disruption

**Validated by third-party research*

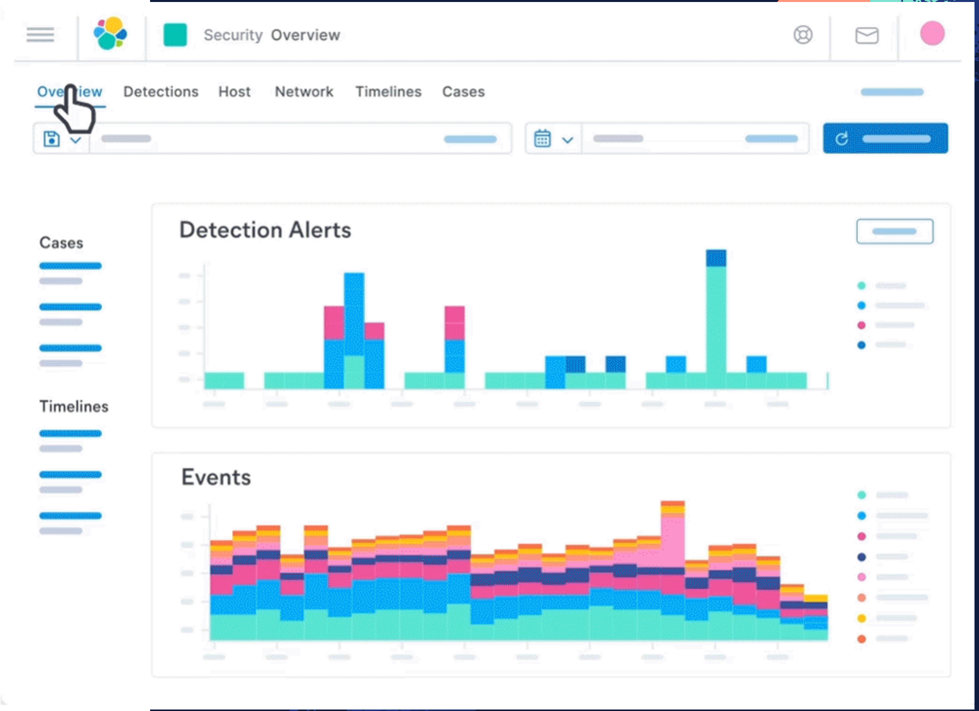
Elastic Observability

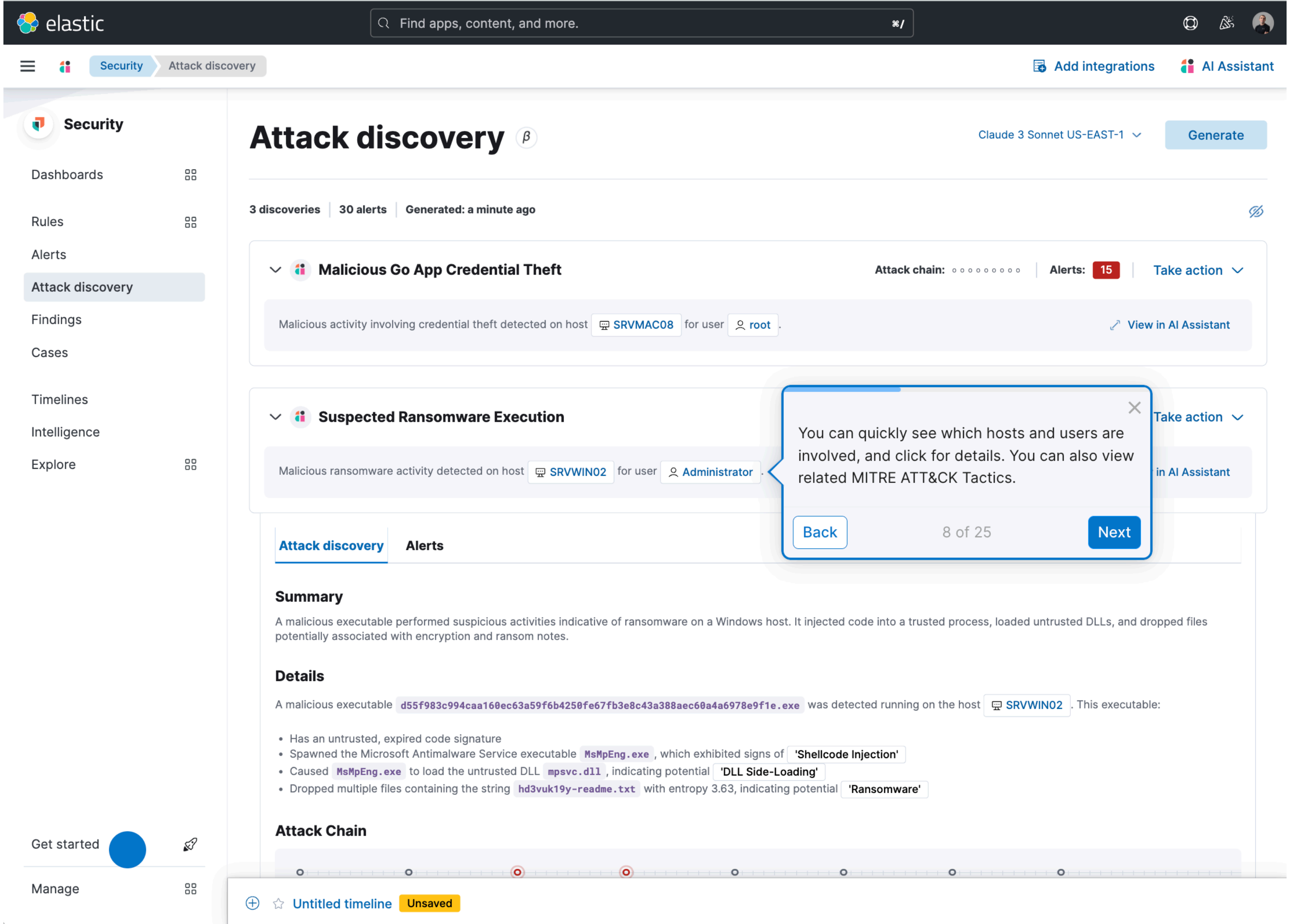
Converge metrics, logs, traces, and more to deliver unified visibility and actionable insights with the most widely deployed observability solution.



Elastic Security

Protect, investigate, and respond to complex threats with a security solution that unifies the capabilities of SIEM, endpoint security, and cloud security.





Attack discovery β

3 discoveries | 30 alerts | Generated: a minute ago

Malicious Go App Credential Theft

Attack chain: ○○○○○○○○○ Alerts: 15

Malicious activity involving credential theft detected on host SRVMAC08 for user root.

Suspected Ransomware Execution

Malicious ransomware activity detected on host SRVWIN02 for user Administrator.

You can quickly see which hosts and users are involved, and click for details. You can also view related MITRE ATT&CK Tactics.

Back 8 of 25 Next

Attack discovery | Alerts

Summary

A malicious executable performed suspicious activities indicative of ransomware on a Windows host. It injected code into a trusted process, loaded untrusted DLLs, and dropped files potentially associated with encryption and ransom notes.

Details

A malicious executable `d55f983c994caa160ec63a59f6b4250fe67fb3e8c43a388aec60a4a6978e9f1e.exe` was detected running on the host SRVWIN02. This executable:

- Has an untrusted, expired code signature
- Spawned the Microsoft Antimalware Service executable `MsMpEng.exe`, which exhibited signs of 'Shellcode Injection'
- Caused `MsMpEng.exe` to load the untrusted DLL `mpsvc.dll`, indicating potential 'DLL Side-Loading'
- Dropped multiple files containing the string `hd3vuk19y-readme.txt` with entropy 3.63, indicating potential 'Ransomware'

Attack Chain

Meetup

www.meetup.com/ElasticFR

@elasticfr

elastic
User Group

discuss.elastic.co

Thank You

elastic | The Search AI Company