elastic

Daily Elastic Observability B(y|i)te

What is the Elastic Common Schema?

David Pilato (@dadoonet)

ECS: Elastic Common Schema

- ECS is an open source specification
  - https://www.elastic.co/guide/en/ecs/current/index.html
  - https://github.com/elastic/ecs

Why ECS?

```
src:10.42.42.42 OR client_ip:10.42.42.42 OR apache2.access.remote_ip:10.42.42.42 OR
context.user.ip:10.42.42.42 OR src_ip:10.42.42.42
```

Why ECS?

```
src:10.42.42.42 OR client_ip:10.42.42.42 OR apache2.access.remote_ip:10.42.42.42 OR
context.user.ip:10.42.42.42 OR src_ip:10.42.42.42
```

```
source.ip:10.42.42.42
```

elastic

source.ip

Source fields capture details about the sender of a network exchange/packet. These fields are populated from a network event, packet, or other event containing details of a network transaction.

Field	Description	Level
source.ip	IP address of the source (IPv4 or IPv6). type: ip	core

https://www.elastic.co/guide/en/ecs/current/ecs-source.html

elastic

host.ip

A host is defined as a general computing instance.

ECS host.* fields should be populated with details about the host on which the event happened, or from which the measurement was taken. Host types include hardware, virtual machines, Docker containers, and Kubernetes nodes.

host.ip	Host ip addresses. type: ip Note: this field should contain an array of values.	core

https://www.elastic.co/guide/en/ecs/current/ecs-host.html

elastic

Contributing

166 lines (140 sloc) | 4.92 KB — Raw | Blame

```yaml
---
- name: host
  title: Host
  group: 2
  short: Fields describing the relevant computing instance.
  description: >
    A host is defined as a general computing instance.

    ECS host.* fields should be populated with details about the host on which
    the event happened, or from which the measurement was taken.
    Host types include hardware, virtual machines, Docker containers, and Kubernetes nodes.
  type: group
  fields:

    - name: hostname
      level: core
      type: keyword
      short: Hostname of the host.
      description: >
        Hostname of the host.

        It normally contains what the `hostname` command returns on the host machine.
```

https://github.com/elastic/ecs/blob/master/schemas/host.yml

elastic

In action

Elastic Common Schema

security analytics

metrics

monitoring

infra

logging

apm