Introduction to CEE v0.6

William Heinbockel
Tom Graves

{heinbockel,tgraves}@mitre.org

First things first

- CEE = Common Event Expression

- CEE Specifications released (v0.6)
- Initial CEE Repository available
- Latest CEE Information available at: http://cee.mitre.org

Who Supports CEE?

- US Government
  - DoD, DHS
  - NIST
- Vendors
  - Microsoft, Red Hat, Cisco, McAfee, Tripwire, AlienVault, Syslog-NG, rsyslog, ArcSight
- International
  - NATO NC3A
  - Canada DRDC

CEE OVERVIEW

Background

- **Event**
  - **a single occurrence within an environment, usually involving an attempted state change**
- **Event Record**
  - **a collection of event fields that, together, describe a single event**
- **Log**
  - **a collection of event records**

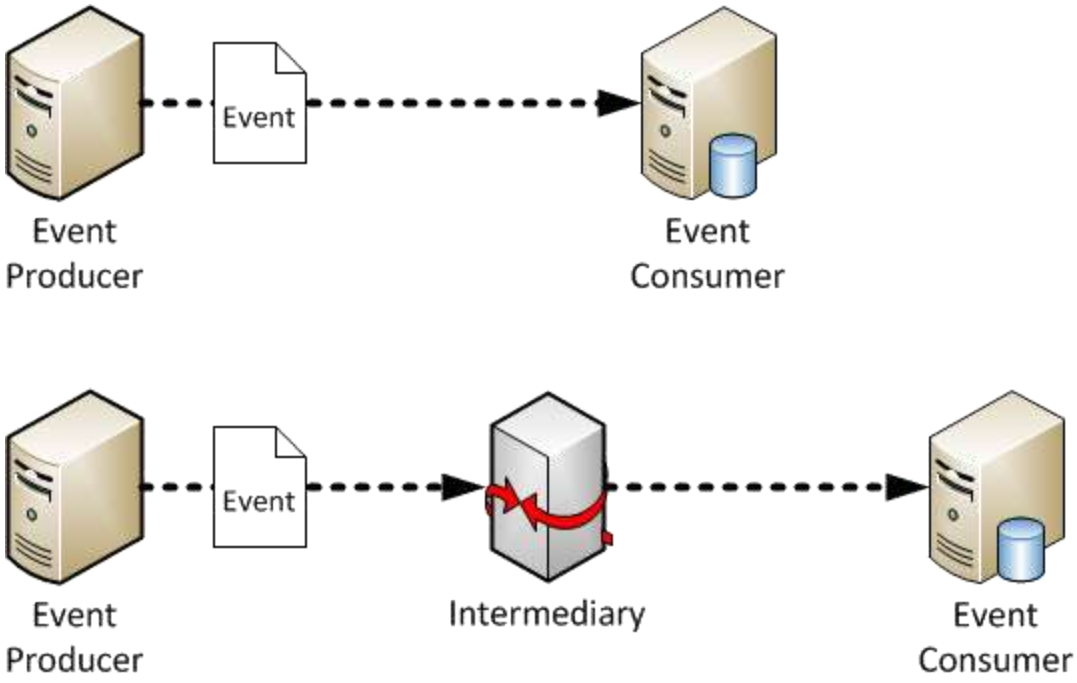
*** From this point, "event" is used as shorthand for "event record" ***

Design Goals

- Open, Neutral Standard
- Efficiency
- Simplicity
- Compatibility
  - Work in existing event environments
  - Work with existing products

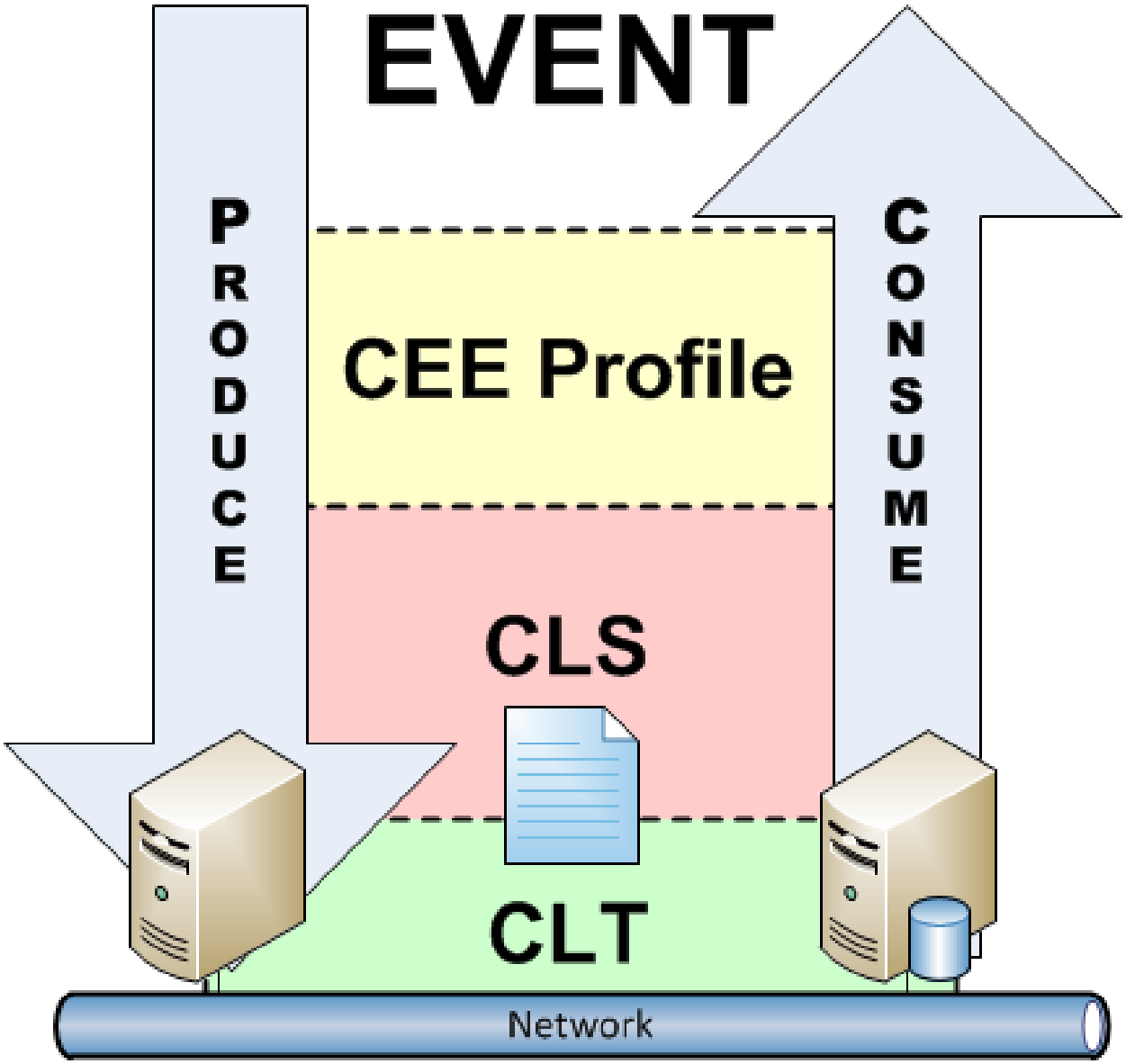
Event Management Environment

- Event Producer
- Event Consumer
- Intermediate System
  - Event Relay
  - Guard



Problem

- Effective analysis requires parsing and comprehension
- Parsing events is hard
- Comprehending events is harder
  - What "type" of event is it?
  - What does the event mean?
- Limited secure, resilient log protocols



CLS Overview

- **CLS Specification**
  - **Defines a set of base field value types**
  - **Defines a Generic CEE Event Record Structure**
  - **CLS Encoding Requirements**
- **CLS Encoding Specification**
  - **Defines encodings to/from various syntaxes**
  - **XML**
  - **JSON**
- **Event Augmentations**

CLS Event Record

- **Events are a sequence of fields**
- **Fields have a name and a sequence of values**
- **Every event must have 6 required core fields**
  - ***id* :: Event ID**
  - ***time* :: Event start time**
  - ***action* :: Primary action of the event (login, read)**
  - ***status* :: Result of the event action (success, fail)**
  - ***p_sys_id* :: ID of the producing system**
  - ***p_prod_id* :: ID of the producing product**

Example (XML)

```
<CEE xmlns="http://cee.mitre.org">
  <Event>
    <id>example-event-2</id>
    <time>2011-04-01T12:01:00-05:00</time>
    <action>download</action>
    <status>-</status>
    <p_sys_id>host.example.com</p_sys_id>
    <p_prod_id>product</p_prod_id>
    <Field name="tags"><tag>web</tag></Field>
    <Field name="file_name"><str>example.txt</str></Field>
    <Field name="file_data">
      <binary>RmlsZSBDb250ZW50Li4uAAo=</binary>
    </Field>
  </Event>
  <Augmentation order="1">
    <time>2011-04-01T14:11:53-04:00</time>
    <status>success</status>
    <p_sys_id>relay.example.com</p_sys_id>
    <p_prod_id>cee-relay</p_prod_id>
    <Field name="tags"><tag>hipaa</tag></Field>
  </Augmentation>
</CEE>
```

Example (JSON)

{"Event":{"id":"example-event-2",
"time":"2011-04-01T12:01:00-05:00","action":"download",
"status":[],"p_sys_id":"10.10.0.1",
"p_prod_id":"process","file_name":"example.txt",
"tags":"web","file_data":"b|RmlsZSBDb250ZW50Li4uAAo="},
"Augmentation":[{"time":"2011-04-01T14:11:53-04:00",
"status":"success","p_sys_id":"relay.example.com",
"p_prod_id":"cee-relay","tags":"g|hipaa"}]}

CEE Profile

- **CEE Profile Specification**
  - **Documents the features and usage of a CEE Profile document**
- **CEE Profile XML Schema (XSD)**
- **CEE Profile Repository**
  - **Collection of CEE Profile XML Documents**

Development (FY12+)

- Software implementations & libraries
- Product Conformance
- Expand repository
  - More field and tag definitions
  - Validation
  - Add i14n support
- Build CEE Profiles
  - Common functionalities
  - Profiles for audit requirements: HIPAA, Common Criteria, PCI-DSS