# Explaining CEE

## The Need for Event Standards

**11 September 2008**



Approved for Public Release 08-1313



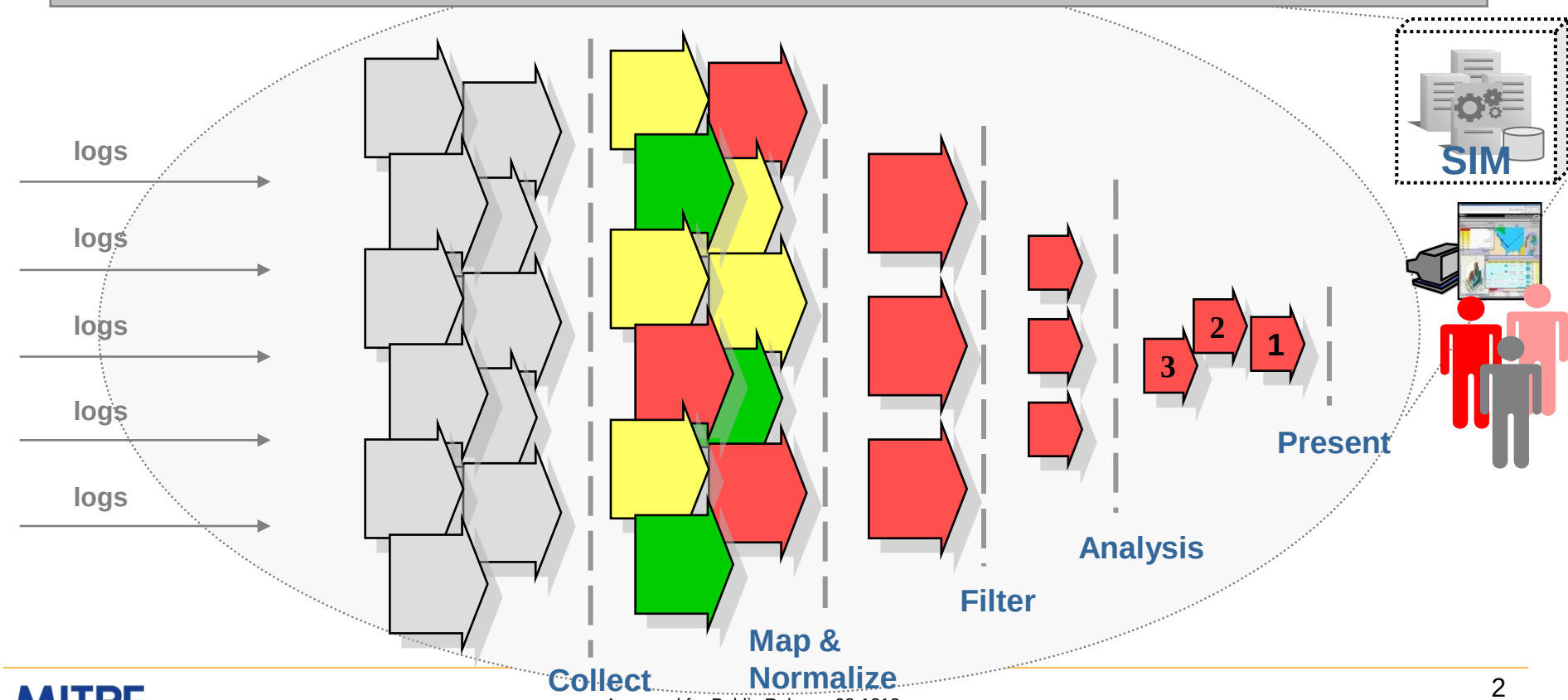
© 2008 The MITRE Corporation. All rights reserved

# Background

**The 'Log' Problem**

**MITRE was involved with research related to Network Operations and Security Center (NOSC) products for security information processing. This effort led to involvement with the analysis of Security Information Management (SIM) Systems.**

**While SIMs show a strong promise for NOSCs, we identified some limitations that would affect its sucess.**



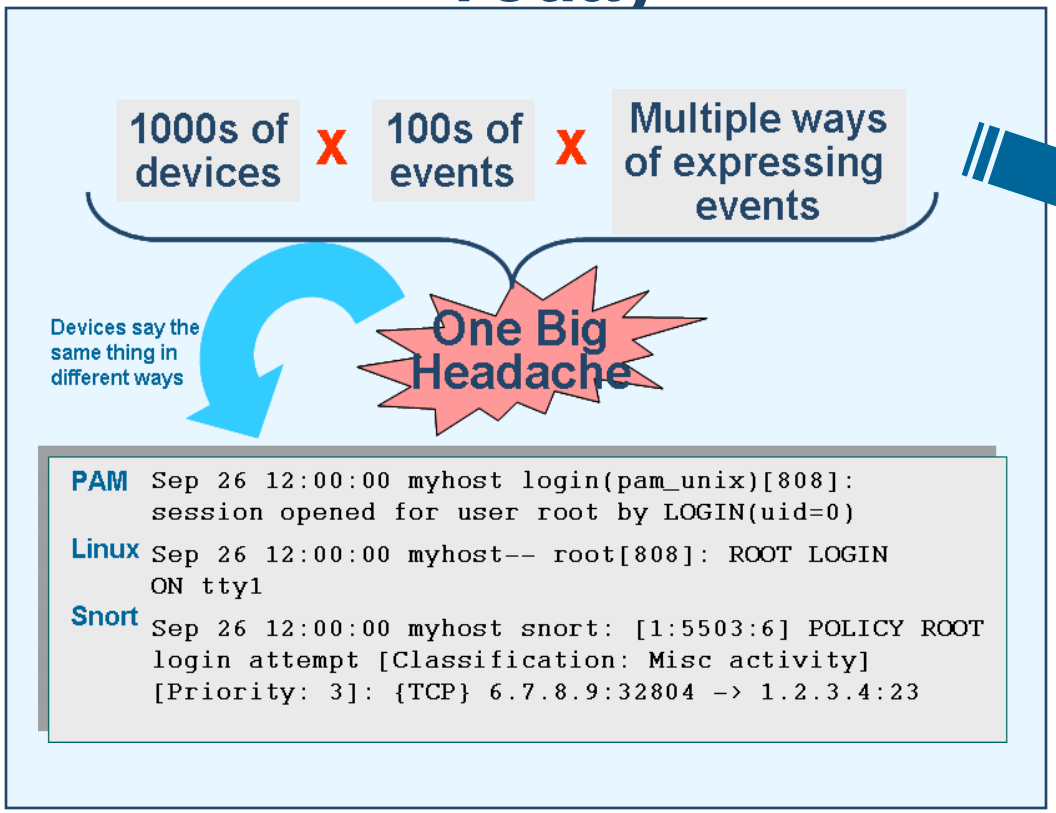


Approved for Public Release 08-1313

© 2008 The MITRE Corporation. All rights reserved

# The Challenge

## Today




Solve the problem of "inconsistent log formats", since "*there is no consensus in the security community as to the standard terms to be used to describe the composition of log entries and files*." (NIST Publication 800-92)

## Tomorrow ++

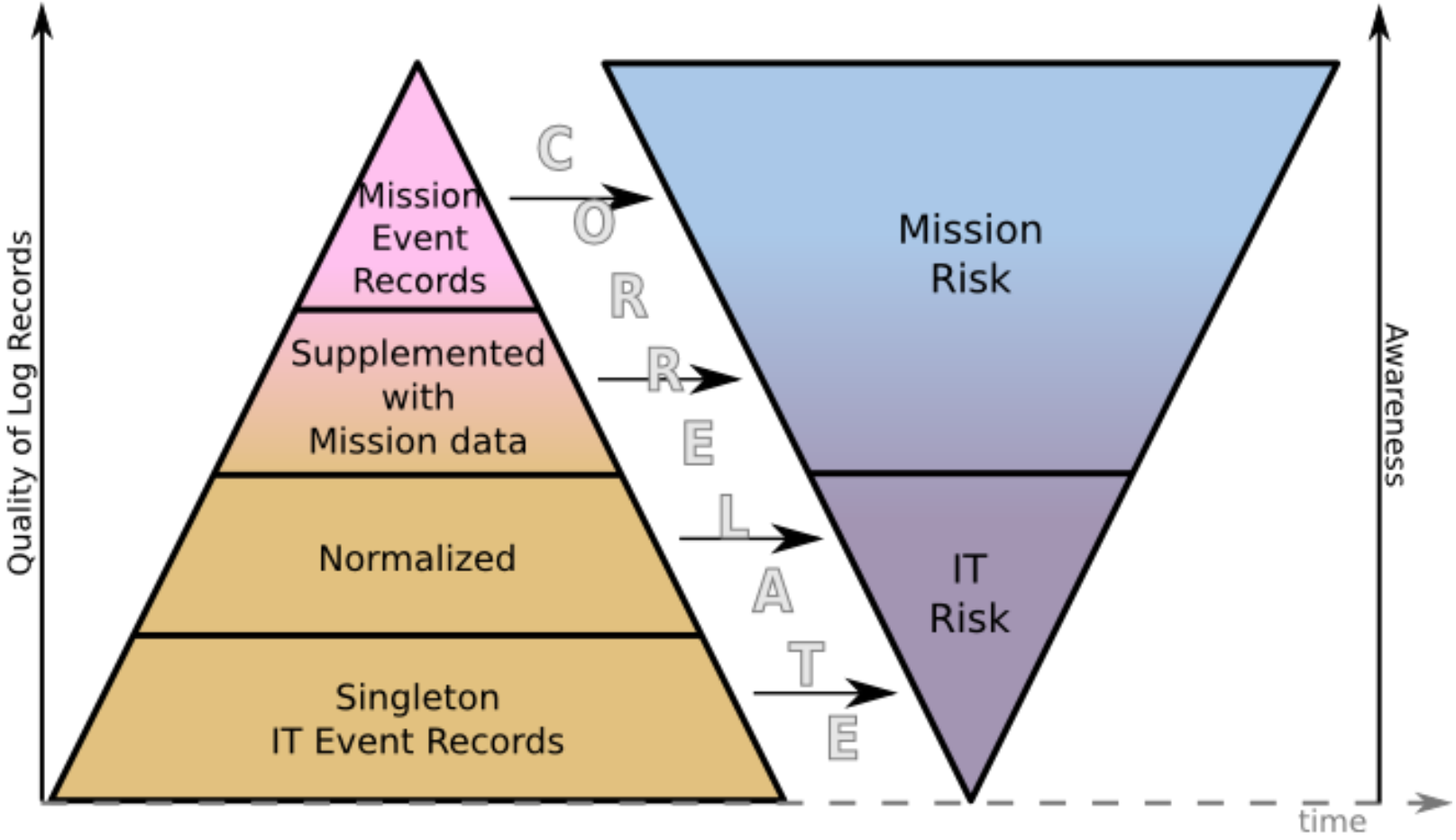
A Common Event Expression will improve

- Log management capabilities
- Log correlation (SIM) capabilities
- Device intercommunication enabling autonomic computing
- Enterprise-level situational awareness
- InfoSec Adversarial Modeling through the integration of Red, Blue, and White Team reports with sensor logs and SIM reports


Approved for Public Release 08-1313

© 2008 The MITRE Corporation. All rights reserved

# Motivation





© 2008 The MITRE Corporation. All rights reserved

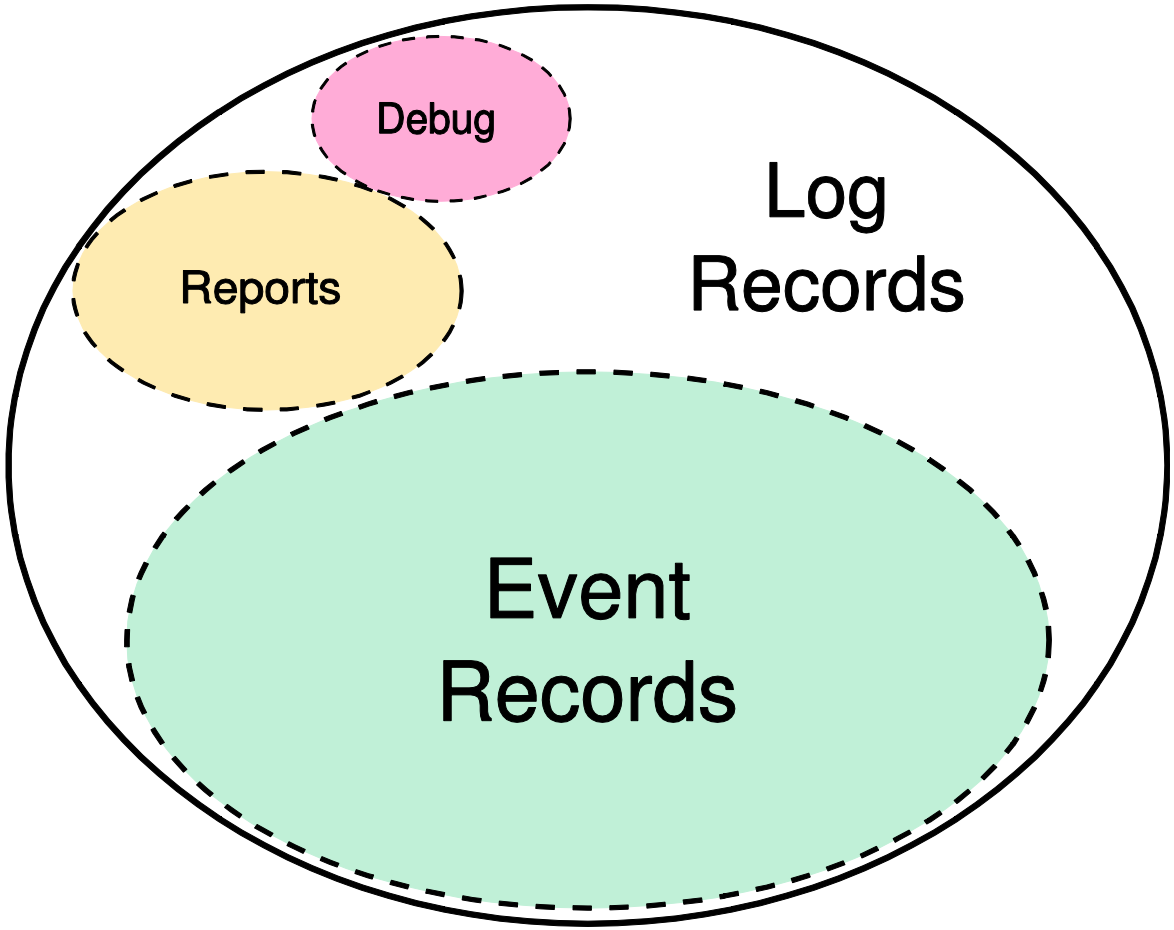
# From Events to Logs



Approved for Public Release 08-1313

© 2008 The MITRE Corporation. All rights reserved

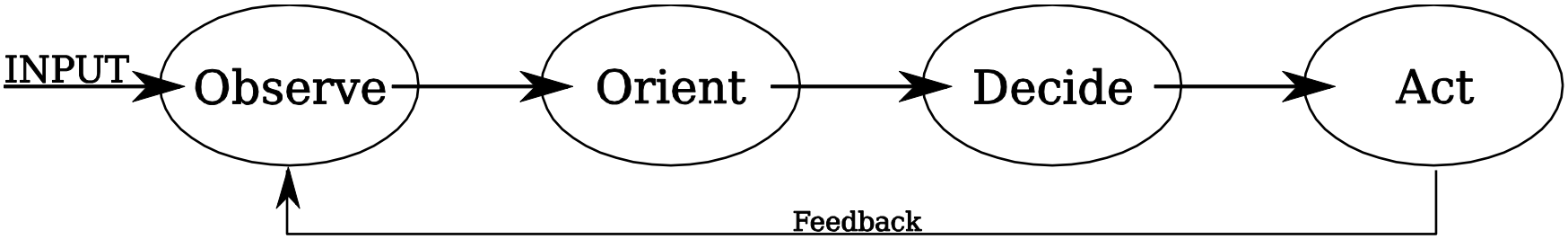
# The Log Space





© 2008 The MITRE Corporation. All rights reserved

# OODA Loop for CND

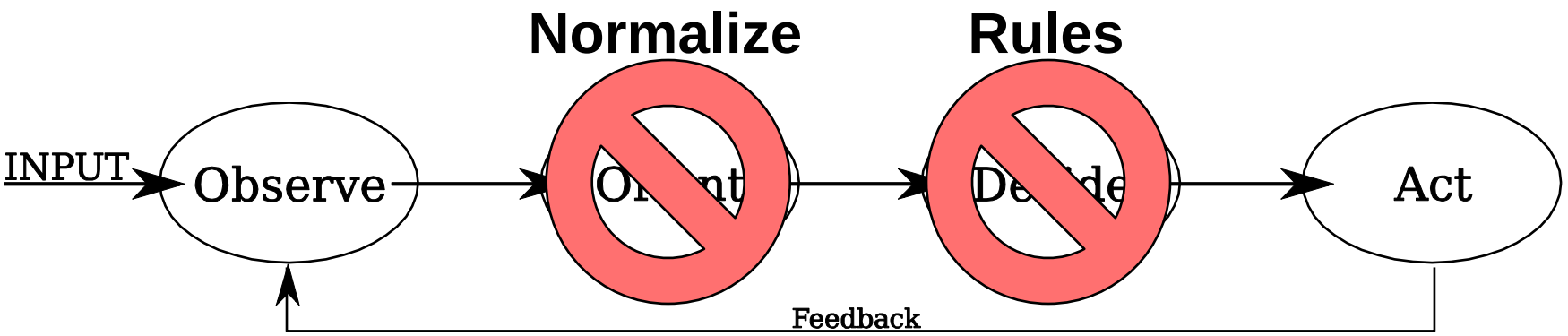



- Observe – Logs, Vulnerability Reports, News
- Orient – History, Policy, IT Information
- Decide – Good, Bad, Unknown, Watch, Ignore…
- Act – Block or Allow? Refine Rules or Policy?


Approved for Public Release 08-1313

© 2008 The MITRE Corporation. All rights reserved

# … Why It Doesn't Work




- CND designed for business efficiency
- Assume static, stable network architectures
- Rely on Normalization and Rules-based Signature Matching


© 2008 The MITRE Corporation. All rights reserved

# Problem

# LOGS ARE PRODUCED FOR THE WRONG AUDIENCE

**Humans understand semantics**

**Systems understand syntactics**


Approved for Public Release 08-1313

© 2008 The MITRE Corporation. All rights reserved

# Why Standardize? (1)

- **Missing Event Details**
- **Cryptic Records**

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

- **Problem: Inconsistent Success/Fail**

```
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
```


Approved for Public Release 08-1313

© 2008 The MITRE Corporation. All rights reserved

# Why Standardize? (2)

- **Inconsistent Event Descriptions**

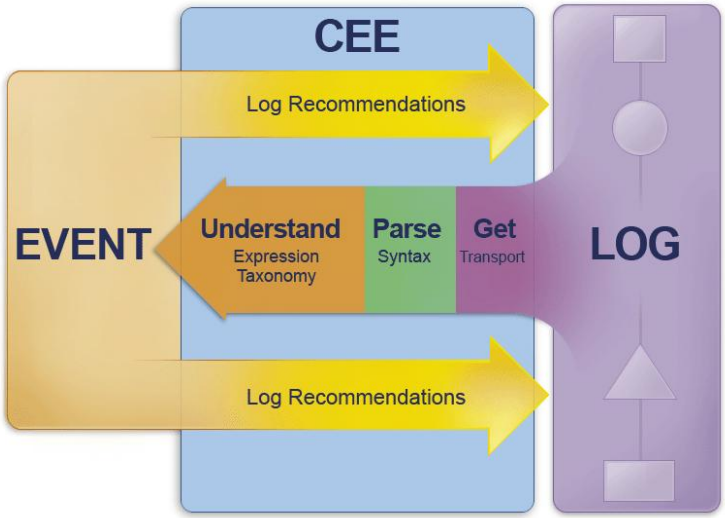
```
Sep 22 10:02:00 myhost login(pam_unix)[808]: session
  opened for user root by LOGIN(uid=0)

Sep 26 12:17:32 myhost-- root[808]: ROOT LOGIN ON tty1

Sep 26 13:00:40 myhost snort: [1:5503:6] POLICY ROOT
  login attempt [Classification: Misc activity]
  [Priority: 3]: {TCP} 6.7.8.9:32804 -> 1.2.3.4:23
```


Approved for Public Release 08-1313

© 2008 The MITRE Corporation. All rights reserved

# CEE Enabled Process

*CEE = Syntax + Vocabulary + Transport + Log Recommendations*

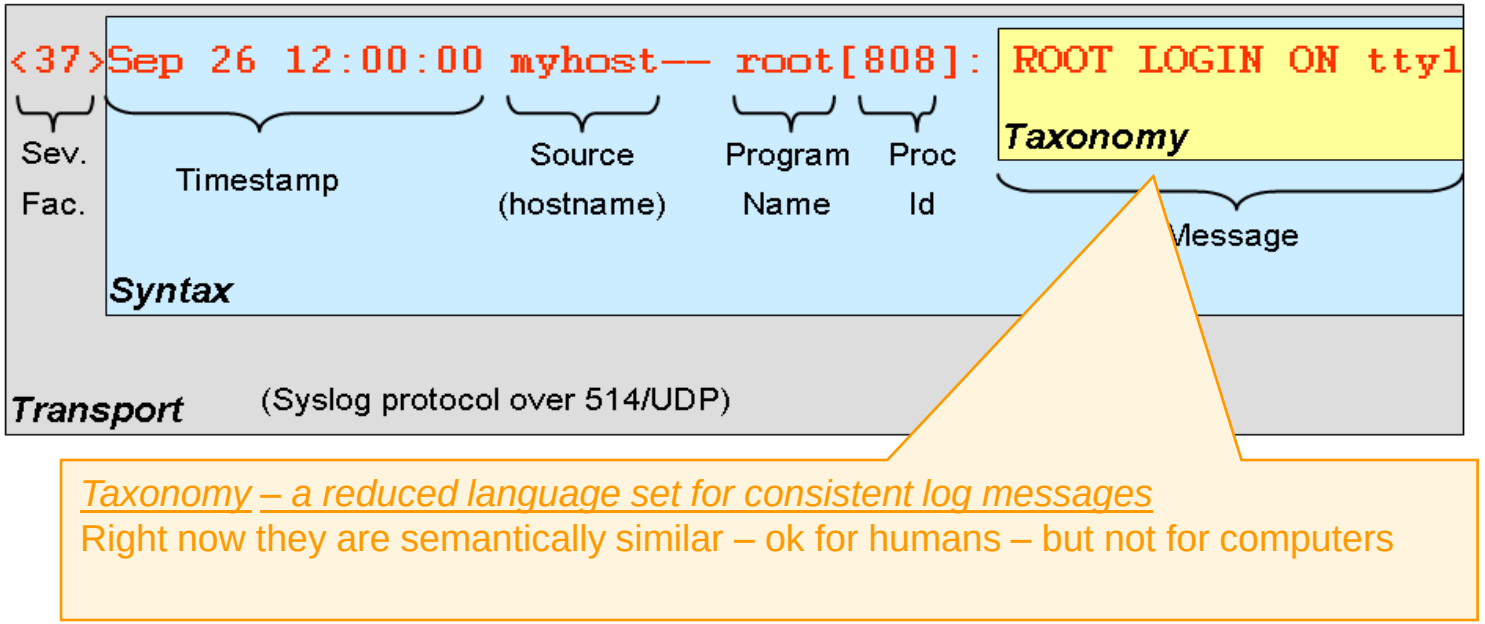



- Events recorded guided by ***Log Recommendations***
  - Events and details needed to be logged by devices (OS, IDS, FWs, etc.)
- Log messages exchanged via a ***Common Log Transport***
- Log messages received in a ***Common Log Syntax*** for parsing out relevant data
- ***Common Event Expression Taxonomy*** to specify the event in a common representation


Approved for Public Release 08-1313

© 2008 The MITRE Corporation. All rights reserved

# CEE Example (Cont.)



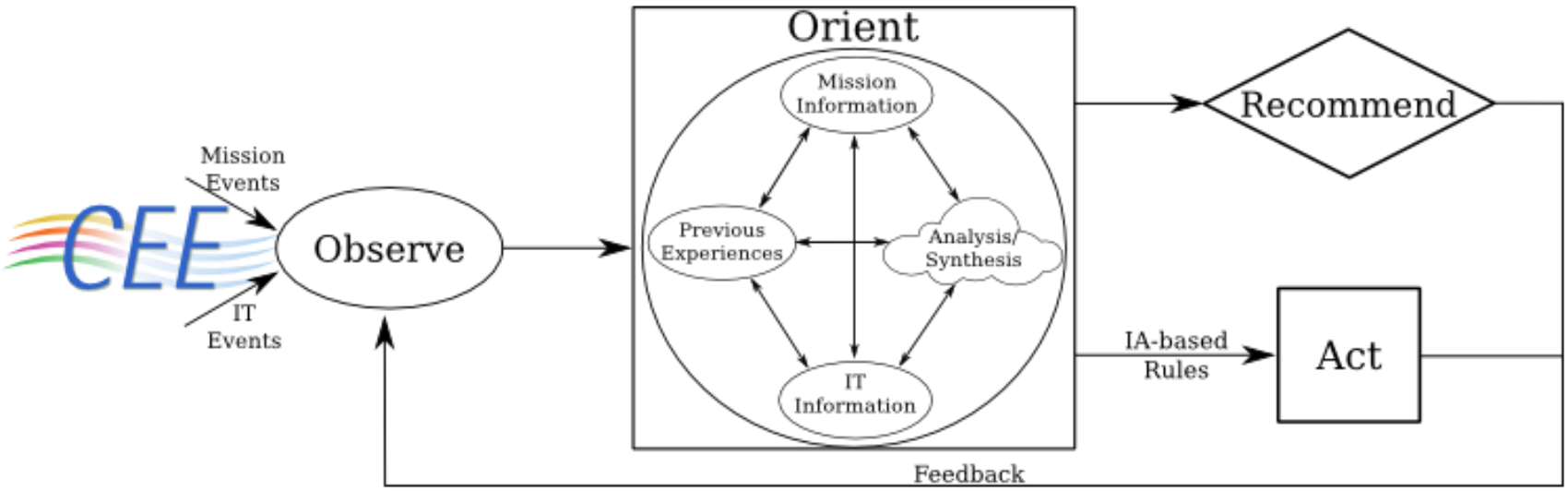

*Taxonomy – a reduced language set for consistent log messages*
Right now they are semantically similar – ok for humans – but not for computers

- **Scenario: An attacker has breached our network**
  - **1. Determine if any successful logins**
    - **What do we search for – 'log in', 'log in', 'logged on' etc.**


Approved for Public Release 08-1313

© 2008 The MITRE Corporation. All rights reserved

# Future Potential (1)

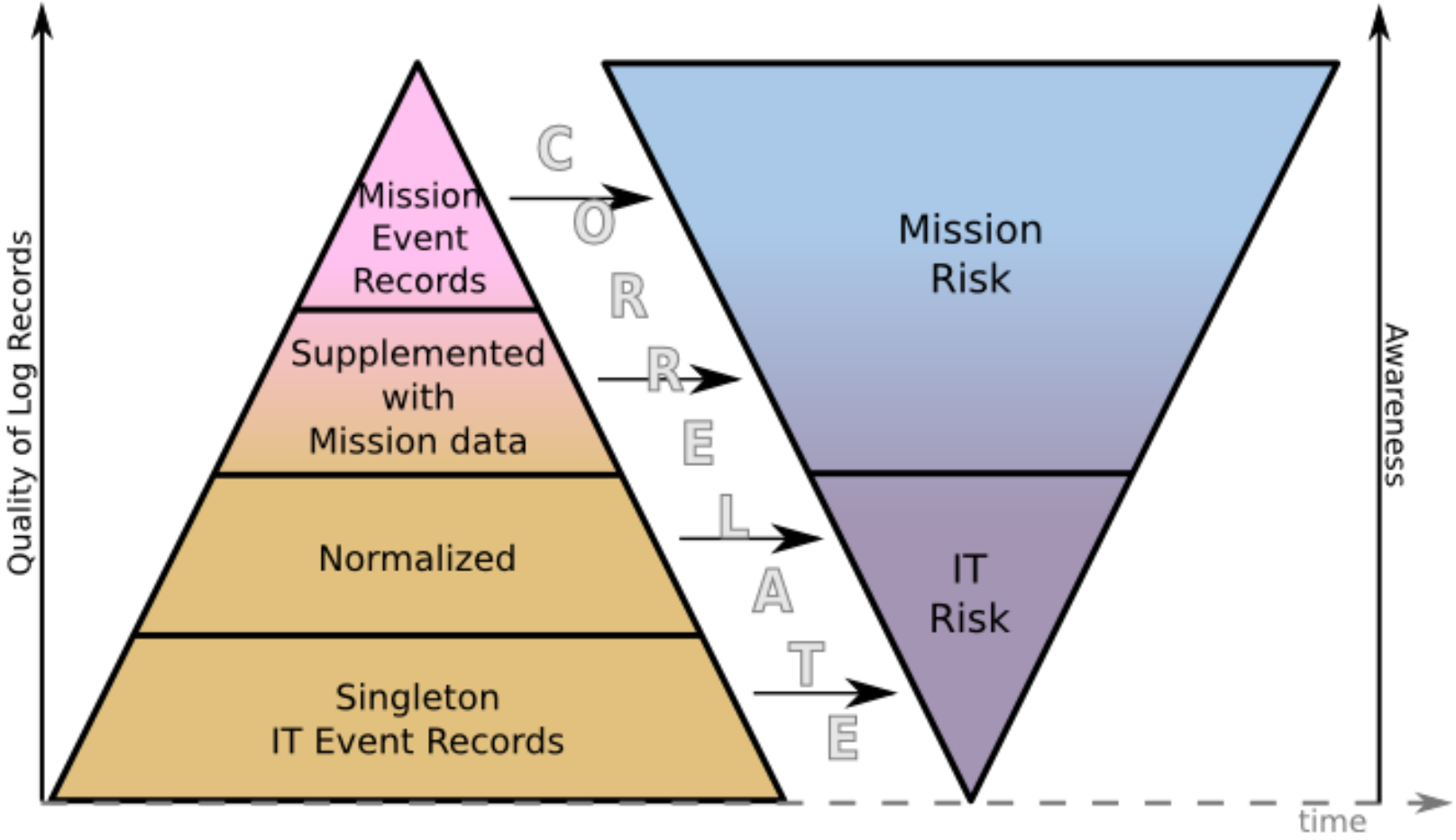



Move from IT to Mission-focused awareness


Approved for Public Release 08-1313

© 2008 The MITRE Corporation. All rights reserved

# Future Potential (2)





Approved for Public Release 08-1313

© 2008 The MITRE Corporation. All rights reserved

# How can You Help?

- Provide Your Log Requirements
- Join the Working Group
- Help Grow the Community
  - Request Vendors to Participate
  - Inform Others about the Effort

**http://cee.mitre.org**


Approved for Public Release 08-1313

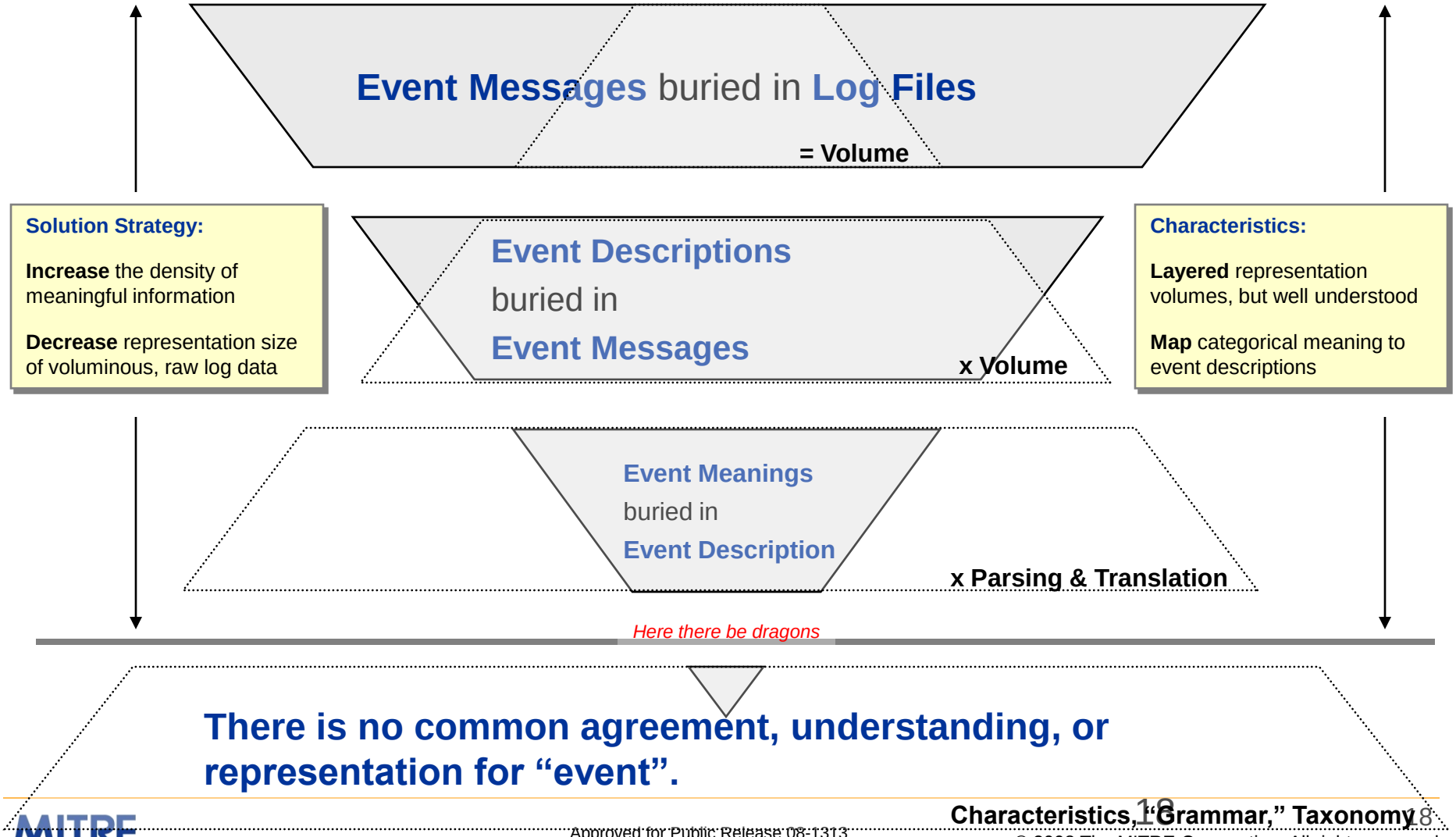
© 2008 The MITRE Corporation. All rights reserved

# Backups


Approved for Public Release 08-1313

© 2008 The MITRE Corporation. All rights reserved

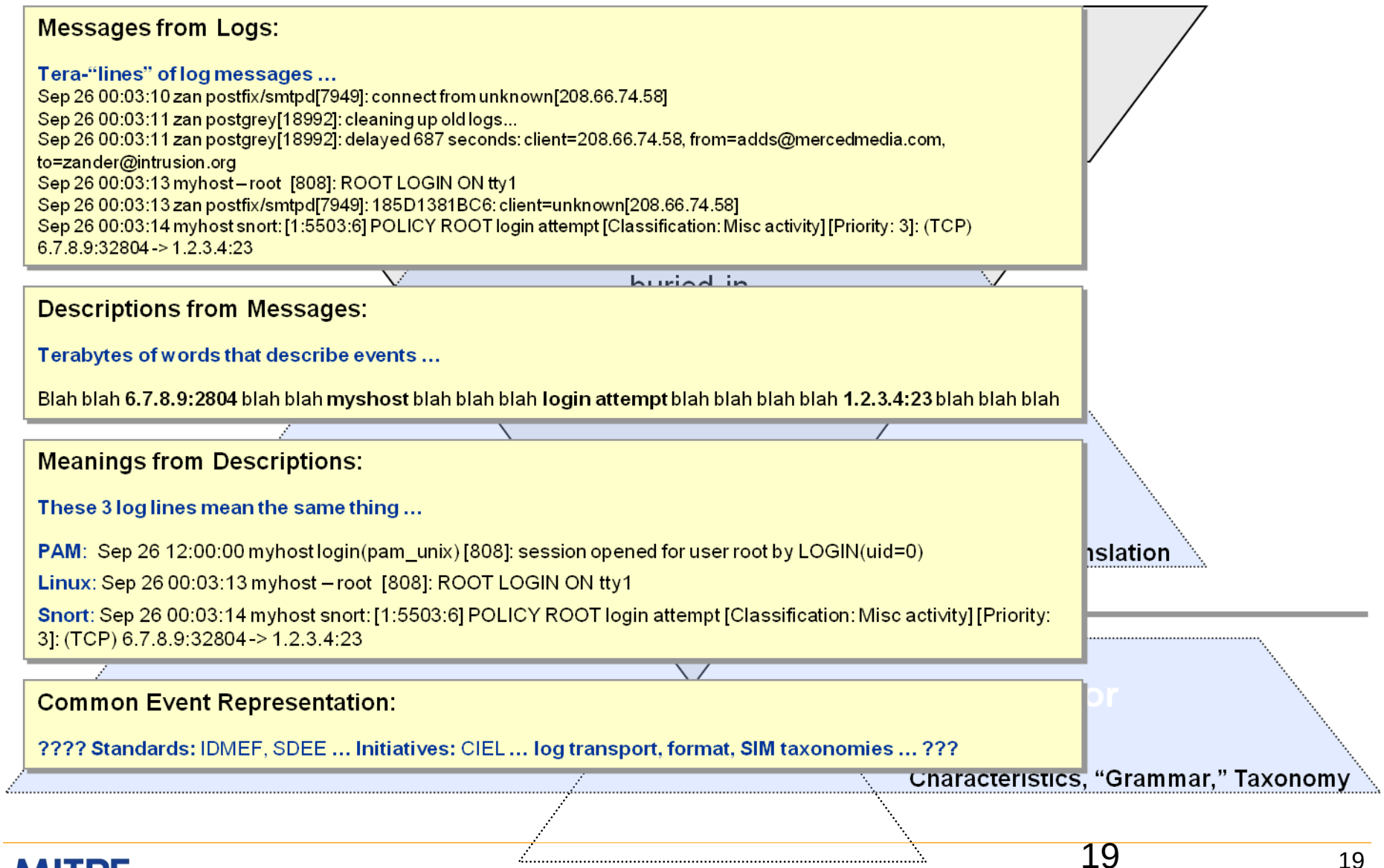
# CEE Challenge






© 2008 The MITRE Corporation. All rights reserved

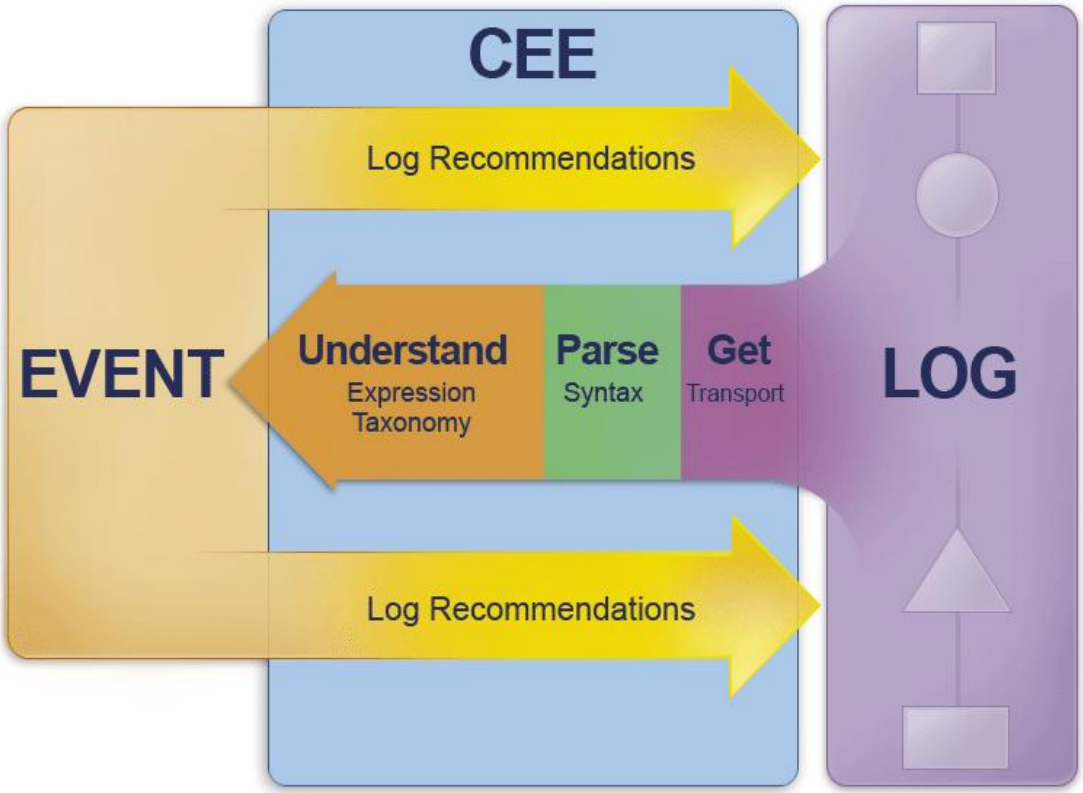
# CEE Challenge





© 2008 The MITRE Corporation. All rights reserved

# CEE




- Event Taxonomy
- Record Syntax
- Record Transport
- Log Recommendations

"[We] must keep it simple and stupid or it'll be ASN.1 before we know what hit us…" – Marcus Ranum


© 2008 The MITRE Corporation. All rights reserved

# CEE Example

## Example Log Messages

*Syntax - details specific to event being logged*

*Format (1 and 2)*
`month day time host program[pid]: message`

In CEE, each of these would be a possible syntax element, whose value and definition would be well defined by a Data Dictionary

```
1. Sep 26 12:00:00 myhost-- root[808]: ROOT LOGIN ON tty1
2. Apr 10 12:30:34 hostname sshd[16682]: error: PAM:
   Authentication failure for user1 from host.domain.com
3. Sep 19 08:26:10 zuric
   CEF:0|security|threatmanager|1.0|100|worm successfully
   stopped|10|src=10.0.0.1 dst=2.1.2.2 spt=1232
```

*Transport - successful log transmission*

Syslog (each log message is transmitted in a single UDP packet usually over port 514/UDP)

*Syntax - details specific to event being logged*
*Format (3) CEF message*

`CEF:Version|Device Vendor|DeviceProduct|DeviceVersion|Signature ID|Name|Severity|Extension`

Extension is a meta item – it imposes a sytax extension to specify addition details - a data dictionary can enumerate these details

Data Dictionary needed to enumerate details associated with the event
It needs to provide flexible syntax options by defining the elements and formats

Ex: dst in the CEF event – defined by a dotted quad IPv4 address


Approved for Public Release 08-1313

© 2008 The MITRE Corporation. All rights reserved

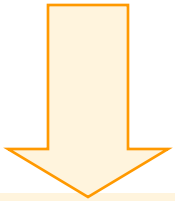
# CEE Taxonomy

Event Message Details

```
1. ROOT LOGIN ON tty1
2. error: PAM: Authentication failure for user1 from
   host.domain.com
3. worm successfully stopped
```

- Scenario: An attacker has breached our network
  - 1. Determine if any successful logins
    - What do we search for – 'log in', 'login', 'logged on', authentication?

Example of CEE Event Taxonomy



```
1. Login (tty1) for user (root) successful
2. Login for user (user1) failed from
   host.domain.com
3. worm stopped
```



Approved for Public Release 08-1313



© 2008 The MITRE Corporation. All rights reserved