



KubeCon



CloudNativeCon

Europe 2026

#KubeCon #CloudNativeCon

Enriching Telemetry Signals with OTel Collector



- João Duarte
- Lisbon, Portugal 
- Elastic @ Observability Ingest 
- Main hobby: collecting hobbies and being bad at them.
- Collected recently: solo board games, painting minis, game engine dev, SDR, lock picking, indoor bouldering, D&D, and more.



KubeCon



CloudNativeCon

Europe 2026

Enrichment?



What's Enrichment?



KubeCon



CloudNativeCon

Europe 2026

- The process of making someone **wealthy** or **wealthier**.

What's Enrichment?



KubeCon



CloudNativeCon

Europe 2026

- The process of making someone **wealthy** or **wealthier**.
- The action of improving or enhancing the quality or value of something.

What's Enrichment?



KubeCon



CloudNativeCon

Europe 2026

- ~~The process of making someone **wealthy** or **wealthier**.~~
- The action of improving or enhancing the quality or value of something.



Enrichment

- The action of improving or **enhancing** the quality or **value** of **something**

Enrichment

- The action of improving or **enhancing** the quality or **value** of **something**
- **Something** = Signals travelling through OTel Collector

Raw Signal Problem



KubeCon



CloudNativeCon

Europe 2026

```
{
  "timestamp": "2026-04-01T10:15:30Z",
  "body": "POST /api/v1/orders returned 500",
  "attributes": {
    "http.method": "POST",
    "http.route": "/api/v1/orders",
    "http.status_code": 500
  },
  "resource": {
    "service.name": "order-service"
  }
}
```

Enrichment: Raw Signal Problem



KubeCon



CloudNativeCon

Europe 2026

- The action of improving or **enhancing** the quality or **value** of **something**
- **Something** = Signals travelling through OTel Collector
- **Enhancing of Value** comes from **Context**

Enrichment: Raw Signal Problem



KubeCon



CloudNativeCon

Europe 2026

- The action of improving or **enhancing** the quality or **value** of **something**
- **Something** = Signals travelling through OTel Collector
- **Enhancing of Value** comes from **Context**

Context (examples):

- Infrastructure context: The app doesn't know it's running on AWS eu-west-1
- Organizational context: The app doesn't know its cost center or owning team
- External context: The app doesn't know 10.244.3.17 maps to a known threat IP

Raw Signal



KubeCon



CloudNativeCon

Europe 2026

```
{
  "timestamp": "2026-04-01T10:15:30Z",
  "body": "POST /api/v1/orders returned 500",
  "attributes": {
    "http.method": "POST",
    "http.route": "/api/v1/orders",
    "http.status_code": 500
  },
  "resource": {
    "service.name": "order-service"
  }
}
```

Enriched Signal



KubeCon



CloudNativeCon

Europe 2026

```
{
  "timestamp": "2026-04-01T10:15:30Z",
  "body": "POST /api/v1/orders returned 500",
  "attributes": {
    "http.method": "POST",
    "http.route": "/api/v1/orders",
    "http.status_code": 500,
    "http.status_class": "5xx"
  },
  "resource": {
    "service.name": "order-service",
    "service.team": "checkout-team",
    "service.tier": "critical",
    "deployment.environment": "production",
    "cloud.provider": "aws",
    "k8s.pod.name": "order-service-7b9f4-xk2mn",
    "k8s.namespace.name": "commerce",
    "k8s.deployment.name": "order-service"
  }
}
```

Types of Enrichment



KubeCon



CloudNativeCon

Europe 2026

- Type 1: Self-Contained Parsing & Derivation
 - ◆ Transform, compute, or extract from existing telemetry data
- Type 2: Contextual Metadata Enrichment
 - ◆ Add infrastructure/environment context (cloud, k8s, host)
- Type 3: Reference Data Lookup
 - ◆ Enrich from files, config maps, or slow-changing external data
- Type 4: Dynamic External Enrichment
 - ◆ Real-time queries to external services (DNS, HTTP APIs, databases)
- Type 5: Cross-Event Correlation & Aggregation
 - ◆ Join or aggregate across multiple events/signals
- Type 6: Analytical & ML-Based Enrichment
 - ◆ Anomaly detection, classification, scoring

Types of Enrichment



KubeCon



CloudNativeCon

Europe 2026

- Type 1: Self-Contained Parsing & Derivation
 - ◆ Transform, compute, or extract from existing telemetry data
- Type 2: Contextual Metadata Enrichment
 - ◆ Add infrastructure/environment context (cloud, k8s, host)
- Type 3: Reference Data Lookup
 - ◆ Enrich from files, config maps, or slow-changing external data
- Type 4: Dynamic External Enrichment
 - ◆ Real-time queries to external services (DNS, HTTP APIs, databases)
- Type 5: Cross-Event Correlation & Aggregation
 - ◆ Join or aggregate across multiple events/signals
- Type 6: Analytical & ML-Based Enrichment
 - ◆ Anomaly detection, classification, scoring

Types of Enrichment



KubeCon



CloudNativeCon

Europe 2026

- Type 1: Self-Contained Parsing & Derivation
 - ◆ Transform, compute, or extract from existing telemetry data
- Type 2: Contextual Metadata Enrichment
 - ◆ Add infrastructure/environment context (cloud, k8s, host)
- Type 3: Reference Data Lookup
 - ◆ Enrich from files, config maps, or slow-changing external data
- Type 4: Dynamic External Enrichment
 - ◆ Real-time queries to external services (DNS, HTTP APIs, databases)
- Type 5: Cross-Event Correlation & Aggregation
 - ◆ Join or aggregate across multiple events/signals
- Type 6: Analytical & ML-Based Enrichment
 - ◆ Anomaly detection, classification, scoring

Types of Enrichment



KubeCon



CloudNativeCon

Europe 2026

- Type 1: Self-Contained Parsing & Derivation
 - ◆ Transform, compute, or extract from existing telemetry data
- Type 2: Contextual Metadata Enrichment
 - ◆ Add infrastructure/environment context (cloud, k8s, host)
- Type 3: Reference Data Lookup
 - ◆ Enrich from files, config maps, or slow-changing external data
- Type 4: Dynamic External Enrichment
 - ◆ Real-time queries to external services (DNS, HTTP APIs, databases)
- Type 5: Cross-Event Correlation & Aggregation
 - ◆ Join or aggregate across multiple events/signals
- Type 6: Analytical & ML-Based Enrichment
 - ◆ Anomaly detection, classification, scoring

Types of Enrichment



KubeCon



CloudNativeCon

Europe 2026

- Type 1: Self-Contained Parsing & Derivation
 - ◆ Transform, compute, or extract from existing telemetry data
- Type 2: Contextual Metadata Enrichment
 - ◆ Add infrastructure/environment context (cloud, k8s, host)
- Type 3: Reference Data Lookup
 - ◆ Enrich from files, config maps, or slow-changing external data
- Type 4: Dynamic External Enrichment
 - ◆ Real-time queries to external services (DNS, HTTP APIs, databases)
- Type 5: Cross-Event Correlation & Aggregation
 - ◆ Join or aggregate across multiple events/signals
- Type 6: Analytical & ML-Based Enrichment
 - ◆ Anomaly detection, classification, scoring

Types of Enrichment



KubeCon



CloudNativeCon

Europe 2026

- Type 1: Self-Contained Parsing & Derivation
 - ◆ Transform, compute, or extract from existing telemetry data
- Type 2: Contextual Metadata Enrichment
 - ◆ Add infrastructure/environment context (cloud, k8s, host)
- Type 3: Reference Data Lookup
 - ◆ Enrich from files, config maps, or slow-changing external data
- Type 4: Dynamic External Enrichment
 - ◆ Real-time queries to external services (DNS, HTTP APIs, databases)
- Type 5: Cross-Event Correlation & Aggregation
 - ◆ Join or aggregate across multiple events/signals
- Type 6: Analytical & ML-Based Enrichment
 - ◆ Anomaly detection, classification, scoring

Types of Enrichment: OTel Collector?



KubeCon



CloudNativeCon

Europe 2026

- Type 1: Self-Contained Parsing & Derivation
 - ◆ Transform, compute, or extract from existing telemetry data
- Type 2: Contextual Metadata Enrichment
 - ◆ Add infrastructure/environment context (cloud, k8s, host)
- Type 3: Reference Data Lookup
 - ◆ Enrich from files, config maps, or slow-changing external data
- Type 4: Dynamic External Enrichment
 - ◆ Real-time queries to external services (DNS, HTTP APIs, databases)
- Type 5: Cross-Event Correlation & Aggregation
 - ◆ Join or aggregate across multiple events/signals
- Type 6: Analytical & ML-Based Enrichment
 - ◆ Anomaly detection, classification, scoring



Types of Enrichment: OTel Collector



KubeCon



CloudNativeCon

Europe 2026

- Type 1: Self-Contained Parsing & Derivation
 - ◆ Transform, compute, or extract from existing telemetry data
- Type 2: Contextual Metadata Enrichment
 - ◆ Add infrastructure/environment context (cloud, k8s, host)
- Type 3: Reference Data Lookup
 - ◆ Enrich from files, config maps, or slow-changing external data
- Type 4: Dynamic External Enrichment
 - ◆ Real-time queries to external services (DNS, HTTP APIs, databases)
- Type 5: Cross-Event Correlation & Aggregation
 - ◆ Join or aggregate across multiple events/signals
- Type 6: Analytical & ML-Based Enrichment
 - ◆ Anomaly detection, classification, scoring

OTTL, transformprocessor,
attributesprocessor



Types of Enrichment: OTel Collector



KubeCon



CloudNativeCon

Europe 2026

- Type 1: Self-Contained Parsing & Derivation
 - ◆ Transform, compute, or extract from existing telemetry data
- Type 2: Contextual Metadata Enrichment
 - ◆ Add infrastructure/environment context (cloud, k8s, host)
- Type 3: Reference Data Lookup
 - ◆ Enrich from files, config maps, or slow-changing external data
- Type 4: Dynamic External Enrichment
 - ◆ Real-time queries to external services (DNS, HTTP APIs, databases)
- Type 5: Cross-Event Correlation & Aggregation
 - ◆ Join or aggregate across multiple events/signals
- Type 6: Analytical & ML-Based Enrichment
 - ◆ Anomaly detection, classification, scoring

OTTL, transformprocessor,
attributesprocessor

resourcedetection,
k8sattributes



Types of Enrichment: OTel Collector



KubeCon



CloudNativeCon

Europe 2026

- Type 1: Self-Contained Parsing & Derivation
 - ◆ Transform, compute, or extract from existing telemetry data
- Type 2: Contextual Metadata Enrichment
 - ◆ Add infrastructure/environment context (cloud, k8s, host)
- Type 3: Reference Data Lookup
 - ◆ Enrich from files, config maps, or slow-changing external data
- Type 4: Dynamic External Enrichment
 - ◆ Real-time queries to external services (DNS, HTTP APIs, databases)
- Type 5: Cross-Event Correlation & Aggregation
 - ◆ Join or aggregate across multiple events/signals
- Type 6: Analytical & ML-Based Enrichment
 - ◆ Anomaly detection, classification, scoring

OTTL, transformprocessor,
attributesprocessor

resourcedetection,
k8sattributes

OTTL, transformprocessor



Types of Enrichment: OTel Collector



KubeCon



CloudNativeCon

Europe 2026

→ Type 1: Self-Contained Parsing & Derivation

- ◆ Transform, compute, or extract from existing telemetry data

OTTL, transformprocessor,
attributesprocessor

→ Type 2: Contextual Metadata Enrichment

- ◆ Add infrastructure/environment context (cloud, k8s, host)

resourcedetection,
k8sattributes

→ Type 3: Reference Data Lookup

- ◆ Enrich from files, config maps, or slow-changing external data

OTTL, transformprocessor

→ ~~Type 4: Dynamic External Enrichment~~

- ◆ Real-time queries to external services (DNS, HTTP APIs, databases)

→ ~~Type 5: Cross-Event Correlation & Aggregation~~

- ◆ Join or aggregate across multiple events/signals

→ ~~Type 6: Analytical & ML-Based Enrichment~~

- ◆ Anomaly detection, classification, scoring



Types of Enrichment: OTel Collector



KubeCon



CloudNativeCon

Europe 2026

→ Type 1: Self-Contained Parsing & Derivation

- ◆ Transform, compute, or extract from existing telemetry data

OTTL, transformprocessor, attributesprocessor

→ Type 2: Contextual Metadata Enrichment

- ◆ Add infrastructure/environment context (cloud, k8s, host)

resourcedetection, k8sattributes

→ Type 3: Reference Data Lookup

- ◆ Enrich from files, config maps, or slow-changing external data

→ Type 4: Dynamic External Enrichment

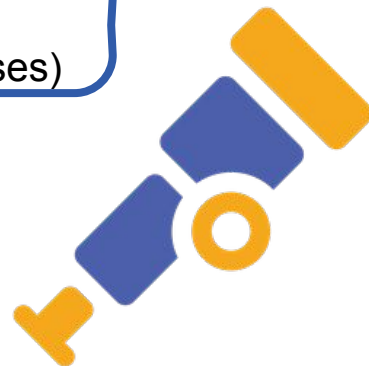
- ◆ Real-time queries to external services (DNS, HTTP APIs, databases)

→ ~~Type 5: Cross-Event Correlation & Aggregation~~

- ◆ Join or aggregate across multiple events/signals

→ ~~Type 6: Analytical & ML-Based Enrichment~~

- ◆ Anomaly detection, classification, scoring



Demand leads to Proposal



KubeCon



CloudNativeCon

Europe 2026

- Prior issues:
 - [Generic resource detector #29627](#)
 - [New component: Enrich Attributes based on key matching from yaml or csv definition #40526](#)
 - [Ability to enrich telemetry with additional resource metadata from an inventory datasource #40936](#)
 - [New component: GRPC processor/connector #20888](#)
 - [New component: Alert Manager Receiver and Exporter #18526](#)
 - [New component: DNS lookup processor #34398](#)

Demand leads to Proposal



KubeCon



CloudNativeCon

Europe 2026

- Prior issues:
 - [Generic resource detector #29627](#)
 - [New component: Enrich Attributes based on key matching from yaml or csv definition #40526](#)
 - [Ability to enrich telemetry with additional resource metadata from an inventory datasource #40936](#)
 - [New component: GRPC processor/connector #20888](#)
 - [New component: Alert Manager Receiver and Exporter #18526](#)
 - [New component: DNS lookup processor #34398](#)
- Proposal [opentelemetry-collector-contrib#41816](#) (August 6th, 2025)
 - **Generic "lookupprocessor" with built in sources + extendable**
 - 18 👍 (not vanity, just interest from the community)
 - Interest in Collector SIG meetings
 - **Volunteer sponsor: Sam DeHaan @ Grafana (@dehaansa) - Thank you ! ❤️**
 - **Accepted Dec 10th, 2025.**

Types of Enrichment: OTel Collector



KubeCon



CloudNativeCon

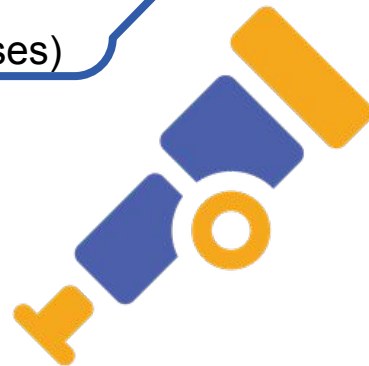
Europe 2026

- Type 1: Self-Contained Parsing & Derivation
 - ◆ Transform, compute, or extract from existing telemetry
- Type 2: Contextual Metadata Enrichment
 - ◆ Add infrastructure/environment context (cloud, k8s, host)
- Type 3: Reference Data Lookup
 - ◆ Enrich from files, config maps, or slow-changing external data
- Type 4: Dynamic External Enrichment
 - ◆ Real-time queries to external services (DNS, HTTP APIs, databases)
- ~~Type 5: Cross-Event Correlation & Aggregation~~
 - ◆ ~~Join or aggregate across multiple events/signals~~
- ~~Type 6: Analytical & ML-Based Enrichment~~
 - ◆ ~~Anomaly detection, classification, scoring~~

OTTL, transformprocessor,
attributesprocessor

resourcedetection,
k8sattributes

lookupprocessor!



lookupprocessor - Main Traits



KubeCon



CloudNativeCon

Europe 2026

- **General-purpose look up processor:** look up a key => get attributes back from a source
- **Sources:** same processor config shape, choose the source.
- **Key is any OTTL expression:** simple attribute path, concatenation, substring, etc.
- **Declarative field mapping:** each lookup specifies source field, destination attribute name, and a default value for misses
 - Scalar or map: One value or multiple fields per key w/ optional defaults
 - Record or resource: Writes to record-level or resource-level attributes

lookupprocessor - Configuration



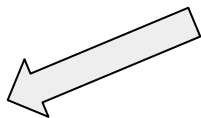
KubeCon



CloudNativeCon

Europe 2026

Source of data for the lookups



```
lookup/ip-reputation:
  source:
    type: yaml
    path: /etc/otel/lookups/ip-reputation.yaml
  lookups:
    - key: log.attributes["src_ip"]
      attributes:
        - source: risk_score
          destination: threat.risk_score
        default: unknown
```

lookupprocessor - Configuration



KubeCon



CloudNativeCon

Europe 2026

```
lookup/ip-reputation:
```

```
  source:
```

```
    type: yaml
```

```
    path: /etc/otel/lookups/ip-reputation.yaml
```

```
  lookups:
```

```
    - key: log.attributes["src_ip"]
```

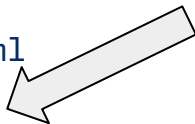
```
      attributes:
```

```
        - source: risk_score
```

```
          destination: threat.risk_score
```

```
          default: unknown
```

Lookup Key



lookupprocessor - Configuration



KubeCon



CloudNativeCon

Europe 2026

```
lookup/ip-reputation:
```

```
  source:
```

```
    type: yaml
```

```
    path: /etc/otel/lookups/ip-reputation.yaml
```

```
  lookups:
```

```
    - key: Substring(log.attributes["user.email"], IndexOf(log.attributes["user.email"], "@")+1)
```

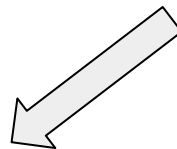
```
      attributes:
```

```
        - source: risk_score
```

```
          destination: threat.risk_score
```

```
          default: unknown
```

(can be an OTTL Value Expr)



lookupprocessor - Configuration



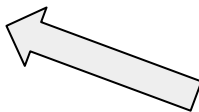
KubeCon



CloudNativeCon

Europe 2026

```
lookup/ip-reputation:
  source:
    type: yaml
    path: /etc/otel/lookups/ip-reputation.yaml
  lookups:
    - key: log.attributes["src_ip"]
      attributes:
        - source: risk_score
          destination: threat.risk_score
        default: unknown
```



Destination attributes
Fallback Value

lookupprocessor - Main Traits



KubeCon



CloudNativeCon

Europe 2026

- **General-purpose look up processor:** look up a key => get attributes back from a source
- **Sources backends:** same processor config shape, choose the source.
- **Key is any OTTL expression:** simple attribute path, concatenation, substring, etc.
- **Declarative field mapping:** each lookup specifies source field, destination attribute name, and a default value for misses
 - Scalar or map: One value or multiple fields per key w/ optional defaults
 - Record or resource: Writes to record-level or resource-level attributes

lookupprocessor - Main Traits



KubeCon



CloudNativeCon

Europe 2026

- **General-purpose look up processor:** look up a key => get attributes back from a source
- **Sources backends:** same processor config shape, choose the source.
- **Key is any OTTL expression:** simple attribute path, concatenation, substring, etc.
- **Declarative field mapping:** each lookup specifies source field, destination attribute name, and a default value for misses
 - Scalar or map: One value or multiple fields per key w/ optional defaults
 - Record or resource: Writes to record-level or resource-level attributes
- **Set of built-in sources:** yaml, dns, http, ?
- **Pluggable sources:** build your own, how?

**ALERT: INCOMING
CODE SLIDES** 

lookupprocessor - Source contract



KubeCon



CloudNativeCon

Europe 2026

```
// Describes how to build and configure a lookup source.
// Used by the processor to create a Source from config.
type SourceFactory interface {
    Type() string
    CreateDefaultConfig() SourceConfig
    CreateSource(ctx context.Context, settings CreateSettings, cfg SourceConfig) (Source, error)
}

type SourceConfig interface {
    Validate() error
}

// Runtime contract for a lookup source: the processor calls these.
type Source interface {
    Lookup(ctx context.Context, key string) (any, bool, error) // do the lookup
    Type() string // source type name (e.g. "yaml" or "dns")
    Start(ctx context.Context, host component.Host) error // optional, called when processor starts
    Shutdown(ctx context.Context) error // optional, called when processor stops
}
```

lookupprocessor - Source contract



KubeCon



CloudNativeCon

Europe 2026

```
// Function type for doing a lookup: (context, key) => (value, found, err).
type LookupFunc func(ctx context.Context, key string) (any, bool, error)

    value: Lookup result
    * Scalar for 1:1
    * map[string]any for 1:N
    * Ignored if err != nil.

    found:
    * true = key had an entry
    * false = "not found" (normal, not a failure)
    * Ignored if err != nil.

    err: Only set on real failure (e.g. network).
    * Processor logs and skips that lookup; batch continues.

// Register your source with the processor
lookupsource.NewSourceFactory("mysource", defaultConfigFunc, createSourceFunc)
```



DEMO TIME!

lookupprocessor - Progress



KubeCon



CloudNativeCon

Europe 2026

Base implementation merged to main [opentelemetry-collector-contrib#45340](https://github.com/open-telemetry/opentelemetry-collector-contrib/pull/45340)



- Includes YAML file source
- Support for Logs signal

DNS lookup source + Generic Caching (in review) [opentelemetry-collector-contrib#46114](https://github.com/open-telemetry/opentelemetry-collector-contrib/pull/46114)



- DNS source
 - PTR queries only (for now)
 - Configurable DNS server or local fallback
- Caching feature (usable by any source)
 - For any source (not just DNS)
 - Positive and negative TTL
 - Fast (~40ns/cache hit)

lookupprocessor - Backlog



KubeCon



CloudNativeCon

Europe 2026

- **New sources:**
 - HTTP source
 - Database sources
- **Enhancing existing sources:**
 - DNS source enhancements: A/AAAA queries, multi-server support
 - YAML file source enhancements: reload support, ?
- Support other signals
- Telemetry: cache hit/miss rates, lookup error rates, latency
- More benchmarks and optimizations
- **Move to alpha** 🙌

Feedback and contributions are most welcome!



KubeCon



CloudNativeCon

Europe 2026

That's it! Thank you!





KubeCon



CloudNativeCon

Europe 2026

**Contribute,
Join the community,
Come say hi!**

Have a great day!





KubeCon



CloudNativeCon

Europe 2026

**Contribute,
Join the community,
Come say hi!**

Have a great day!

Any Questions?



KubeCon



CloudNativeCon

Europe 2026

