Identifying Datatypes and Document Mappings in Elasticsearch

Aaron Rosenmund

AUTHOR EVANGELIST – SECURITY OPERATIONS

@arosenmund   www.AaronRosenmund.com

Overview

Now you have data

Bend it to your use case

- Field Data Types
- Index Mapping
- Index Templates

Discovering the Basics

`Logon`	◀ Free text search
`Logon Type: *`	◀ Searching a specific field
`Fieldname: “value”`	◀ Searching by values within a field
`Fieldanme: *$*`	◀ Text pattern matching
`Fieldname_IP: 10.0.0.0/24`	◀ Working with IPs
`AND, OR, NOT`	◀ Logical functions

Demo

Search demo.

Field Data Type

Defines the nature or type of the data within a field for the purpose of search functionality. A close analogue to variable types in programming languages.

Date

String

- number
- URL
- Boolean

Number

- Standard integer
- Bytes
- Ranges

Geo_point

IP

- Comes in many formats, important for time series information
- String type for text fields
- Displayed for different purposes
- True/False can be in the format of text but reflect a boolean
- Numbers are stored in the fields as various number based variable types
- But can be formatted to represent different use cases
- Leveraged for maps, converted to lat, long
- Structured data that is tokenized to support additional functionality

A Security Analyst’s Relationship with Data

Network Data: IPs, Bytes, Geo Locations, Protocols

Application Logs: URLs, Truncated Strings, Error Codes

Endpoint Logs: Logon Type, Process ID, Thread ID

Demo

Combine the index patterns and the quick search demo!

Index Mapping

Assigns the ingested data to a field or multiple fields, as well as assigning the type by which the data is stored within that field.

Creating an Index Map

```
PUT /securityinfo/_mapping
{
  “properties”: {
    url.orignal: {         #refers or “maps” directly to the field names ingested
      “type”: “keyword”
}}}
```

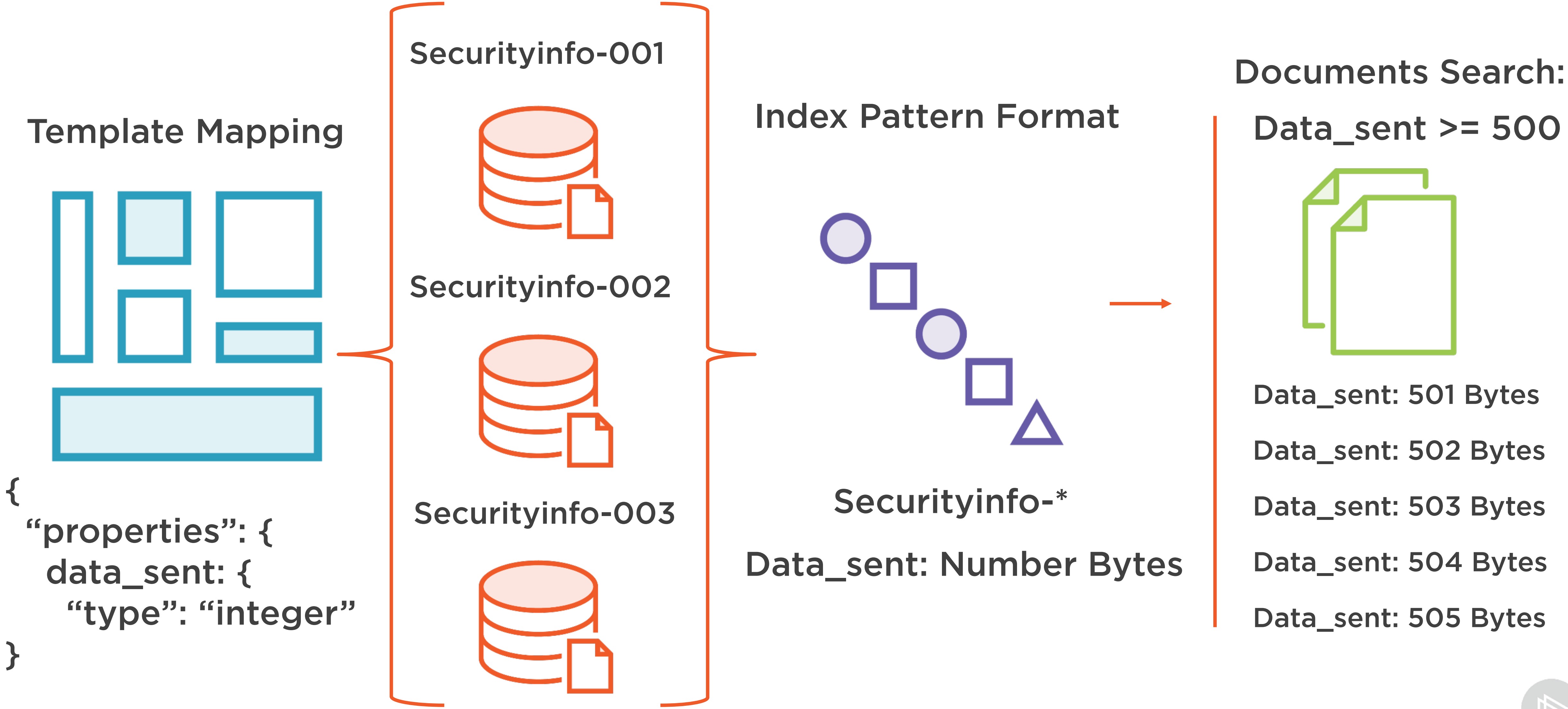
Demo

Look at existing index mappings, and how to create a new one inside index templates single index vs the template.

Index Template

Defines settings and mappings for an index before it is created.

Diagram for Templates vs. Index Maps



Template Mapping

```
{
  “properties”: {
    data_sent: {
      “type”: “integer”
}
```

Securityinfo-001

Securityinfo-002

Securityinfo-003

Index Pattern Format

Securityinfo-*

Data_sent: Number Bytes

Documents Search:

Data_sent >= 500

Data_sent: 501 Bytes

Data_sent: 502 Bytes

Data_sent: 503 Bytes

Data_sent: 504 Bytes

Data_sent: 505 Bytes

Demo

Look at existing index mappings, and how to create a new one inside index templates single index vs the template.

ECS

Normalize

Elastic Common Schema

Normalizing field names across input sources:

destination.ip

host.os

http.request.method

[Elastic Common Schema (ECS) Reference [1.7] | Elastic]

Summary

Field types and formats

Mapping data types to fields

Leveraging templates for index config

Elastic Common Schema