Common Event Expression — CEE™

A standard log language for event interoperability in electronic systems

CEE standardizes the way computer events are described, logged, and exchanged. By utilizing a common language and syntax, CEE takes the guesswork out of even the most menial of event- or log-related tasks. Tasks including log correlation and aggregation, enterprise-wide log management, auditing, and incident handling which once required expensive, specialized analysts or equipment can now be performed more efficiently and produce better results.

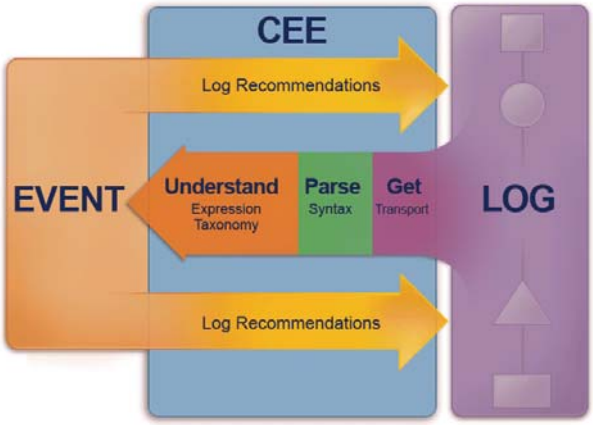
Why CEE

If multiple systems observe the same occurrence, it should be expected that their description of that event is identical. When combined with relevant event details (time, source, destination), a computer should be able to immediately determine whether two or more logs, data logs, audit logs, alerts, alarms, or audit trails refer to the same event. In order to make this happen, there needs to be a scalable, well-defined way to express events.

Currently, vendors and products employ varying logging practices such as using inconsistent formats and terminology when describing events. This presents a significant burden to analysts and products in normalizing the vast quantities of heterogeneous log records, allowing for aggregation, correlation, and further processing. With the potential for varying interpretations among event log consumers, the network and security awareness levels will fluctuate. *NIST Publication 800-92: Guide to Computer Security Log Management* describes this as a major problem stemming from “inconsistent log formats,” noting that “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.”

Solution

CEE addresses the problem of event representation and communication. Previous attempts in this area have failed in gaining adoption since they only target a portion of the larger problem by providing log format guidelines and ignoring the content. As a solution, the CEE Initiative recommends that the industry coordinate in four areas to facilitate log transmission and interpretation:



A CEE-Enabled Process

- Create an event expression taxonomy for uniform and precise log definitions that lead to a common event representation.
- Create log syntaxes utilizing a single data dictionary to provide consistant event specific details.
- Standardize flexible event transport mechanisms to support mulitple environments.
- Propose log recommendations for the events and attributes devices generate.

CEE™

The MITRE Corporation—a Federally Funded Research and Development Center—maintains CEE and provides impartial technical guidance to the CEE Working Group throughout the process to ensure CEE serves the public interest.

202 Burlington Road, Bedford, MA 01730-1420
www.mitre.org

MITRE

CEE Benefits

CEE provides vendors, end-users, event producers, and event consumers many advantages over the current log management space.

Single, Consistent, Unambiguous Log Records	Log standardization reduces false positive alerts while improving event-related content, resulting in more accurate and efficient log management, correlation, and forensic analysis. By utilizing common syntaxes and terminology, you will never have to guess the meaning of your log records again.
Better Regulatory Compliance	CEE simplifies the task of establishing and maintaining of various compliance standards that incorporate audit or security guidelines, including PCI DSS, SOX, and GLBA.
Improved Security Awareness	CEE represents a large component of the "Monitor and Evaluate" portion of the COBIT structure and supports many of the management procedures present in the ITIL framework.
De-Facto Enterprise Event Communication Standard	With every device supporting the same event log standard there is instant interoperability potential for devices deployed across multi-national enterprises and governments.
Vendor and Device Agnostic	Established log management infrastructures rely on the logs generated by several chosen devices, essentially locking the customer into the use of those products. The purchasing of replacements or upgrades requires a costly testing and process overhaul to maintain an equivalent level of awareness. CEE frees customers from product dependency, enabling new devices to be quickly integrated into the current environment.
Reduced IT and Security Operations Costs	Decreased log management overhead combined with more efficient analysis and an increased capability for log library and product reuse means that companies can drastically reduce their log-related budgets. With a standard set of information, operations centers will not require auditors and operators to be trained in interpreting messages in product-specific languages. Fewer operators can be leveraged to manage more systems.
Log Message Internationalization	Standard expressions result in unambiguous interpretation. Instead of vendors needing to individually produce and maintain libraries of international log messages, CEE allows for a single application to more easily translate any CEE-compatible log record.

Join the CEE Working Group

We have established a CEE Working Group mailing list for those interested in actively participating in this initiative.

If you or your organization would like to be considered for possible involvement in this working group, please contact us at cee@mitre.org.

Member of

http://measurablesecurity.mitre.org

Making Security Measurable™

To Participate - cee@mitre.org