Standardizing Event Management

CEE and EMAP Specifications

NIST ITSAC, Baltimore, MD
27-29 September 2010

William Heinbockel
heinbockel@mitre.org

Motivation

- **Products use different event formats**
- **Hard to combine and correlate events**

- **Example:**

```
header,103,2,execve(2),,Mon Jan 25 11:38:31 2010,
+ 52420844 msec path,/usr/bin/ls attribute,100555,
bin,bin,8388608,0,0 subject,user123,root,other,root,
other,8722,408,0 0 hostname1 return,success,0
```

More Motivation

- **Cryptic Records**

```
Sep 01 08:11:53 Last message repeated 5 times
```

- **Missing and Inconsistent Event Details**

```
Apr 10 12:31:34 host sshd[16682]: error: PAM:
  Authentication failure for user from
  remote-pc.mitre.org

Apr 10 12:31:39 host sshd[16701]: Accepted
  keyboard-interactive/pam for user from
  192.168.0.1 port 2880 ssh2
```

Example

You are in an accident and need to describe it in a police report…

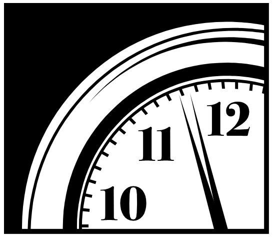
Image by Shuets Udono: http://acobox.com/node/239361. CC by-sa

Reporting Events

Event

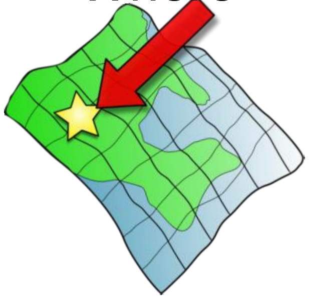
=

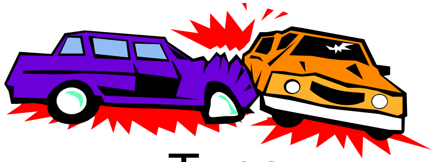
When



+

Where





Type

+

Initiator

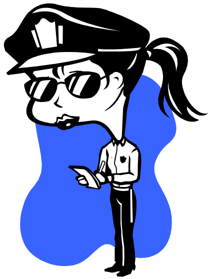
+

Target

+

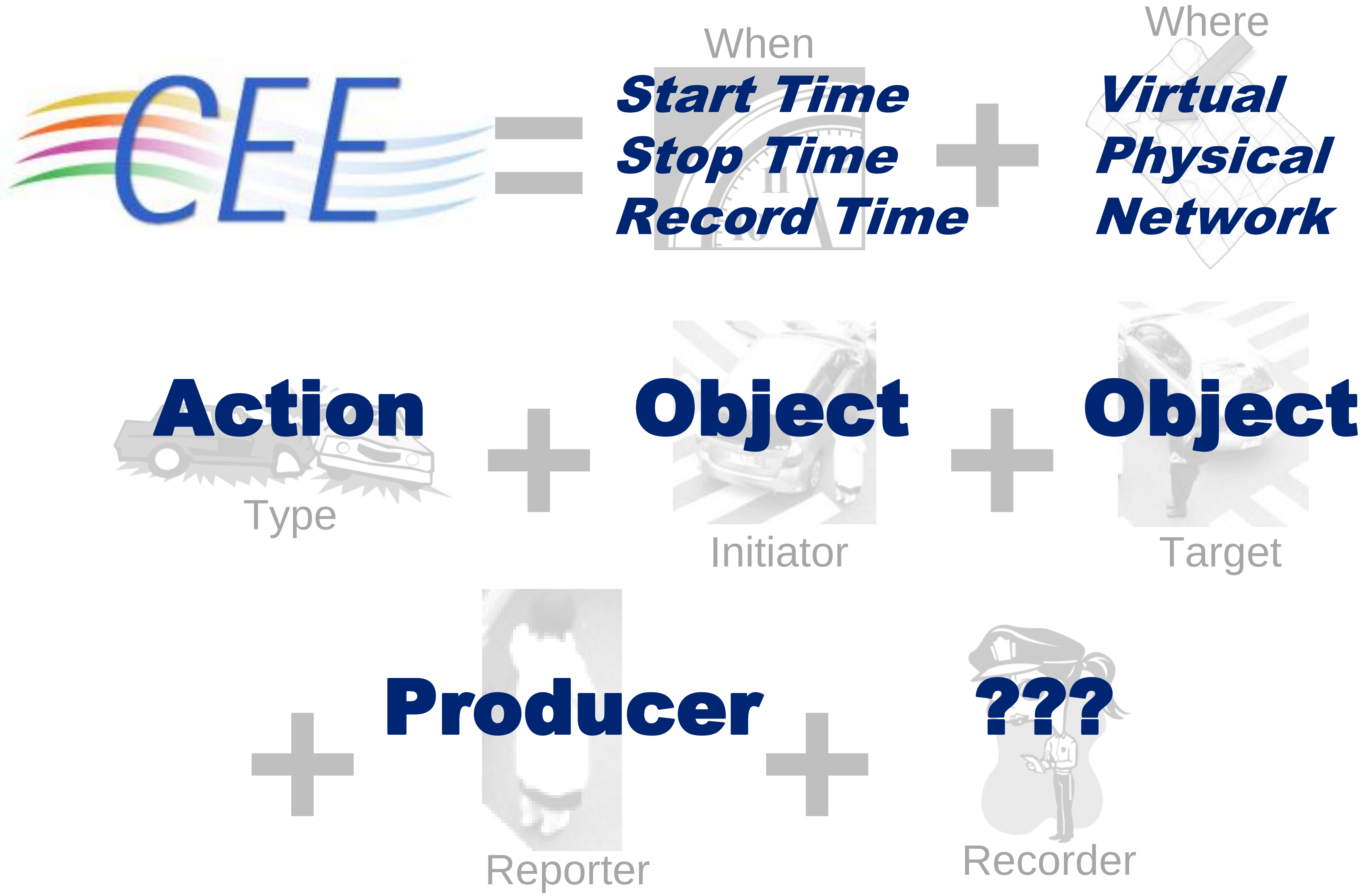
Reporter

+



Recorder

Recording Events



CEE =

When

Start Time
Stop Time
Record Time

+

Where

Virtual
Physical
Network

Action

Type

+ **Object**

Initiator

+ **Object**

Target

+ **Producer**

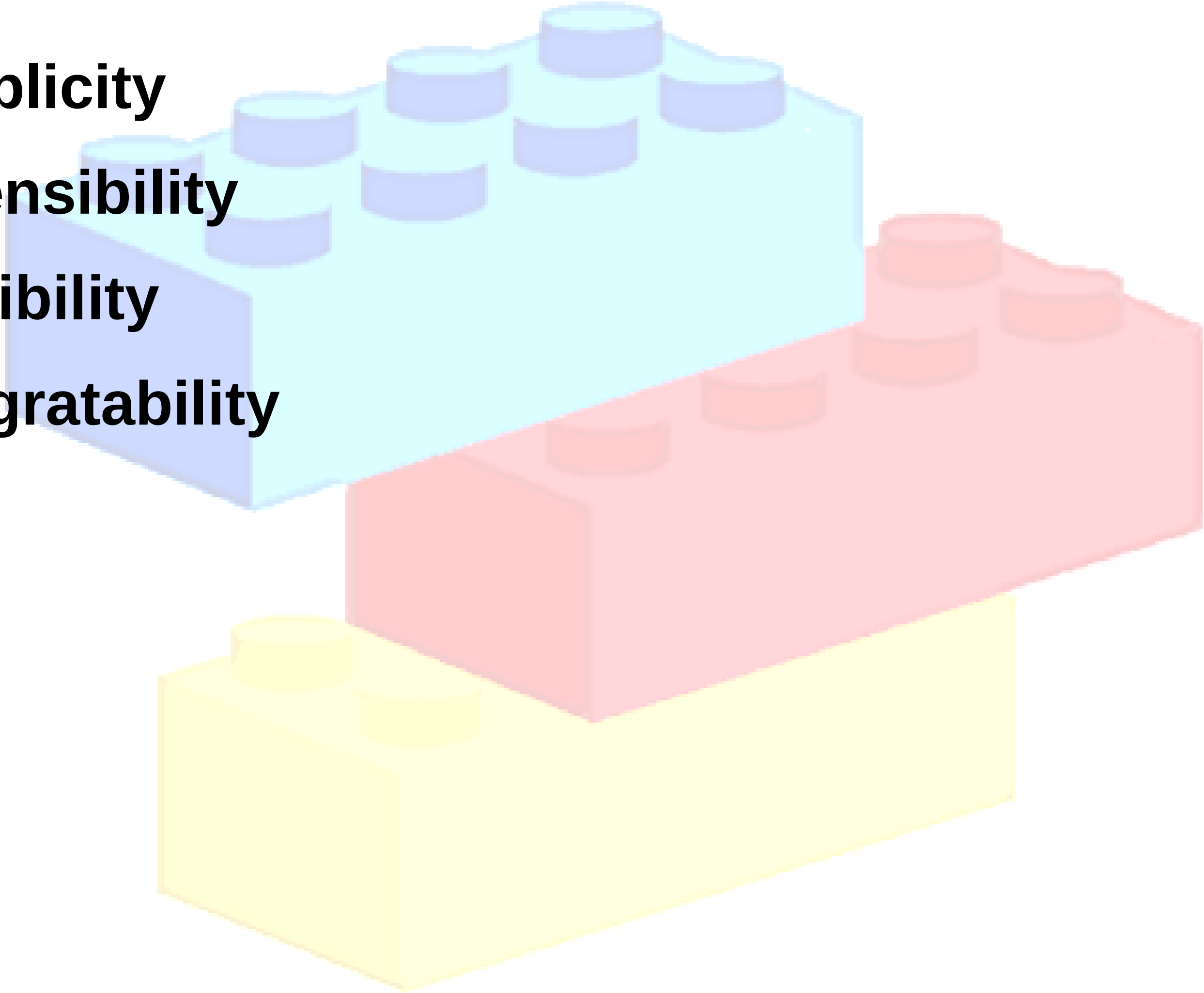
Reporter

+ **???**

Recorder

Approved for Public Release. Case 10-3537. Distribution Unlimited

CEE Goals



- Simplicity
- Extensibility
- Flexibility
- Integratability

CEE Members

- Microsoft
- RedHat
- ArcSight
- Cisco
- US Department of Defense
- NIST
- NATO Consultation, Command and Control Agency (NC3A)
- and many more…

Example

- **What if I wanted to describe this presentation?**
  - **Type of Event:** What is happening?
  - **Temporal:** Time, Timezone, Duration
  - **Location:** Hotel, Room Information
  - **Presenter:** Name, Organization, Email, Phone
  - **Observer Details:** Audience Count
  - **Presentation Information:** Title, Topic, Slide count, Previous/Next Presentation
  - **Other:** Importance, Related Topics
- **These fields are defined in the CEE Dictionary**

Example (Cont.)

- … and represented using a CEE Syntax

```
<Event>

  <Timestamp>2010-09-27T13:30:00-05:00</Timestamp>
  <EventAction>present</EventAction>

  <LocationType>Conference Room</LocationType>
  <LocationName>Baltimore Convention Center</LocationName>
  <LocationCity>Baltimore</LocationCity>

  <PersonName>William Heinbockel</PersonName>
  <PersonEmail>heinbockel@mitre.org</PersonEmail>

  <PresentationTitle>Standardizing Event Mgt</PresentationTitle>
  <PresentationDuration>PT30M</PresentationDuration>

</Event>
```

Representing Events

- **Need many syntax options to support different environments**
  - **Binary :** Small and fast for maximum resource utilization
  - **Syslog, JSON, XML (min) :** Minimal structured event representation that is easy to use
  - **XML (full) :** Formal XML representation with full XML Schema definitions allowing for event XML validation

However…

- A standardized event format only goes so far

THE BUFFALO NEWS CAGLECARTOONS.COM ©2009 ADAM ZYGLIS
WE'RE IN A RECESSION. IT MAY BE A SMART TIME TO BUY...
BUY?!
BYE. ARE YOU LEAVING?
DID SHE GET FIRED?
LAYOFFS! THIS IS SO DE-PRESSING!
DEPRESSION?
WE'RE IN A DEPRESSION?
SELL! SELL!

We need context!

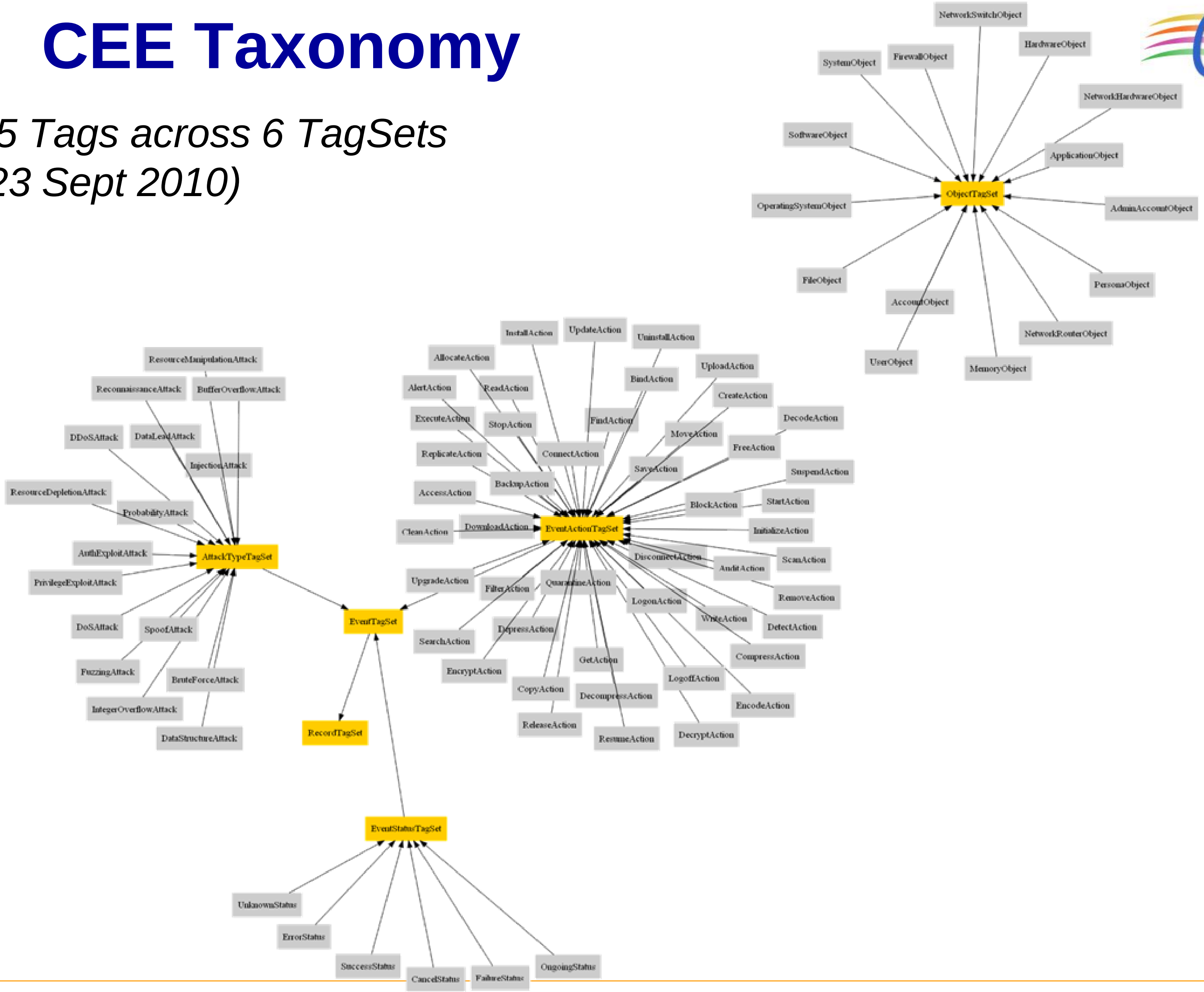
- CEE Taxonomy defines the type of event
- Defines common terms and relations
  - Built on RDF, OWL, SKOS concepts

```
<EventActionTagSet> rdf:type <TagSet> ;
      rdfs:subClassOf <skos:Concept> .

<LogonAction> rdf:type <Tag> ;
      cee:TagSet <EventActionTagSet> ;
      cee:definition “a successful authentication attempt
                  resulting in the opening of a new session”@en ;
      cee:prefLabel “logon”@en ;
      cee:altLabel “login”@en ;
      cee:related <AuthenticationAction> ;
      cee:opposite <LogoutAction> .
```

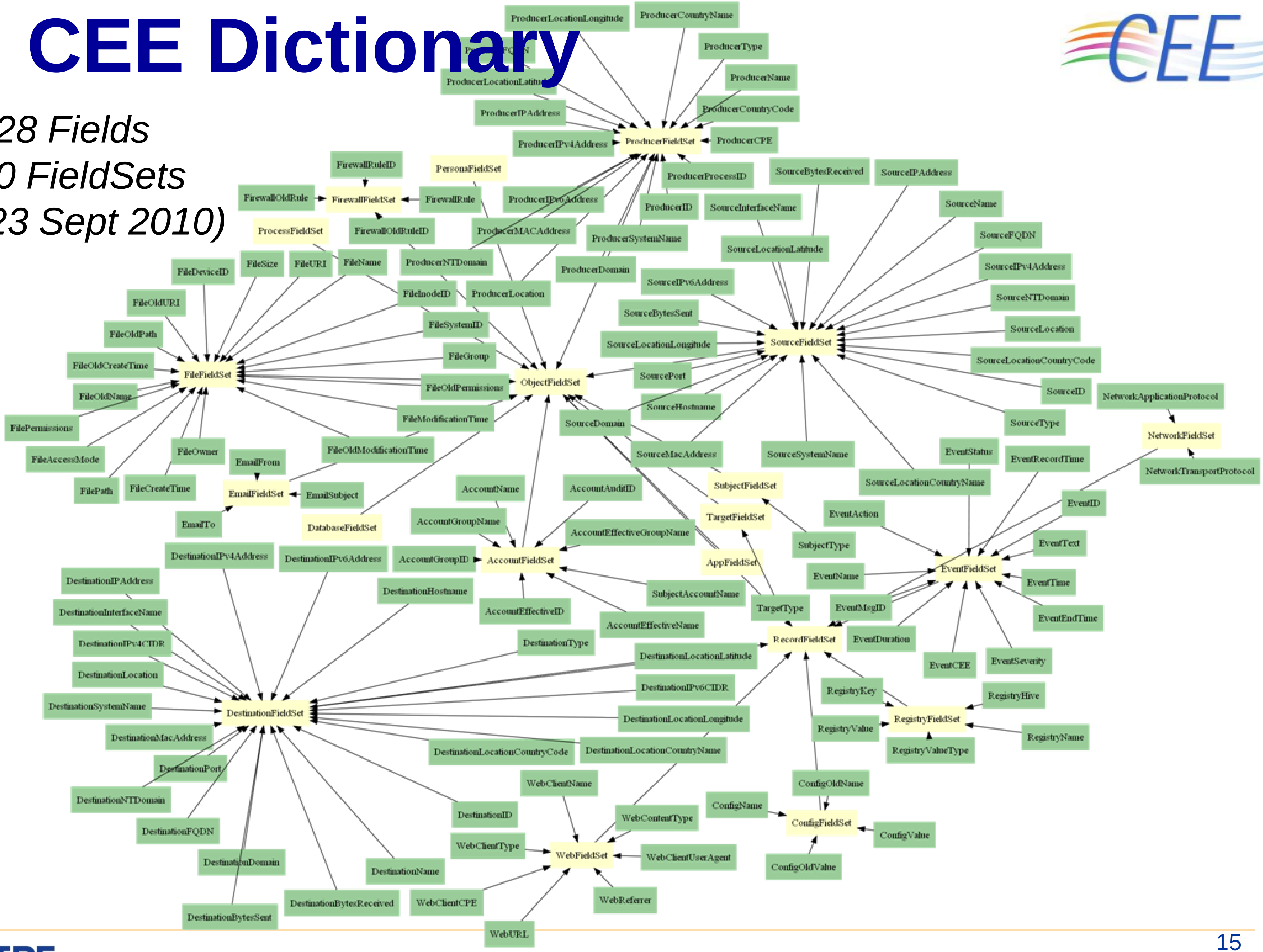
CEE Taxonomy

85 Tags across 6 TagSets
(23 Sept 2010)

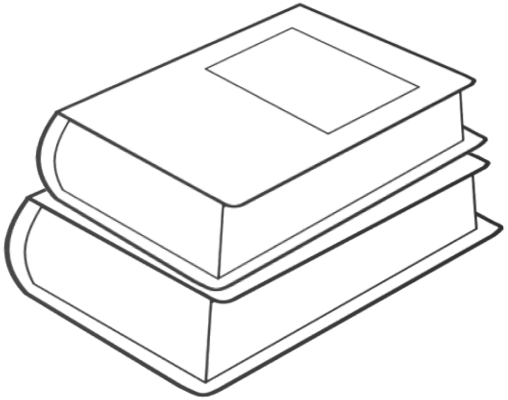


CEE Dictionary

128 Fields
20 FieldSets
(23 Sept 2010)



CEE Organization



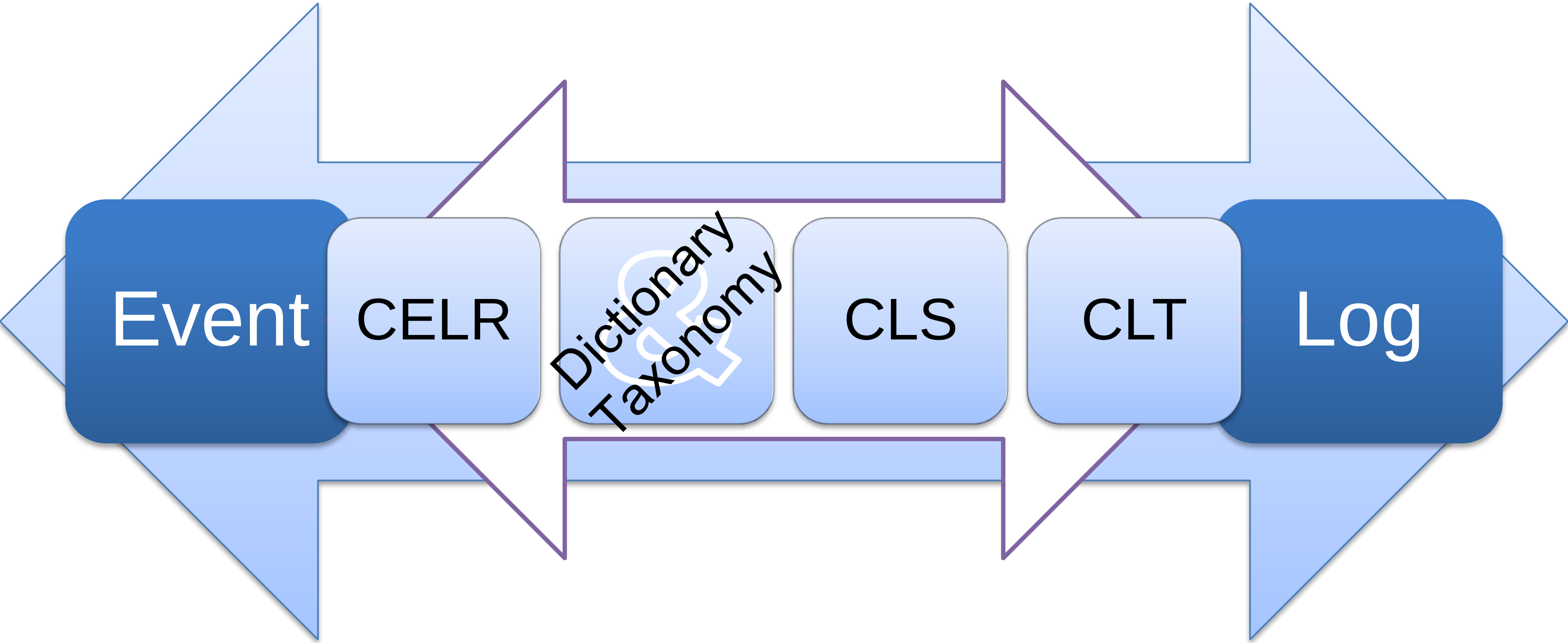
Dictionary & Taxonomy

Transport (CLT)

Syntax (CLS)

Recommendations (CELR)

CEE Process



Solved

- Products use different ev formats
- Hard to combi e events

Solution: CEE

- Example:

```
header,103,2,execve(2),,Mon Jan 25 11:38:31 2010,
+ 52420844 msec path,/usr/bin/ls attribute,100555,
bin,bin,8388608,0,0 subject,user123,root,other,root,
other,8722,408,0 0 hostname1 return,success,0
```

Solution: CEE!

```
<Event>
    <EventTime>2010-01-25T11:38:31.524208</EventTime>
    <EventAction>execute</EventAction>
    <EventStatus>success</EventStatus>
    <EventMsgID>execve(2)</EventMsgID>
    <FilePath>/usr/bin/ls</FilePath>
    <FilePermissions>100555</FilePermission>
    <FileOwnerName>bin</FileOwnerName>
    <FileGroupName>bin</FileGroupName>
    <FileSystemID>8388608</FileSystemID>
    <FileInodeID>0</FileInodeID><FileDeviceID>0</FileDeviceID>
    <AccountAuditID>user123</AccountAuditID>
    <AccountEffectiveName>root</AccountEffectiveName>
    <AccountEffectiveGroupName>other</AccountEffectiveGroupName>
    <AccountName>root</AccountName>
    <AccountGroupName>other</AccountGroupName>
    <ProducerProcessID>8722</ProducerProcessID>
    <AuditSessionID>408</AuditSessionID>
    <ProducerSystemName>hostname1</ProducerSystemName>
  </Event>
```

Too Verbose?

```
{ "Event" : {
    "timestamp" : "2010-01-25T11:38:31.524208",
    "action" : "execute",
    "status" : "success",
    "msgid" : "execve(2)",
    "file_path" : "/usr/bin/ls",
    "file_perm" : "100555",
    "file_own" : "bin“, "file_grp" : "bin",
    "file_sysid" : 8388608,
    "file_inode" : 0,
    "acct_audit" : "user123",
    "acct_effname" : "root",
    "acct_effgrp" : "other",
    "acct_name" : "root",
    "acct_grp" : "other",
    "prod_procid" : 8722,
    "sessionid" : 408,
    "prod_sysname" : "hostname1" }}
```

Developing CEE Data

- ***Step 1***: **Identify event types**
- ***Step 2***: **Identify associated event data**
- ***Step 3***: **Integrate into CEE Dictionary and Taxonomy**
  - **Option 1: Merge event data into the existing CEE Dictionary & Taxonomy**
  - **Option 2: Add the data into a domain- or product-specific profile**
- ***Step 4*** **(optional): Build event profiles for the events identified in Step 1**
  - **CELR Profiles are used for event validation and guidance**

Status

- Initial documents published for review (v0.5)
  - CEE Architecture Overview
  - CEE Dictionary & Event Taxonomy Specification
- Upcoming releases
  - CEE Log Syntax Specification
  - CEE Event Log Recommendations Specification
- Changes being applied to next draft release (v0.6)

EMAP

- Event Management Automation Protocol
- Related to SCAP
- Goal

To create interoperability specifications to enable standardized content, representation, exchange, correlation, searching, storing, prioritization, and auditing of event records within an organizational IT environment

Where to go from here?

- EMAP requires a normalized event representation format
  - Everything builds upon CEE
- EMAP Questions
  - How does EMAP support legacy log formats?
  - Which events pose more organizational risk?
  - What is the relationship between EMAP and existing audit policy and regulatory requirements (e.g., FISMA, HIPAA, PCI-DSS, Sarbanes-Oxley)?
  - How can organizations quickly write and distribute new filters, correlation rules or search patterns?

Questions?

William Heinbockel
heinbockel@mitre.org

http://cee.mitre.org

BACKUP SLIDES

Event Management Challenges

- **Systems must be able to understand the syntax of the event records that they receive.**
- **Systems must be able to parse the data in the fields of the event records that they receive.**
- **Systems must be able to understand the meaning of the data in the fields of the event records that they receive.**

Event Management Challenges (2)

- **Systems must be able to understand the event that an event record represents.**
- **Event consumers need a way of communicating a desired set of event records and fields to event producers.**
- **Event producers need a way of communicating the set of event records and fields that a product generates, to event producers.**

Event Management Challenges (3)

- Event consumers must receive event records from event producers, with all CEE-required metadata intact.