CEE Status Update

John Wunder
Tom Graves

cee@mitre.org

First things first

- Common Event Expression
  - Common structure and vocabulary for event reporting
- http://cee.mitre.org
  - Specifications
  - Mailing lists
  - Other documents, FAQ, etc.
- Current version is 1.0-alpha
  - 1.0-beta will be released soon

CEE BASICS

Terms

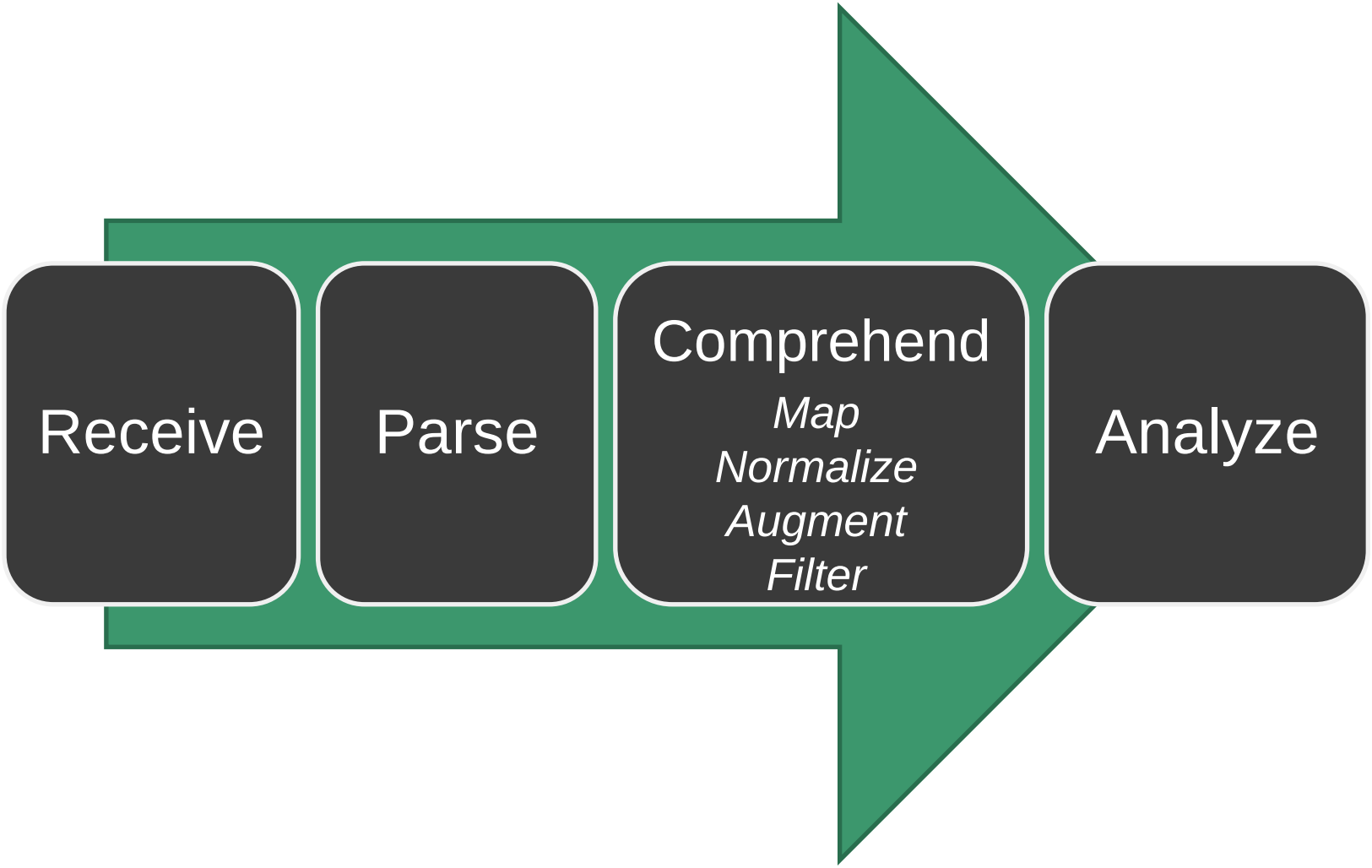
- Event
  - a single occurrence within an environment, usually involving an attempted state change
- Event Record
  - a collection of event fields that, together, describe a single event
- Log
  - a collection of event records

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

Design Goals

- Openness
- Efficiency
- Simplicity
- **Compatibility**
  - **Work in current event environments**
  - **Work with existing products**

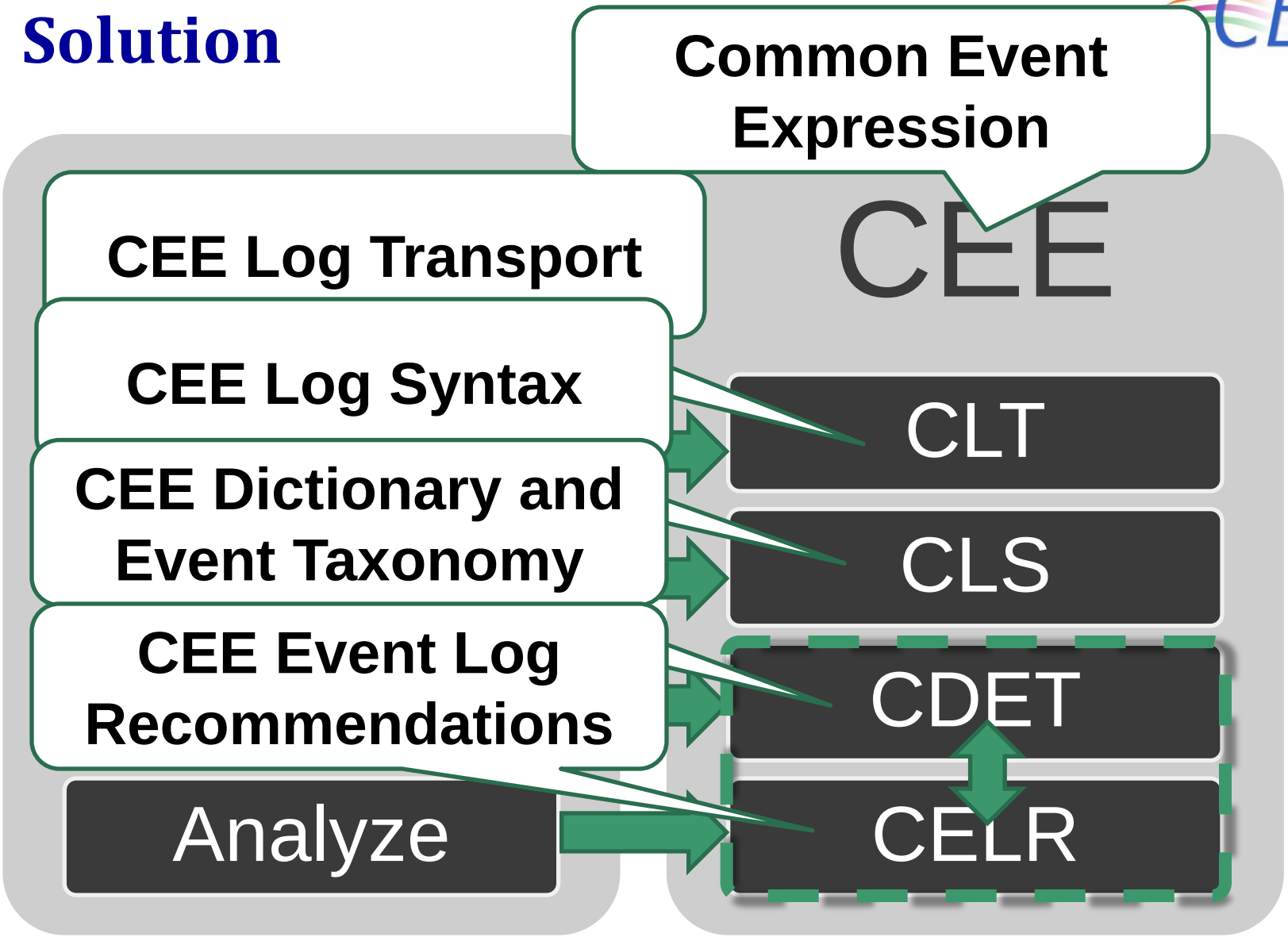
Consuming Events



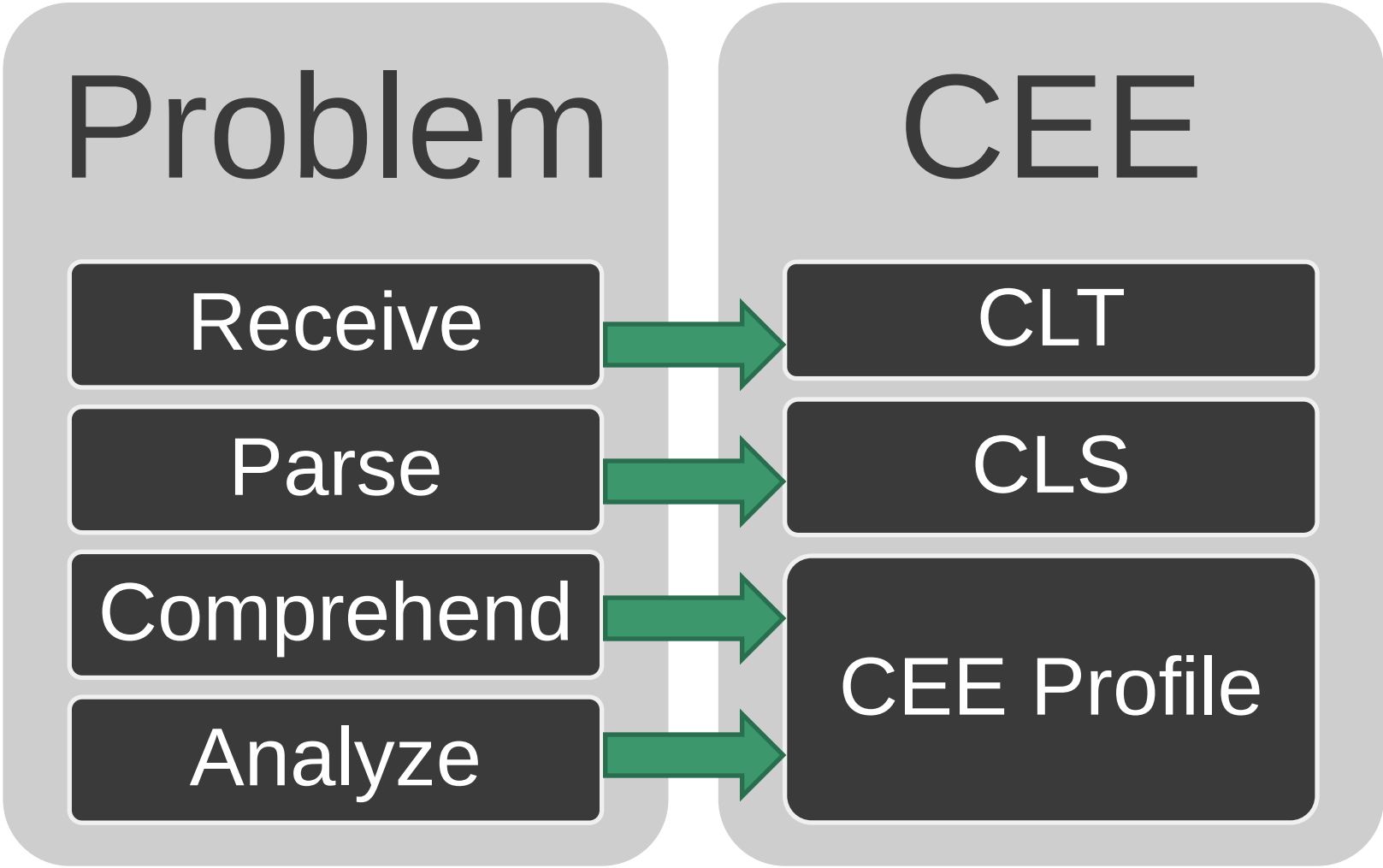
Problem

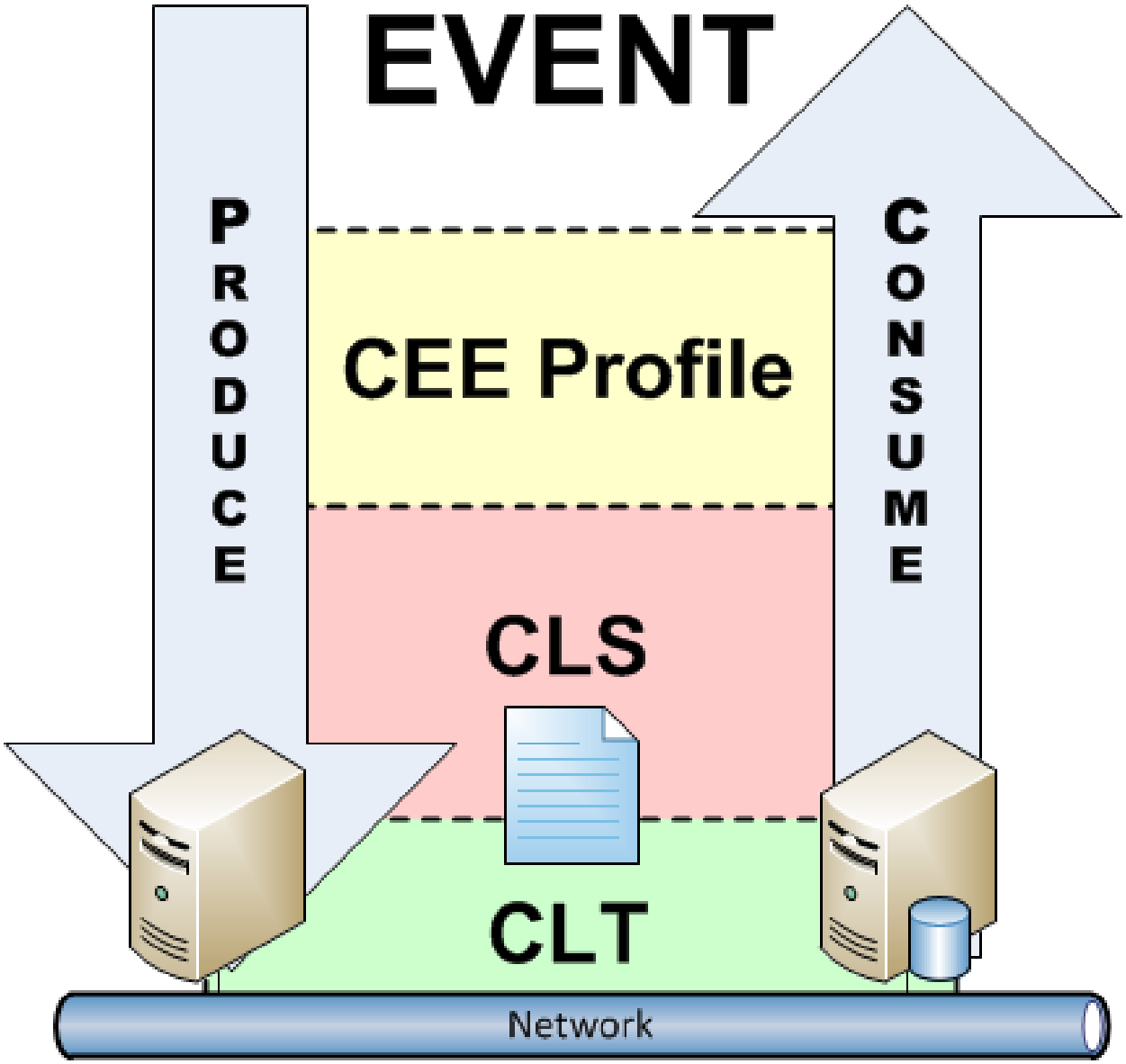
- Effective analysis requires parsing and comprehension
- Parsing events is hard
- Comprehending events is harder
  - What "type" of event is it?
  - What does the event mean?
- Limited secure, resilient log protocols

Solution



New Approach





EVENT MODELING

How CEE views events

Field & Tags

- Events are just a series of fields and tags
- **Field**: a name and value(s) associated with an object or property of an event
- **Tag:** the event "type"
  - action tags: login, remove, read, block, search
  - status tags: success, fail, error
  - others: HIPAA, audit, critical, warning, info
  - Conceptually, tags are just fields with enumerated values used to classify events

- *Example: "User jwunder logged on"*

CEE LOG SYNTAX

Structured Encoding for Event Records

CLS Overview

- CLS Event Specification
  - Defines a generic CEE Event Record Structure
- CLS Encoding Specifications
  - Define encodings to and from this structure to two common formats: JSON and XML
  - Both formats represent same data but have some differences
    - Validation capabilities
    - Message size
    - Adoption community
    - Use cases

Event Record

- Field list
  - From CEE Field Dictionary, referenced profile, or custom
  - Fields may be optional or required based on profile
- Optional classification into the CEE Taxonomy

Example (JSON) - NOTIONAL

```
{
  "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",
  "file_data":"RmlsZSBDb250ZW50Li4uAAo=“
}
```

EVENT COMPREHENSION & ANALYSIS

CEE Profiles

CEE Profile Overview

- CEE Profile Specification
  - Documents the features and usage of a CEE Profile document
- CEE Core Profile
  - Official field dictionary and taxonomy
  - In itself a profile
  - The “base” profile that all others inherit from
- CEE Profile Repository
  - Collection of CEE Profile XML Documents

CEE Profile Types

- CEE Core Profile
  - Only one, provided by CEE
  - Core field dictionary and taxonomy
- Function Profile
  - Defines the event profiles for events associated with a specific function
  - Example: Firewall, Session Management Profile
- Product Profile
  - Defines event profiles for events that a specific product may generate

SHARING CEE EVENTS

Common Log Transport (CLT)

CLT Overview

- CLT Requirements
  - Mandatory and optional requirements for log transport protocols
  - Divided into conformance levels
- CLT Protocol Mappings
  - How to send CLS Encoded CEE Events over specific protocols
  - Currently just syslog (RFC3164, RFC5424)

CLT Protocol Mapping

- Specification defines how to encode a CEE Event and transmit over a protocol
- CLT Mapping: Syslog
  - Encode CEE Event using CLS JSON Spec
  - Add `@cee:` flag
  - Place in the end of the Syslog message area

CEE-over-Syslog Example

```
<165>1 2011-04-01T17:01:20Z 10.10.0.1 process -
       example-event-1 @cee:{"Event":{"id":"example-event-1",
        "time":"t|2011-04-01T17:00:00.123456789Z","action":
        "g|remove","status":"g|failed","p_sys_id":"host.example.com",
        "p_prod_id":"cpe:2.3:Vendor:Product:Version:*:*:*:*:*:*",
        "file_name":"example.txt","proc_dur":"d|PT.0014S",
        "sess_id":"user1"}}
```

```
<0>Apr  4 17:01:20 10.10.0.1 process[35]: @cee:{"Event":{
       "id":"example-event-2","time":
       "2011-04-01T17:00:00.123456789Z","action":"download",
       "status":"success","p_sys_id":"host.example.com",
       "p_prod_id":"cpe:2.3:Vendor:Product:Version:*:*:*:*:*:*",
       "example_internal_id":10000,"proc_dur":"PT.0014S",
       "sess_id":12345,"file_name":"example.txt",
       "file_content":"b|RmlsZSBDb250ZW50Li4uAAo="}}
```

WHAT'S NEXT?

The Road to CEE 1.0

Where are we?

- Architecture and syntax are close to finalized
- Still work to go on core spec for 1.0-final
  - Profile specification (?)
  - CEE Core Profile content (field dictionary and taxonomy)
- More work on profiles
  - Profiles for popular use cases, products, and audit requirements
  - Identify further CEE Profile requirements and iterate specification
- Do we need more CLT Mappings?
  - To support validation, high assurance, etc.

Ongoing Activities

- Adoption program
  - Need support in vendor products
    - Reference implementation
    - Lumberjack
    - libumberlog
- Validation program
  - What do you validate? How do you validate?
- Versioning policy
  - How is the spec versioned?
  - Is the Core Profile versioned w/ the spec?
- Stand up profile repository

Integration into other efforts

- CybOX
  - Correlation across audit and threat communities
- EMAP
  - Provide recommendations on top of CEE?

Questions?

cee.mitre.org

cee@mitre.org