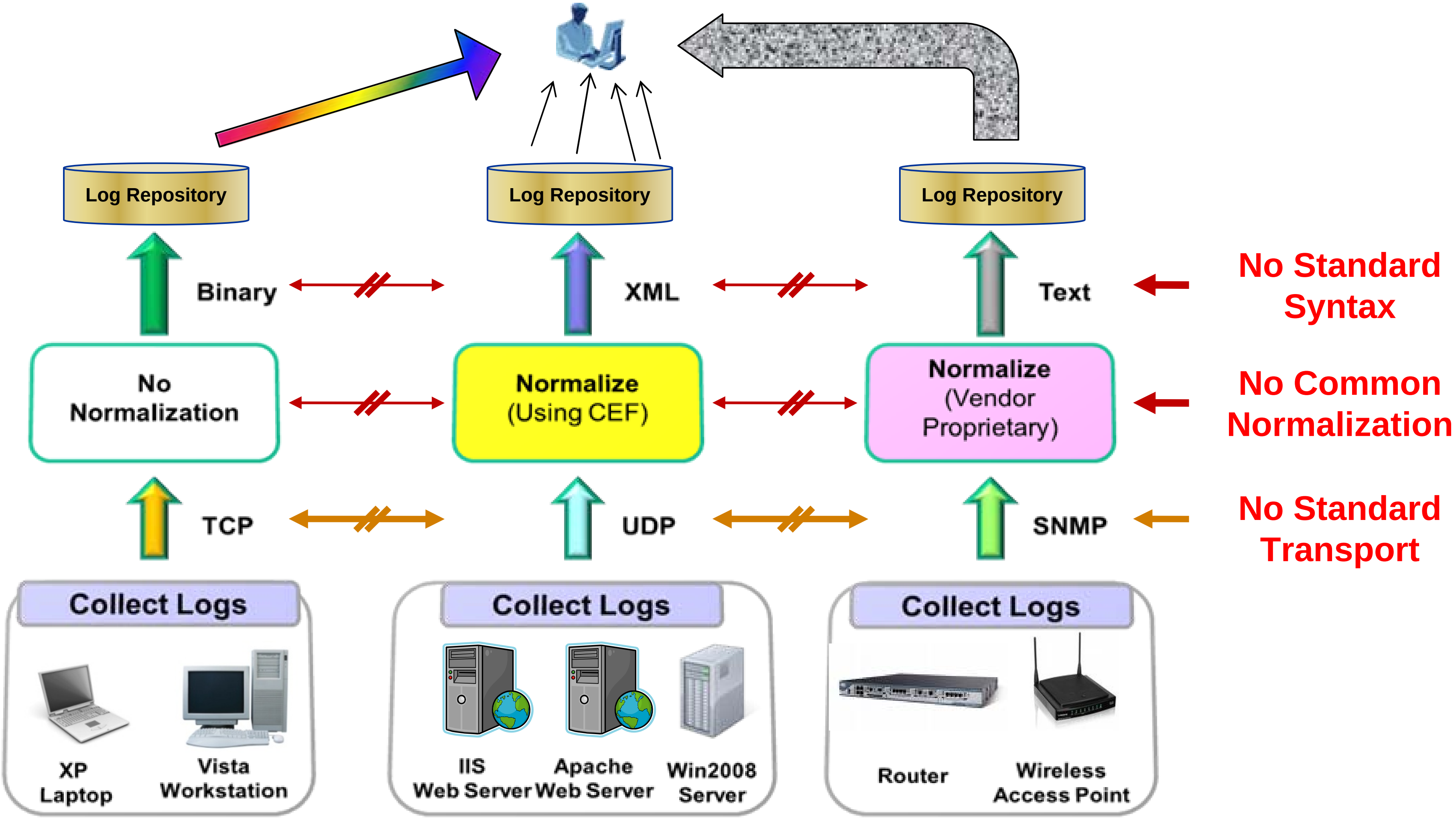
# Using Standardization to Enhance Insider Threat Analysis of Audit Data

Dr. Bruce Gabrielson (BAH)
CND R&T PMO
28 October 2009

# Audit Log Problems

- Audit logs are cumbersome and traditionally used after the fact for forensics analysis.
- Identifying insider threat activities in near real time using audit logs is a useful technique to approach the problem.
  - Efficiently analyzing platform generated audit log data using industry vetted normalization and transport standards would enable automated analysis including multi-platform analysis.

# Nonstandard Audit Log Formats



Log Repository | Log Repository | Log Repository

Binary | XML | Text ← No Standard Syntax

No Normalization | Normalize (Using CEF) | Normalize (Vendor Proprietary) ← No Common Normalization

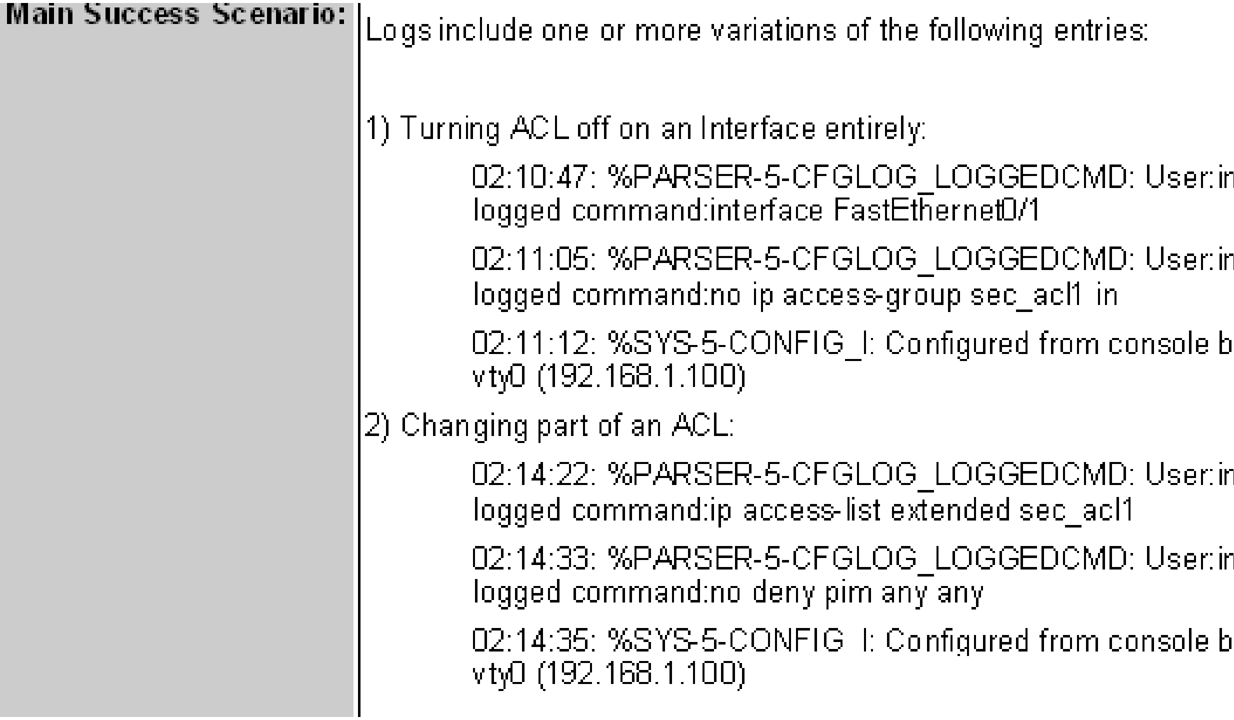
TCP | UDP | SNMP ← No Standard Transport

Collect Logs: XP Laptop, Vista Workstation

Collect Logs: IIS Web Server, Apache Web Server, Win2008 Server

Collect Logs: Router, Wireless Access Point

# Example of Use Case Log Formats



**Main Success Scenario:**

Logs include one or more variations of the following entries:

1) Turning ACL off on an Interface entirely:

```
02:10:47: %PARSER-5-CFGLOG_LOGGEDCMD: User:insider
logged command:interface FastEthernet0/1

02:11:05: %PARSER-5-CFGLOG_LOGGEDCMD: User:insider
logged command:no ip access-group sec_acl1 in

02:11:12: %SYS-5-CONFIG_I: Configured from console by insider on
vty0 (192.168.1.100)
```

2) Changing part of an ACL:

```
02:14:22: %PARSER-5-CFGLOG_LOGGEDCMD: User:insider
logged command:ip access-list extended sec_acl1

02:14:33: %PARSER-5-CFGLOG_LOGGEDCMD: User:insider
logged command:no deny pim any any

02:14:35: %SYS-5-CONFIG  I: Configured from console by insider on
vty0 (192.168.1.100)
```

**The problem is understanding what the specific data element means for the platform sensor being analyzed.**

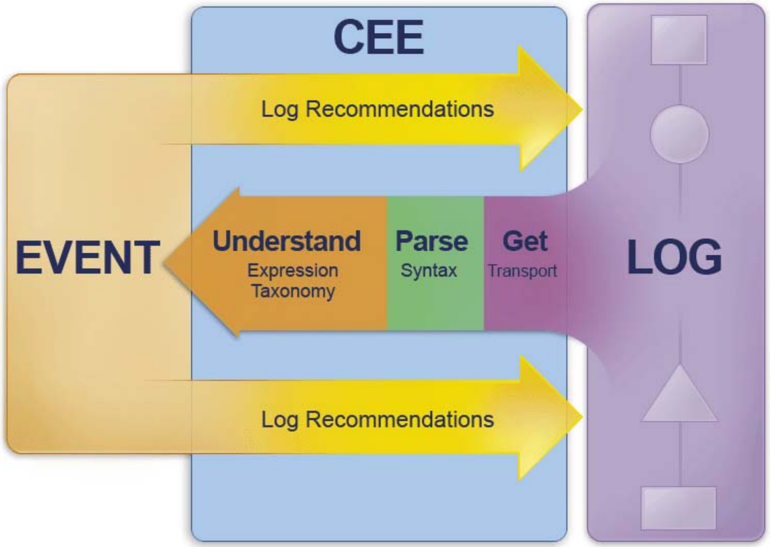
# EMAP

- EMAP (Event Management Application Protocol) is a framework for describing a standardized format to express, enumerate, measure, and interact with event data from heterogeneous sources in an attempt to streamline event management.
- The EMAP framework will have similarities to the Security Content Automation Protocol (SCAP) in its construction.

# CEE Normalizes Data Across Platforms

**CEE differs from other log standards in that it breaks the recording and exchanging of logs into four (4) components:**

- **Event Taxonomy**
  - **Specifies the type of event. A reduced language set or event listing can be used to ensure that all events of the same type are recorded in the same way.**
- **Log Syntax**
  - **How the event and its details are recorded. The syntax could be a binary encoded, XML, or other text-based specification, and allows the data to be unambiguously parsed from the logs. To maintain consistency and compatibility among the different syntaxes, CEE provides a data dictionary. The dictionary contains the unique syntax identifiers along with their meaning, format, and usage suggestions.**
- **Log Transport**
  - **The transport simply defines how the logs are transmitted.**
- **Logging Recommendations**
  - **A collection of logging best practices and log-related information. While not a standard itself, it is a complementary portion of CEE to ensure maximum utility.**



# Questions?

**Dr. Bruce Gabrielson**

**bcgabri@nsa.gov**