Supplementing Event Standards for Mission Assurance

William Heinbockel
The MITRE Corporation
heinbockel@mitre.org
The role of Computer Network Defense (CND) is mission support.

- Obtain Cyber Situational Awareness
- Enable Key Components for Cyber Defense
- Fight Through Cyber Attacks

Events (Logs) are the input into the CND process. Common Event Expression (CEE) is attempting to standardize log data, improving cyber awareness.
How well does your CND work in this environment?
CND Methodology

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

Problem: There is no “mission” in Computer Network Defense!

Solution: Mission Network Defense (MND)
MND Framework

What is Different?
CEE Overview

CEE = Syntax + Vocabulary + Transport + Log Recommendations

- Events recorded guided by **Log Recommendations** – *Events and details needed to be logged by devices*
- 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 type
Mission Assurance via CEE

- **Taxonomy:** Expression of Mission-based Events (e.g., Tasking, Objectives)

- **Syntax:** Mission-relevant Details (e.g., geolocation, weather, service, unit identification)

- **Transport:** Efficiency, Support for high latency, low bandwidth connections

- **Recommendations:** IT-Mission Event Relationships, Mission- or Environment-based Event Prioritization
MND Vision

- Mission Event Records
- Supplemented with Mission data
- Normalized
- Singleton IT Event Records

- Mission Risk
- IT Risk

Quality of Log Records vs. Awareness over time
The Way Forward

- Experimentation (fielding trial at JEFX ’09)
- Provide Your IT/Mission Requirements
- Join the CEE Working Group
- Help Grow the Community
  - Must Get Vendor Participation
  - Inform Others about the Effort

http://cee.mitre.org
If you go as far as you can see, you will then see enough to go even farther.
- John Wooden